

Manuel

Guide pour accroître la résilience des TIC dans le secteur de l'électricité

La «voie à suivre» pour accroître la résilience
des TIC dans le secteur de l'électricité

LVR – CH 2024

Mentions légales et contact

Éditeur

Association des entreprises électriques suisses AES
Hintere Bahnhofstrasse 10
CH-5000 Aarau
Téléphone +41 62 825 25 25
Fax +41 62 825 25 26
info@electricite.ch
www.electricite.ch

Auteurs et autrices de la première édition

Stefan Mattmann	CKW AG	Auteur
Reto Amsler	ALSEC AG	Co-auteur

Collaboration des experts de la Cyber Security Task Force de l'AES suivants

Mattia Bardelli	AET	Membre de la Cyber Security Task Force de l'AES
Reto Bondolfi	EWZ	Membre de la Cyber Security Task Force de l'AES
Marc Engeli	EKZ	Membre de la Cyber Security Task Force de l'AES
Christian Gubler	AES	Membre de la Cyber Security Task Force de l'AES
Stéphane Henry	OFEN	Membre de la Cyber Security Task Force de l'AES
René Hugentobler	BKW	Membre de la Cyber Security Task Force de l'AES
Dimitri Klimov	Alpiq	Membre de la Cyber Security Task Force de l'AES
Michael Knuchel	Swissgrid	Membre de la Cyber Security Task Force de l'AES
Renald Marmet	BKW	Membre de la Cyber Security Task Force de l'AES
Dominik Märki	Axpo	Membre de la Cyber Security Task Force de l'AES
Adrian Märklin	Swisspower	Membre de la Cyber Security Task Force de l'AES
Michele Paganini	Repower	Membre de la Cyber Security Task Force de l'AES
Markus Riner	AES	Membre de la Cyber Security Task Force de l'AES

Responsabilité commission

La Task Force Cyber Security de l'AES est responsable de la maintenance et du développement du document.



Chronologie

Date	Brève description
15.01.2024	Version 0.1 Première édition en projet
28.02.2024	Versions 0.1 ... 0.5 Révisions par la Cyber Security Task Force de l'AES
15.03.2024	Version 1.0 pour traduction et consultation / validation
19.09.2024	Version 1.1 ajustements après feedback / révision

Ce document a été élaboré avec l'implication et le soutien de l'AES et de représentants de la branche.

L'AES approuve ce document à la date du 21.10.2024.

Imprimé n° LVR/FR, édition 2024

Copyright

© Association des entreprises électriques suisses AES

Tous droits réservés. L'utilisation des documents pour un usage professionnel n'est permise qu'avec l'autorisation de l'AES et contre dédommagement. Sauf pour usage personnel, toute copie, distribution ou tout autre usage de ces documents que celui prévu pour le destinataire sont interdits. Les auteurs déclinent toute responsabilité en cas d'erreur dans ce document et se réservent le droit de le modifier en tout temps sans préavis.

Égalité linguistique entre femmes et hommes

Dans le souci de faciliter la lecture, seule la forme masculine est utilisée dans le présent document. Toutes les fonctions et les désignations de personnes s'appliquent toutefois tant aux femmes qu'aux hommes. Merci de votre compréhension.



Table des matières

Préface	10
Introduction	11
1. Contexte	12
1.1 Objectif, but et portée	13
1.2 Public cible	14
1.3 Structure du document	15
1.4 Conseils, remarques, invitations et informations	15
2. Introduction	16
2.1 Amélioration continue de la résilience des TIC	16
2.2 Délimitation	17
2.3 Contexte	17
2.4 Menaces et risques	18
3. Environnement Alimentation électrique pour accroître la résilience des TIC	19
3.1 Règles de l'AES pour le secteur de l'électricité visant à accroître la résilience des TIC	19
3.2 Acteurs / parties prenantes	19
3.2.1 Parties prenantes au niveau fédéral	19
3.2.2 L'Association des entreprises électriques suisses (AES)	20
3.2.3 Entreprise d'approvisionnement en électricité EAE (domaine électrique)	20
3.2.4 CERT, CIRT, CSIRT et SOC	20
3.2.5 Fabricants et fournisseurs	21
3.3 Bases légales: lois et règlements obligatoires	23
3.3.1 Aperçu des lois, ordonnances et dispositions légales en rapport avec la sécurité de l'approvisionnement et de l'information	23
3.3.2 OFPP Stratégie nationale de protection des infrastructures critiques	24
3.3.3 Guide de l'OFPP sur la protection des infrastructures critiques	25
3.3.4 OFAE Norme minimale TIC pour améliorer la résilience des TIC	25
3.3.5 OFAE Norme minimale TIC - Outil d'évaluation selon NIST CSF 1.1	26
3.3.6 OFEN Engagement de la norme minimale pour les TIC pour accroître la résilience des TIC	28
3.3.6.1 Niveau de protection selon l'OFEN	29
3.3.6.2 Attribution des tâches au niveau de la sous-catégorie à chaque catégorie et valeurs de niveau de protection définies pour chaque maturité (tiers)	30
3.3.7 ECom: suivi de l'approche et des résultats en matière d'amélioration de la résilience des TIC	31
3.3.8 Office fédéral de la cybersécurité (BACS): obligation de signalement et aide	32
3.3.8.1 Obligation de déclaration pour les infrastructures critiques	32
3.3.8.2 Obligation de la Confédération de fournir une assistance en cas de cyberattaque	32
3.4 Institutions, cadres, normes, standards, spécifications et lignes directrices pour améliorer la résilience des TIC	33
3.4.1 Frameworks, normes, standards et spécifications	33
3.4.2 Guidelines et publications spéciales	33
3.5 Certifications et formations pour accroître la résilience des TIC	34
3.5.1 Formations initiales et continues avec certifications	35
3.5.1.1 Cybersécurité IT/OT de l'AES pour les ingénieurs système	35
3.5.1.2 Offre de formation de l'AES dans le cadre du guide	35
3.5.1.3 Autres possibilités de formation et de perfectionnement	35
3.5.2 Certifications de sécurité pour les entreprises et les unités organisationnelles	36
3.5.2.1 Certification de l'ISMS selon la norme ISO 27001	36
3.5.2.2 Certification de l'application du cadre de cybersécurité du NIST	36
4. Base de l'efficacité pour améliorer la résilience des TIC	37
4.1 Le système de gestion intégré SGI	37
4.2 La gestion de la sécurité de l'information (GSI) comme base pour accroître la résilience des TIC	38



4.3	Système de gestion de la sécurité et de la santé au travail pour soutenir l'augmentation de la résilience des TIC.....	38
4.4	Gestion des processus, des risques, de la continuité des activités et des urgences comme bases supplémentaires pour augmenter la résilience des TIC.....	39
4.4.1	Gestion des processus	39
4.4.2	Gestion des risques	40
4.4.3	Gestion de la continuité des activités (BCM)	41
4.4.3.1	Analyse d'impact sur les activités (BIA).....	42
4.4.4	Gestion des situations d'urgence.....	43
4.5	Stratégie de cybersécurité selon le principe Defense in Depth	43
5.	Les bases pour augmenter la résilience des TIC.....	44
5.1	Compréhension fondamentale de la démarche	44
5.2	Complexité et portée de la sécurité de l'information pour accroître la résilience des TIC	45
5.3	Efforts en matière de sécurité de l'information pour accroître la résilience des TIC	45
5.4	Les bases d'une augmentation réussie de la résilience des TIC.....	46
5.4.1	Éléments nécessaires à une augmentation réussie de la résilience des TIC	46
5.4.2	Des ressources suffisantes pour accroître la résilience des TIC	46
5.4.3	Système de gestion intégré (SGI).....	47
5.4.4	Augmenter la résilience des TIC selon le cycle de Deming	48
5.4.5	Sécurité de l'information: politique et stratégie.....	50
5.4.5.1	Politique de sécurité de l'information (PSI).....	50
5.4.5.2	Stratégie de sécurité de l'information (SSI)	51
5.4.6	Sécurité de l'information: Responsabilité.....	52
5.4.6.1	Responsabilités selon le modèle RASCI	53
5.4.7	Sécurité de l'information: organisation et organigramme	54
5.4.7.1	Fonctions de l'organigramme de sécurité au niveau stratégique:	55
5.4.7.2	Fonctions de l'organigramme de sécurité au niveau tactique:	55
5.4.7.3	Fonctions de l'organigramme de sécurité au niveau opérationnel:	56
5.4.7.4	Éléments transversaux de l'organigramme de sécurité à tous les niveaux:.....	60
5.4.8	Sécurité de l'information: Maison des processus (House of Processes)	61
5.4.8.1	Structure de la Maison des processus.....	61
5.4.8.2	Responsabilités et compétences au sein de la Maison des processus	65
5.4.9	Sécurité de l'information: Maison des politiques (House of Policies)	65
5.4.9.1	Structure de la Maison des politiques	65
5.4.9.2	Responsabilités et compétences au sein de la Maison des politiques.....	67
5.4.9.3	Objectifs et preuves	67
5.4.9.4	Maîtrise des documents à la Maison des politiques	67
5.4.9.5	Aperçu des documents de la Maison des politiques sur l'augmentation de la résilience des TIC aux niveaux 0 à 3	68
5.4.9.6	Cartographie de la Maison des politiques avec le CSF NIST CSF 1.1	69
5.4.9.7	Mapping de l'ISO 27001:2022 Annexe A avec les documents de la Maison de la politique.....	70
5.4.9.8	Listes des objectifs et des preuves dans la Maison des politiques	70
5.4.10	Système de gestion de la sécurité de l'information (ISMS)	70
5.4.10.1	Raisons de la mise en place d'un ISMS:	70
5.4.10.2	Mise en place d'un ISMS	71
5.4.10.3	ISMS selon ISO 27001	72
5.4.10.4	Les phases de l'AES pour la mise en place d'un ISMS.....	73
5.4.11	Sécurité de l'information: CSF NIST version 1.1	74
5.4.12	Sécurité de l'information: mise en réseau de l'ISMS avec le CSF NIST 1.1	74
5.4.13	Sécurité de l'information: collaboration.....	75
5.5	Outils pour améliorer la résilience des TIC	76
5.5.1	Outils de l'AES pour accroître la résilience des TIC	77
5.5.2	Autres outils disponibles pour aider à augmenter la résilience des TIC.....	78
6.	Procédure pour augmenter la résilience des TIC: mise en place du ISMS avec mise en réseau du CSF NIST 1.1	78



6.1	Phase 1: base et planification; décision d'adopter un ISMS; définition des objectifs	80
6.1.1	Sensibilisation et engagement des cadres supérieurs en matière de sécurité de l'information.....	80
6.1.2	Identification des groupes d'intérêt (stakeholders)	81
6.1.3	Présenter et appliquer les exigences légales et réglementaires	81
6.1.4	Définir l'applicabilité (outils d'évaluation)	82
6.1.5	Mise en évidence et déclinaison des processus commerciaux	83
6.1.6	Identifier les champs d'action pour la sécurité de l'information	84
6.1.7	Définir / adapter l'objectif de la sécurité de l'information	85
6.1.8	Décision de principe pour l'introduction d'un ISMS au niveau du groupe ou de la direction (niveau C).....	86
6.1.9	Définir et initier les objectifs du ISMS	87
6.2	Phase 2: direction et initialisation; état des lieux	88
6.2.1	Créer et mettre en place la politique et la stratégie de sécurité de l'information: Comment traiter la sécurité de l'information ?	88
6.2.2	Définir le cadre de la sécurité de l'information: Créer une directive sur la sécurité de l'information et une directive sur le cadre de la sécurité de l'information.	89
6.2.3	Création des conditions préalables.....	89
6.2.4	Déterminer le statu quo / effectuer une analyse de la situation actuelle dans le domaine de la sécurité de l'information	90
6.2.5	Définir le champ d'application du ISMS dans son ensemble	90
6.2.6	Mettre en place et adapter l'organisation de la sécurité	91
6.2.7	Définir / adapter les responsabilités.....	91
6.2.8	Définir des indicateurs de performance (KPI).....	92
6.2.9	Définir une procédure pour les audits.....	92
6.3	Phase 3: planification de la mise en place et du déroulement; sensibilisation et formation; définition de l'«état souhaité»	93
6.3.1	Mettre en place, adapter et étendre un ISMS.....	94
6.3.2	Introduire / adapter la maîtrise des documents	94
6.3.3	Élaborer, compléter et adapter les documents de référence axés sur la base de référence du ISMS (directives, lignes directrices, instructions de travail, etc.	95
6.3.4	Établir / habilitier / adapter l'organisation de la sécurité	96
6.3.5	Impliquer tous les employés dans l'établissement d'une culture de la sécurité à l'échelle de l'entreprise	97
6.3.6	Introduire / élargir / adapter la sensibilisation et la formation	98
6.3.7	Définir l'«état souhaité» de la sécurité de l'information (définition de l' «objectif»)	98
6.3.8	Etablir un catalogue de mesures, définir les mesures à appliquer	100
6.3.9	Planifier les audits	101
6.4	Phase 4: état des lieux; détermination de l'«état réel».	102
6.4.1	Faire un inventaire détaillé.....	102
6.4.2	Identification de la chaîne d'impact.....	103
6.4.3	Déterminer les mesures mises en œuvre pour la sécurité de l'information	103
6.4.4	Audit de l'état réel: déterminer l'état réel de la sécurité de l'information	104
6.4.5	Réaliser un assessment de l'état «Actuel»	105
6.4.6	Créer un registre des risques	106
6.4.7	Déterminer un scénario de référence (baseline) pour les KPI.....	106
6.5	Phase 5: analyse de l'écart entre l'état réel et l'état souhaité; analyse des besoins de protection et des risques	107
6.5.1	Analyse de l'écart entre l'état réel et l'état souhaité	107
6.5.2	Définir le besoin de protection pour un champ d'application supplémentaire dans l'ISMS	108
6.5.3	Définir une méthodologie de gestion des risques.....	108
6.5.4	Définir les catégories et les critères de risque	109
6.5.5	Détermination des propriétaires des risques (Risk-Owner).....	109
6.5.6	Effectuer une gestion des risques	110
6.5.7	Analyse des risques sur les menaces TOP	110
6.6	Phase 6: priorisation, établissement et mise en œuvre des mesures; exploitation	111
6.6.1	Elaborer un plan de mesures à partir de l'analyse GAP ou de l'analyse des risques	111



6.6.2	Hiérarchiser les mesures	112
6.6.3	Définir les exigences et les compétences du personnel.....	113
6.6.4	Mettre en œuvre les mesures conformément à la priorisation	113
6.6.5	Mettre en œuvre des mesures de communication, de formation et de sensibilisation	114
6.6.6	Mise en œuvre continue des mesures.....	115
6.7	Phase 7: détermination de l'efficacité; mesure et contrôle	116
6.7.1	Vérifier l'efficacité des mesures mises en œuvre	116
6.7.2	Réaliser des audits internes et des audits de fournisseurs	116
6.7.3	Surveillance de l'ISMS	117
6.7.4	Traiter les indicateurs de performance (KPI)	118
6.7.5	Mettre en place un fonctionnement régulier avec monitoring et reporting	118
6.7.6	Assurer les processus de documentation	119
6.8	Phase 8: Améliorations	120
6.8.1	Correction et mesures préventives	120
6.8.2	Examen des possibilités d'amélioration.....	120
6.8.3	Maintenir un processus d'amélioration continue	121
7.	Interaction entre les documents de l'AES et les outils de l'AES	122
8.	Conclusion et résumé.....	123
Anhang A:	Annexe A: Glossaire	124
Anhang B:	Liste des abréviations	132
Anhang C:	Bases légales: lois et règlements obligatoires.....	134
C.0	Niveau national.....	134
C.1	Niveau international.....	139
Anhang D:	Institutions, cadres, normes, standards, spécifications et lignes directrices pour améliorer la résilience des TIC.....	140
D.0	Organisations et institutions	140
D.1	Frameworks.....	143
D.2	Normes et standards spécifiques importants	147
Anhang E:	Outils de l'AES pour accroître la résilience des TIC	150
E.0	Outil «VSE & BFE Assessment-Tool NIST CSF 1.1 ++» y compris SoA, maturités selon l'OFEN et aides à la mise en œuvre	150
E.0.1	Objectif et but.....	150
E.0.2	Onglet «Document Owner & History» (propriétaire et historique du document)	150
E.0.3	Onglet «Assessment NIST CSF 1.1 ++» (évaluation NIST CSF 1.1 ++)	150
E.0.4	Évaluation graphique dans les onglets «Results» (résultats).....	151
E.0.5	Onglet «Assistance Information» (informations d'assistance).....	151
E.1	VSE&BFE-Tool for NIST-CSF-1.1 Checkpoints acc.to NIST-SP800-53_CCM_CIS	152
E.1.1	Objectif et but.....	152
E.1.2	Onglet «Document Owner & History» (propriétaire et historique du document)	152
E.1.3	Onglets «All Functions» (toutes les fonctions), «IDENTIFY (ID)» (identifier), «PROTECT (PR)» (protéger), «DETECT (DE)» (détecter), «RESPOND (RE)» (répondre) et «RECOVER (RC)» (restaurer).....	152
E.1.4	Onglet «Assistance Information» (informations d'assistance).....	153
E.2	Outil AES CSF NIST 1.1 Mappage HoP	153
E.2.1	Onglet «Document Owner & History» (propriétaire et historique du document)	153
E.2.2	Onglet «All Function HoP» (toutes les fonctions HoP)	154
E.3	Outil «VSE Assessment-Tool ISO27001 Annex A incl. Controls acc.to ISO27002»	154
E.3.1	Objectif et but.....	154
E.3.2	Onglet «Document Owner & History» (propriétaire et historique du document)	154
E.3.3	Onglet «Assessment Tool ISO 27001» (outil d'évaluation ISO 27001).....	155
E.3.4	Évaluation graphique dans l'onglet «Graphics All Area» (graphiques de toutes les zones).....	155
E.3.5	Onglet «Assistance Information» (informations d'assistance).....	156
E.4	Outil «VSE Assessment-Tool ISO27001 ISMS-Goals incl. HoP-Mapping»	156
E.4.1	Objectif et but.....	156



E.4.2	Onglet «Document Owner & History» (propriétaire et historique du document)	156
E.4.3	Onglet «Assessment ISMS Goals» (évaluation des objectifs de l'ISMS)	156
E.4.4	Évaluation graphique dans l'onglet «Graphics ISMS Goals» (graphiques des objectifs de l'ISMS)	157
E.4.5	Onglet «Assistance Information» (informations d'assistance)	158
E.5	Outil «VSE-Tool ISO27001 Annex A HoP-Mapping»	158
E.5.1	Onglet «Document Owner & History» (propriétaire et historique du document)	158
E.5.2	Onglet «All Function HoP» (toutes les fonctions HoP)	158
E.6	Outil AES IMS Répertoire de documents HoP	158
Anhang F:	Description des prescriptions de la Maison des politiques Niveau 0 à 3	159
F.0	Maison des politiques au niveau 0: politique (conseil d'administration / direction du groupe)	159
F.1	Maison des politiques au niveau 1: instructions et directives (direction, niveau C)	159
F.2	Maison des politiques au niveau 2: directives et lignes directrices (CISO, CRO, DPO)	160
F.3	Maison des politiques au niveau 3: guides de travail et instructions (ISO, ISC et équipe de cybersécurité)	162
Anhang G:	Littérature complémentaire	172

Liste des figures

Figure 1:	le chemin vers l'objectif (source OFEN)	11
Illustration 2:	Top 10 des risques commerciaux dans le monde en 2022 selon Allianz (source Allianz)	12
Illustration 3:	Ensemble de règles de l'AES pour la branche électrique visant à augmenter la résilience des TIC (source AES)	19
Figure 4:	Augmentation de la cybersécurité (source BWL)	26
Figure 5:	Extrait de l'outil d'évaluation de la norme minimale TIC de l'OFAE (source OFAE)	27
Figure 6:	OFAE Standard minimal TIC Maturités (source OFAE)	28
Figure 7:	Schéma de déroulement de la mise en œuvre des exigences minimales de cybersécurité (source ECom)	32
Figure 8:	Système de gestion intégré SGI (Source TÜV Süd)	37
Figure 9:	Les éléments nécessaires pour réussir à augmenter la résilience des TIC (source AES)	46
Figure 10:	SGI (source TÜV NORD)	47
Figure 11:	Cycle de Deming PDCA (source AES)	48
Figure 12:	Responsabilité (source weka.ch)	51
Figure 13:	Responsabilité (source meinekrankenkasse.de)	52
Figure 14:	Structure de principe d'un organigramme de sécurité possible (source AES)	54
Figure 15:	Structure dans la Maison du processus (source AES)	62
Figure 16:	Processus dans la Maison des processus (source AES)	64
Figure 17:	Structure de principe de la Maison des politiques avec le mapping vers le CSF NIST 1.1 (source AES)	66
Figure 18:	Objectifs et preuves avec transition fluide (source AES)	67
Figure 19:	Documents de la Maison de la politique aux niveaux 0 à 3 (source AES)	68
Figure 20:	Spirale de maturité de l'ISMS	72
Figure 21:	Phases de l'AES pour la mise en place de l'ISMS (source AES)	73
Illustration 22:	Cadre de cybersécurité du NIST	74
Figure 23:	Mise en réseau ISMS avec CSF NIST	74
Figure 24:	Collaboration (source allegra Blog)	75
Figure 25:	Circuit détaillé des huit phases de l'AES pour la mise en place et l'exploitation de l'ISMS (source AES)	79
Figure 26:	Processus dans les entreprises et les unités organisationnelles (source AES)	84
Figure 27:	Détermination du point focal selon l'OApEI (source AES)	85
Figure 28:	Interaction des documents de l'AES avec les outils de l'AES pour augmenter la résilience des TIC (source AES)	122



Liste des tableaux

Tableau 1: Parties prenantes au niveau fédéral (source AES)	20
Tableau 2: Définition des profils d'entreprises selon l'OApEI (source OFEN/AES)	30
Tableau 3: Responsabilités selon RASCI (source AES)	53
Tableau 4: Responsabilités et compétences dans la Maison des processus (source AES)	65
Tableau 5: Responsabilités et compétences au sein de la Maison des politiques (source AES)	67
Tableau 6: Mapping Maison des politiques avec les niveaux dans le CSF NIST 1.1	69
Tableau 7: Phase 1 ISMS: base et planification; décision d'adopter un ISMS; définition des objectifs	80
Tableau 8: Phase 2 ISMS: direction et initialisation; état des lieux	88
Tableau 9: Phase 3 ISMS: planification de la mise en place et du déroulement; sensibilisation et formation; définition de l'«état souhaité».	93
Tableau 10: Phase 4 ISMS: état des lieux; détermination de l'«état réel».	102
Tableau 11: Phase 5 ISMS: analyse de l'écart entre l'état réel et l'état souhaité; analyse des besoins de protection et analyse des risques	107
Tableau 12: Phase 6 ISMS: priorisation, établissement et mise en œuvre des mesures; exploitation	111
Tableau 13: Phase 7 ISMS: détermination de l'efficacité; mesure et contrôle	116
Tableau 14: Phase 8 ISMS: Améliorations	120



Préface

Le présent document est un document de la branche publié par l'AES. Il fait partie d'une large réglementation relative à l'approvisionnement en électricité sur le marché ouvert de l'électricité. Les documents de la branche contiennent des directives et des recommandations reconnues à l'échelle de la branche concernant l'exploitation des marchés de l'électricité et l'organisation du négoce de l'énergie, répondant ainsi à la prescription donnée aux entreprises d'approvisionnement en électricité (EAE) par la loi sur l'approvisionnement en électricité (LApEI) et par l'ordonnance sur l'approvisionnement en électricité (OApEI).

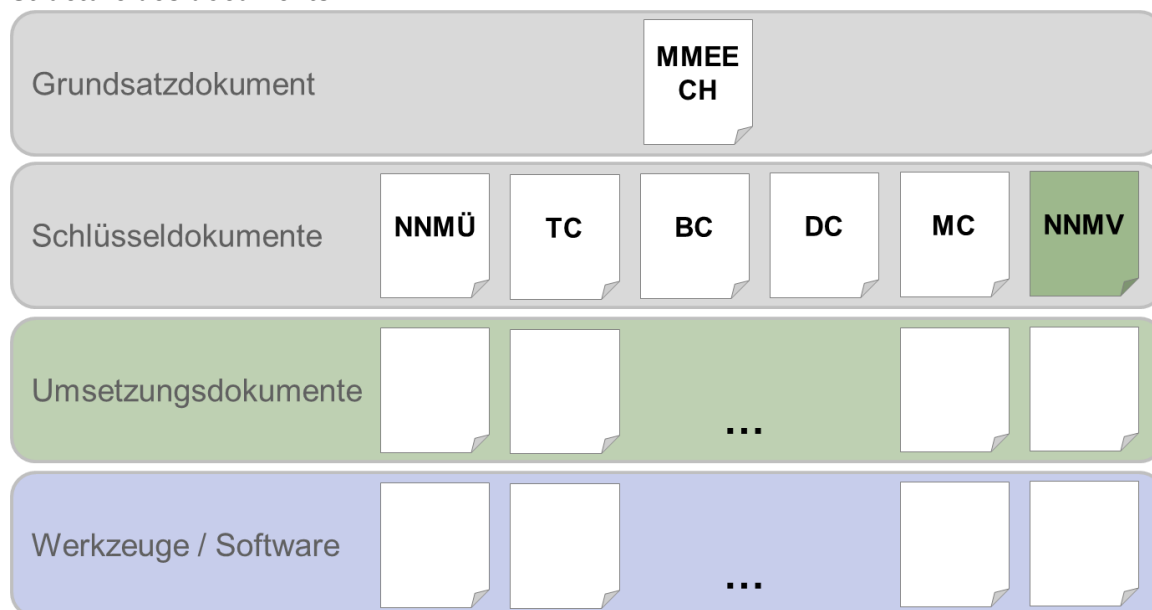
Les documents de la branche sont élaborés par des spécialistes de la branche selon le principe de subsidiarité; ils sont régulièrement mis à jour et complétés. Les dispositions qui ont valeur de directives au sens de l'OApEI sont des normes d'autorégulation.

Les documents sont répartis en quatre catégories hiérarchisées:

- Document principal
- Documents clés
- Documents d'application: Guide pour accroître la résilience des TIC dans le secteur de l'électricité
- Outils / Logiciels

Le présent document «Guide pour accroître la résilience des TIC dans le secteur de l'électricité» est un document d'application.

Structure des documents



Introduction

- (1) Dans le monde numérique d'aujourd'hui, les technologies de l'information et de la communication (TIC) sont essentielles au bon fonctionnement des entreprises, des unités organisationnelles et des institutions de toutes sortes. Bien que les progrès technologiques nous offrent de nombreux avantages et opportunités, nous sommes également de plus en plus exposés aux défis et aux risques inhérents à un environnement numérique et hautement connecté. Les perturbations des TIC, les cyber-attaques, les catastrophes naturelles et les erreurs humaines peuvent mettre en péril le fonctionnement des systèmes et des services TIC et avoir de graves répercussions sur les entreprises et les entités organisationnelles.
- (2) La nécessité de rendre nos systèmes TIC plus résistants à ces menaces est donc au cœur de nos préoccupations. Ce guide sur l'amélioration de la résilience des TIC a été conçu pour aider les entreprises et les unités organisationnelles à renforcer leur capacité à réagir et à se remettre d'une perturbation ou d'une catastrophe liée aux TIC. L'augmentation de la résilience des TIC n'est pas seulement une question de continuité des activités, mais aussi de sécurité des informations, de protection des données et de protection de la réputation d'une organisation.
- (3) Dans ce guide, nous allons vous présenter les bonnes pratiques et une approche systématique qui vous aideront à accroître votre résilience en matière de TIC. Nous aborderons la création d'une culture de la sécurité, l'identification des ressources critiques, l'élaboration de plans d'urgence, la formation du personnel et l'amélioration continue. Ce guide est conçu pour les dirigeants, les responsables de la cybersécurité, les responsables IT/OT, les responsables de la sécurité et tous les employés qui ont un rôle à jouer dans la garantie de la résilience des TIC.
- (4) L'augmentation de la résilience des TIC n'est pas une mesure optionnelle, mais un engagement indispensable envers votre organisation, vos clients et vos partenaires. Elle garantit que vous êtes en mesure de faire face de manière souveraine aux défis inattendus du monde numérique et de maintenir l'activité, même si les circonstances rendent cela difficile. Nous vous invitons à utiliser ce guide comme un outil pour renforcer votre résilience en matière de TIC et rendre votre organisation plus résistante et mieux préparée.

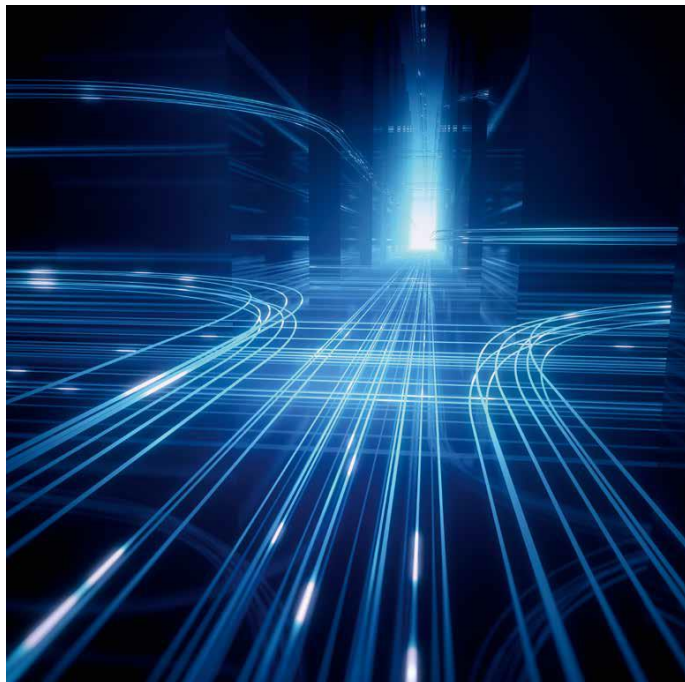


Figure 1: le chemin vers l'objectif (source OFEN)

Ce guide décrit explicitement

«La voie à suivre»

et donc la procédure à suivre pour augmenter la résilience des TIC. Il n'est volontairement pas question de mesures explicites concernant les environnements, les systèmes ou les réseaux.



1. Contexte

- (1) Dans une ère marquée par le développement rapide des technologies de l'information et de la communication (TIC), les entreprises et les unités organisationnelles sont confrontées à des opportunités et des défis sans précédent. Les TIC constituent l'épine dorsale de notre monde moderne et sont un élément clé de presque toutes les activités commerciales. L'interconnexion des systèmes, le transfert des services vers le cloud et la dépendance aux données numériques ont révolutionné les activités commerciales et amélioré l'efficacité. Mais en même temps, ils ont créé une vulnérabilité accrue aux perturbations et aux cyber-attaques, qui peuvent mettre en péril les activités commerciales et causer des dommages considérables.
- (2) La situation de départ est marquée par de multiples risques, notamment
- **Les cyber-attaques:** la menace de piratage, de logiciels malveillants et d'autres cyberattaques est présente en permanence. Ces attaques peuvent paralyser toute une entreprise et des unités organisationnelles, provoquer des pertes de données et mettre en péril la confiance des clients et des partenaires.
 - **Les catastrophes naturelles:** les inondations, les tremblements de terre, les tempêtes et autres catastrophes naturelles peuvent causer des dommages physiques aux infrastructures TIC et entraîner des temps d'arrêt importants.
 - **L'erreur humaine:** même les erreurs humaines, qu'il s'agisse d'employés négligents ou d'une mauvaise manipulation des technologies, peuvent entraîner des dysfonctionnements critiques des TIC.
 - **La dépendance à l'égard de fournisseurs tiers:** l'externalisation de services et la dépendance à l'égard de fournisseurs tiers augmentent le risque de pannes et accroissent les exigences en matière de gestion de la chaîne d'approvisionnement.
 - **Les exigences légales et réglementaires:** les gouvernements et les autorités de surveillance édictent constamment de nouvelles lois et réglementations qui obligent les entreprises et les unités organisationnelles à respecter certaines normes de sécurité et exigences en matière de protection des données.

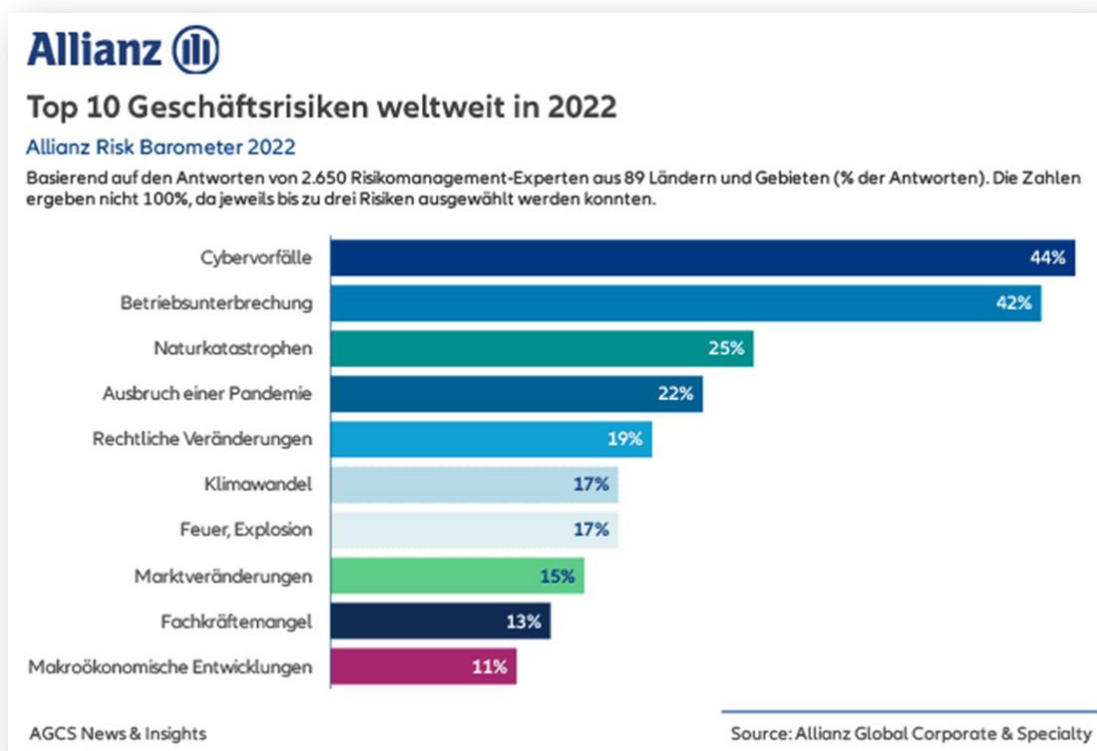


Illustration 2: Top 10 des risques commerciaux dans le monde en 2022 selon Allianz (source Allianz)



- (3) Face à ces risques et aux inévitables incertitudes auxquelles sont confrontées les entreprises et les unités organisationnelles, il est essentiel d'accroître la résilience des TIC. Cela signifie renforcer la capacité à réagir aux perturbations ou aux catastrophes et à maintenir un fonctionnement normal. Une stratégie de résilience TIC efficace peut faire la différence entre une panne temporaire et un dommage à long terme pour l'organisation.
- (4) L'augmentation de la résilience des TIC n'est pas seulement une mesure de prudence, mais une nécessité stratégique dans le monde numérique actuel. Ce guide a été conçu pour aider les entreprises et les unités organisationnelles à atteindre ces objectifs en leur fournissant les outils et les connaissances nécessaires pour devenir plus résistantes aux défis du paysage numérique et pour les gérer de manière proactive.

1.1 Objectif, but et portée

- (1) Le guide sur l'amélioration de la résilience des TIC (résilience des technologies de l'information et de la communication) a pour objectif général de montrer l'approche systématique à adopter pour renforcer la capacité d'une entreprise et de ses unités organisationnelles à réagir et à se remettre d'une perturbation ou d'une catastrophe liée aux TIC. La résilience des TIC comprend la capacité de maintenir ou de rétablir rapidement le fonctionnement des systèmes et services informatiques, même en cas d'événements inattendus. Voici les objectifs poursuivis par ce guide:
- **Assurer la continuité:** la résilience des TIC doit garantir que l'organisation peut maintenir le fonctionnement continu de ses systèmes et services informatiques/OT en période de perturbations, de cyberattaques, de catastrophes naturelles ou d'autres événements inattendus.
 - **Réduction des risques:** la mise en œuvre de bonnes pratiques et de mesures de sécurité relatives à la résilience des TIC doit permettre de minimiser le risque de panne informatique ou de perte de données. Cela contribue à la sécurité et à l'intégrité des informations.
 - **Améliorer la capacité de réaction:** l'organisation devrait être en mesure de réagir rapidement aux perturbations des TIC et de prendre des contre-mesures afin de maintenir le fonctionnement. Cela inclut des plans et des procédures d'urgence clairs.
 - **Assurer la capacité de récupération:** même si des perturbations ou des catastrophes surviennent, l'organisation doit être en mesure de récupérer rapidement ses systèmes et services TIC et de reprendre ses activités normales le plus rapidement possible.
 - **Respecter la conformité et la réglementation:** les politiques de résilience des TIC doivent garantir que l'organisation respecte toutes les exigences légales pertinentes et les normes du secteur en matière de sécurité et de protection des données.
 - **Faire prendre conscience de la situation:** ce guide sur l'amélioration de la résilience des TIC vise à sensibiliser l'ensemble de l'organisation à l'importance de la résilience des TIC et aux responsabilités de tous les employés à cet égard.
 - **Amélioration continue:** ce guide a pour but de montrer la nécessité de surveiller, d'évaluer et d'améliorer en permanence la résilience des TIC. Cela implique de s'adapter à l'évolution des menaces et des exigences.
 - **Minimiser les temps d'arrêt:** l'objectif est de réduire au maximum les temps d'arrêt afin de maintenir la productivité de l'organisation et de limiter les dommages financiers que peuvent causer les pannes IT/OT.
 - **Protection des données et des informations:** la résilience des TIC doit garantir que les données et les informations sont protégées et disponibles dans toutes les situations.
 - **Communication et coopération:** la directive vise à établir des mécanismes clairs de communication et de coordination afin de garantir une coopération efficace dans la gestion des incidents liés aux TIC.
 - **Efficacité des ressources:** les lignes directrices devraient garantir que les ressources destinées à améliorer la résilience des TIC sont utilisées de manière efficace tout en restant effectives.
- (2) L'augmentation systématique de la résilience des TIC selon ce guide est essentielle pour garantir que les entreprises et les unités organisationnelles soient préparées et puissent réagir efficacement aux défis



inattendus liés aux technologies de l'information et de la communication. Les objectifs précis peuvent varier en fonction des besoins et des risques spécifiques des entreprises et des unités organisationnelles.

- (3) Le guide a pour but de montrer aux entreprises et aux unités organisationnelles une approche systématique pour augmenter la résilience des TIC. Il se base sur l'ensemble de l'environnement d'une entreprise d'approvisionnement en électricité en rapport avec la résilience TIC afin de créer une compréhension commune. Il doit aider les entreprises et les unités organisationnelles à développer et à mettre en œuvre des stratégies et des mesures afin d'augmenter durablement leur résilience TIC. Il doit en outre renforcer leur capacité à réagir de manière appropriée aux cyberattaques et aux dysfonctionnements ou catastrophes TIC qui en résultent, et à s'en remettre.
- (4) Pour renforcer la résilience des TIC, la portée peut varier en fonction des exigences et des risques spécifiques à l'entreprise et aux unités organisationnelles. Ce guide complet sur le renforcement de la résilience des TIC propose une feuille de route claire et une stratégie globale.
- (5) **«Ce guide décrit la voie à suivre.» Ce document a pour but d'introduire le sujet, de créer une compréhension commune, de présenter et de décrire les principes de base, de présenter et de décrire les directives et de mettre en lumière la procédure à suivre pour accroître la résilience des TIC. Ce guide a été conçu de la manière la plus vaste possible pour répondre à tous les besoins des parties prenantes. Les éléments importants sont répétés pour éviter les renvois confus.**

1.2 Public cible

- (1) Le public cible pour l'augmentation de la résilience TIC (résilience des technologies de l'information et de la communication) comprend un large éventail d'acteurs au sein d'une organisation. Les principaux groupes cibles concernés par les mesures d'amélioration de la résilience des TIC sont décrits ci-dessous:
 - **Leadership et direction:** il s'agit des décideurs les plus hauts placés dans l'organisation. Ils doivent encourager l'engagement en faveur de la résilience des TIC, fournir des ressources et donner une orientation à l'ensemble de l'organisation.
 - **Département IT/OT et experts technologiques:** le département IT/OT et les experts techniques jouent un rôle clé dans la mise en œuvre des mesures de résilience des TIC. Ils sont responsables de la planification, de la mise en œuvre et du suivi des mesures de sécurité TIC.
 - **Responsables de la sécurité et de la conformité:** ce groupe est responsable de la conformité aux exigences légales et aux normes de sécurité. Ils veillent à ce que la résilience des TIC soit conforme aux exigences légales.
 - **Experts en gestion des risques et en conformité:** ils identifient et évaluent les risques liés aux TIC et aident à développer des stratégies d'atténuation des risques.
 - **Employés:** tous les employés de l'organisation ont un rôle à jouer dans la résilience des TIC. Ils doivent respecter les politiques et les procédures de sécurité et contribuer à vivre et à promouvoir un comportement conscient de la sécurité.
 - **Prestataires de services et fournisseurs externes:** les entreprises et les unités organisationnelles qui fournissent des services ou des composants technologiques externes sont également pertinentes, car elles doivent être impliquées dans le processus de résilience des TIC.
 - **Les auditeurs et contrôleurs internes et externes:** les auditeurs internes et externes ont un rôle à jouer dans l'examen et l'évaluation de la résilience des TIC afin de s'assurer que l'organisation respecte les pratiques et les normes appropriées.
 - **Clients et partenaires:** la résilience des TIC peut avoir un impact sur les clients et les partenaires commerciaux. Il est donc important d'informer ces groupes des changements prévus ou des plans d'urgence.
 - **Autorités et organismes de réglementation:** dans certains secteurs, les entreprises et les unités organisationnelles sont soumises à des exigences légales et à des réglementations spécifiques en matière de résilience des TIC. Les organismes publics peuvent jouer le rôle d'auditeurs pour contrôler et faire respecter les exigences légales.



- **Équipes de gestion et d'intervention d'urgence:** ces équipes sont responsables de la gestion des perturbations et des crises TIC. Elles doivent être impliquées dans les stratégies et les plans de résilience des TIC.
- (2) Le public cible pour l'augmentation de la résilience des TIC est varié et comprend différents départements, niveaux et parties prenantes au sein et en dehors de l'organisation. La participation et la collaboration de ces groupes sont essentielles pour rendre la résilience des TIC efficace et garantir que l'organisation est en mesure de réagir de manière appropriée aux perturbations et aux catastrophes informatiques/OT.

1.3 Structure du document

- (1) Une approche pragmatique a été adoptée pour la structure ou l'organisation du document et le guide est structuré comme suit:
- Introduction à la thématique
 - Créer une compréhension commune
 - Principes et objectifs pour accroître la résilience des TIC
 - Procédure pour augmenter la résilience des TIC

1.4 Conseils, remarques, invitations et informations

- (1) Le guide contient des champs d'information à travers lesquels les auteurs donnent au lecteur des conseils, des remarques, des recommandations ou des informations supplémentaires qui sont essentiels pour une mise en œuvre réussie du guide. Les champs d'information sont décrits ci-dessous:



Recommandation des experts de la Task Force Cyber Security de l'AES:
Ces points aident l'utilisateur pour une augmentation systématique et efficace de la résilience des TIC du point de vue des experts de la Task Force Cyber Security de l'AES



Voici un outil de l'AES qui devrait être utilisé



Les annexes contiennent des exemples qui peuvent être appliqués.



Références à des documents complémentaires



Bases et directives légales et réglementaires qui doivent impérativement être respectées



Informations supplémentaires pour t'aider



Directives et indications à respecter



Directives et indications qui doivent être impérativement respectées et remplies



2. Introduction

- (1) Le guide sur l'amélioration de la résilience des TIC sert de manuel complet pour aider les entreprises et les unités organisationnelles à renforcer leurs technologies de l'information et de la communication face à de multiples menaces. L'accent est mis sur une stratégie proactive de gestion des risques, l'intégration des meilleures pratiques en matière de sécurité de l'information et la création d'une culture de résilience organisationnelle. Le guide fournit des directives, des outils et des formations clairs pour améliorer la résilience systématique de l'infrastructure TIC et répondre efficacement au paysage dynamique des menaces. D'une manière générale, le guide a pour objectif de garantir les objectifs de protection de la confidentialité, de l'intégrité et de la disponibilité (triade CIA), qui constituent le fondement de la sécurité de l'information. La confidentialité garantit que les informations sensibles ne sont accessibles qu'aux personnes autorisées, en contrôlant l'accès et la transmission. L'intégrité garantit l'exactitude et l'exhaustivité des données et des systèmes en empêchant ou en détectant les manipulations ou les modifications indésirables. La disponibilité garantit que les utilisateurs autorisés peuvent accéder à tout moment aux informations et aux ressources, sans être gênés par des pannes ou des attaques. Ces trois objectifs constituent la base d'objectifs de protection étendus tels que la traçabilité, l'autorisation et l'authentification, en ce qui concerne l'origine et le destinataire en cas de communication. La prise en compte de ces objectifs étendus permet de développer une stratégie de sécurité globale qui s'adresse à l'ensemble des menaces et garantit la confidentialité, l'intégrité et la disponibilité des informations et des systèmes.

2.1 Amélioration continue de la résilience des TIC

- (1) L'amélioration continue de la résilience des TIC (technologies de l'information et de la communication) est un processus par lequel une organisation s'efforce en permanence de renforcer sa capacité à réagir et à se rétablir en cas de perturbation ou de catastrophe liée aux TIC. Ce processus vise à augmenter continuellement la résilience de l'infrastructure informatique et des ressources technologiques d'une organisation. Voici une description de l'amélioration continue de la résilience des TIC:
 - **Objectif et finalité:** l'amélioration continue de la résilience des TIC a pour objectif global de rendre l'organisation plus résistante aux perturbations et aux catastrophes liées aux TIC. Cela signifie renforcer la capacité à maintenir le fonctionnement normal ou à le rétablir aussi rapidement que possible, même si des événements inattendus se produisent.
 - **Examen systématique:** l'organisation procède à des examens et des évaluations réguliers de ses pratiques de résilience TIC. Cela peut inclure des audits internes, des évaluations des risques et des examens externes. L'objectif est d'identifier les points faibles et les possibilités d'amélioration.
 - **S'adapter aux changements:** l'amélioration continue tient compte de l'évolution du paysage informatique, des développements technologiques et de l'évolution des menaces. L'organisation adapte ses stratégies de résilience TIC afin d'être prête à relever de nouveaux défis.
 - **Apprendre de ses échecs:** chaque événement, qu'il s'agisse d'une panne informatique, d'un incident de sécurité ou d'une catastrophe naturelle, offre des possibilités d'apprentissage. L'organisation tire les leçons de ces expériences et adapte ses stratégies de résilience en conséquence.
 - **Mise en œuvre des meilleures pratiques:** l'amélioration continue s'appuie sur les bonnes pratiques et les normes en matière de résilience des TIC, telles que ISO 27031 ou ISO 22301. Ces pratiques servent de guide pour la mise en œuvre.
 - **Implication de toutes les parties prenantes:** l'amélioration continue requiert la participation active et l'engagement de tous les acteurs concernés de l'organisation, y compris la direction, les experts en informatique, les responsables de la sécurité et les employés.
 - **Identification des ressources critiques:** l'organisation identifie et classe les ressources et les données informatiques critiques afin de s'assurer que des mesures de protection et de récupération appropriées sont mises en œuvre.
 - **Élaboration de plans d'urgence:** dans le cadre de l'amélioration continue, des plans et des procédures d'urgence détaillés sont élaborés et entrent en vigueur en cas de dysfonctionnement des TIC ou de catastrophe.
 - **Formation et sensibilisation:** l'organisation forme son personnel et le sensibilise à la résilience des TIC afin de s'assurer que les employés sont en mesure de mettre en œuvre des pratiques sûres et résilientes dans leur environnement de travail quotidien.



- **Révision et mise à jour régulières:** les stratégies et les plans de résilience des TIC sont régulièrement révisés et mis à jour pour s'assurer qu'ils répondent aux exigences et aux menaces actuelles.
- (2) L'amélioration continue de la résilience des TIC est un processus répétitif qui garantit qu'une organisation reste flexible et résiliente pour faire face efficacement aux défis liés aux technologies de l'information et de la communication. Il s'agit d'une approche dynamique visant à assurer la continuité des activités et à minimiser les dommages causés par les perturbations des TIC.

2.2 Délimitation

- (1) Ce guide se concentre sur les processus d'entreprise qui ont une influence directe sur la régulation et la commande sûres des réseaux électriques ainsi que sur la production et le stockage d'électricité. En raison de l'obligation du standard minimal TIC pour l'augmentation de la résilience TIC dans l'OApEI, les directives légales doivent être mises en œuvre et respectées avec une attention particulière. Les définitions et points de délimitation suivants définissent la portée de ce guide:
- La sécurité des TIC pour les infrastructures critiques englobe tous les actifs TIC nécessaires à une exploitation sûre et intégrée du réseau dans le domaine de l'électricité, à une production sûre d'électricité et à un stockage sûr de l'électricité, ou qui interagissent directement avec de tels systèmes.
 - Les modalités pour les entreprises et les unités organisationnelles sont définies dans l'OApEI avec les niveaux de protection correspondants.
 - La sécurité de l'informatique bureautique et de l'informatique de gestion n'est pas au centre du document. Toutefois, des exigences sont posées en ce qui concerne les interfaces et l'échange d'informations avec les domaines contenant les actifs TIC critiques.
 - La sécurité électrique et opérationnelle des équipements du réseau électrique ne fait pas partie de ce guide.
 - Les mesures de sécurité au travail ne font pas partie de ce guide. Les dispositions de l'ordonnance sur le courant fort s'appliquent à cet égard.
 - Il s'agit de mettre en œuvre une approche à l'échelle du secteur pour accroître la résilience des TIC, qui servira de base à un niveau de sécurité accru.
 - Les centrales nucléaires ne sont pas soumises aux prescriptions de l'OApEI, elles sont soumises aux prescriptions de l'IFSN et de l'AIEA (Agence internationale de l'énergie atomique).

2.3 Contexte

- (1) Au cours des 15 dernières années, les technologies de l'énergie ont fortement évolué vers des systèmes informatiques ou TIC. Cette évolution technologique permet de centraliser la commande et la régulation des informations en temps réel. On devient ainsi beaucoup plus agile dans la gestion du réseau et on peut réagir en temps réel et de manière automatisée à des événements critiques. Mais cette évolution vers les technologies de l'information entraîne également de nouveaux risques que les entreprises énergétiques doivent reconnaître, évaluer et traiter afin de pouvoir remplir leur mission légale conformément à la loi sur l'approvisionnement en électricité, à l'ordonnance sur l'approvisionnement en électricité ou à la loi sur l'énergie.
- (2) Le secteur de l'énergie est de plus en plus soutenu par des composants IT/OT. Cela se produit au sein de l'organisation, des activités administratives aux éléments de commutation dans une sous-station, en passant par les modèles de calcul pour le flux d'électricité. Bien que la mise en réseau ne se soit pas encore complètement imposée, elle sera inévitable à plus ou moins long terme. Aujourd'hui déjà, les commutations dans les sous-stations ne sont généralement plus effectuées localement, mais de manière centralisée à partir d'un centre de contrôle. Outre les commutations, le centre peut surveiller entièrement une sous-station à distance et lire les valeurs de mesure des flux de courant en temps réel.
- (3) De même, la production locale d'électricité par des installations photovoltaïques et éoliennes entraîne une mise en réseau de plus en plus importante. Comme chaque exploitant d'une installation correspondante peut être raccordé au réseau d'un producteur d'électricité, il en résulte un réseau énergétique national d'une grande complexité. De même, ces producteurs sont reliés entre eux par des processus commerciaux et des interfaces.
- (4) L'intégration rapide des technologies informatiques à évolution rapide conduit à une collision entre deux mondes. Étant donné que de nombreux composants ont été construits dans l'optique d'une longévité



maximale, certains éléments SCADA ont été construits à une époque où les fabricants ne se concentraient pas encore sur la cybersécurité. De même, la plupart des spécialistes n'ont pas été formés en tenant compte des risques actuels. Il en résulte le défi d'intégrer des concepts de sécurité et des technologies toujours plus récents dans un environnement plus ou moins statique.

2.4 Menaces et risques

- (1) L'Office fédéral de la protection de la population (OFPP) a effectué une analyse des risques et de la vulnérabilité du sous-secteur de l'approvisionnement en électricité et en a tiré les conclusions suivantes:
- Tout au long de la chaîne d'approvisionnement, la production d'électricité dans les centrales est aujourd'hui moins vulnérable aux risques liés aux TIC que l'exploitation des réseaux de distribution et de transport.
 - En théorie, les centrales et sous-centrales peuvent toujours être exploitées sur place. Mais en cas de panne à grande échelle, les entreprises d'approvisionnement en énergie ne seraient plus guère en mesure d'occuper assez rapidement toutes les installations critiques avec suffisamment de personnel.
 - Si la menace concerne les prestataires de services TIC des entreprises d'approvisionnement en énergie, la communication entre les installations et les centres de contrôle ne pourrait éventuellement être maintenue que par des systèmes de communication d'urgence.
 - L'exploitation des réseaux à très haute, haute et moyenne tension est aujourd'hui centralisée et est en grande partie surveillée et commandée par des systèmes numériques. L'exploitation des réseaux est donc plus vulnérable aux menaces TIC que la production d'électricité proprement dite. Dans ce domaine, les systèmes SCADA revêtent une importance particulière.
 - Le risque que des employés fassent des erreurs de manipulation, intentionnelles ou non, sur les systèmes SCADA est donc également significatif et augmente encore en raison du processus de centralisation dans les centres de contrôle.
 - Avec l'installation de systèmes de mesure intelligent et d'appareils «smart grid», le réseau suisse de conduites devient un réseau composé d'une multitude de petits ordinateurs. Cela offre des avantages en termes d'efficacité pour l'exploitation des réseaux de lignes, mais crée de nouvelles vulnérabilités aux TIC.
 - Dans l'ensemble, la vulnérabilité de l'approvisionnement en électricité aux TIC va continuer à augmenter à l'avenir.



3. Environnement Alimentation électrique pour accroître la résilience des TIC

3.1 Règles de l'AES pour le secteur de l'électricité visant à accroître la résilience des TIC

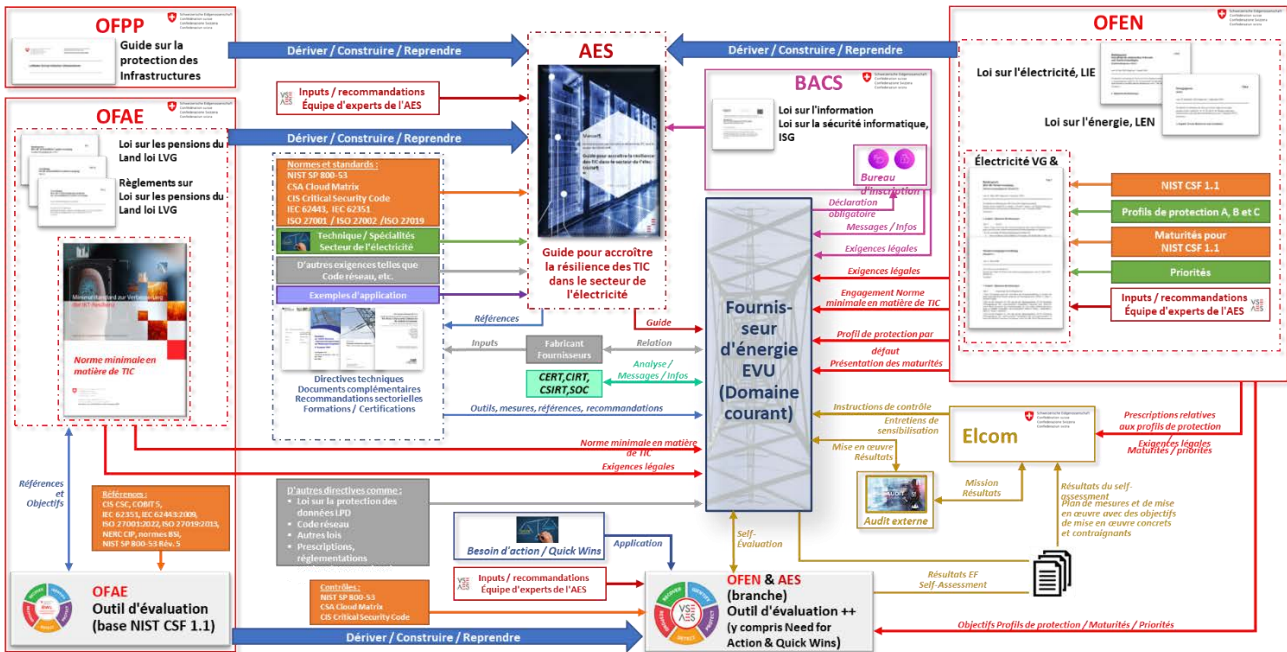


Illustration 3: Ensemble de règles de l'AES pour la branche électrique visant à augmenter la résilience des TIC (source AES)

(1) Le règlement de l'AES pour la branche électrique visant à augmenter la résilience des TIC présente tous les éléments importants nécessaires à une mise en œuvre complète. Les différents éléments et leur interaction sont décrits et mis en lumière ci-après.

3.2 Acteurs / parties prenantes

3.2.1 Parties prenantes au niveau fédéral

(1) Les organismes suivants au niveau fédéral sont impliqués dans ce guide sur l'augmentation de la résilience des TIC:

Office fédéral	Brève description
Office fédéral de la protection de la population (OFPP)	L'Office fédéral de la protection de la population (OFPP) est l'autorité fédérale suisse responsable de la planification et de la coordination des mesures dans le domaine de la sécurité civile et de la protection de la population.
Office fédéral pour l'approvisionnement économique du pays (OFAE)	L'Office fédéral pour l'approvisionnement économique du pays (OFAE) est l'autorité fédérale suisse responsable de la garantie de l'approvisionnement économique du pays dans les situations d'urgence. En établissant la norme minimale en matière de TIC, l'OFAE a joué un rôle décisif dans la définition de l'approche et du cadre permettant d'accroître la résilience des TIC dans les installations critiques pour l'approvisionnement.
Office fédéral de l'énergie (OFEN)	L'Office fédéral de l'énergie (OFEN) est l'autorité fédérale responsable de la politique et de la réglementation énergétiques en Suisse, ainsi que de la promotion de l'utilisation durable de l'énergie. Dans le cadre de l'OApEI, l'OFEN définit les exigences minimales légalement obligatoires pour augmenter la résilience des TIC au niveau fédéral.
Commission fédérale de l'électricité (ElCom)	La Commission fédérale de l'électricité (ElCom) est l'autorité suisse de régulation du marché de l'électricité. Elle surveille l'approvisionnement en électricité, les tarifs et l'accès au réseau en Suisse. Dans le cadre des dispositions légales visant à renforcer la cyber-résilience, l'ElCom vérifie et contrôle le respect des prescriptions légales.

Office fédéral	Brève description
Office fédéral de la cybersécurité (OFCS)	L'Office fédéral de la cybersécurité (BACS) est l'autorité suisse compétente en matière de cybersécurité nationale. Il est responsable de la coordination des mesures visant à contrer les cybermenaces et à améliorer la sécurité des TIC. Avec la nouvelle loi sur la sécurité de l'information (LSI) en Suisse, il existe une obligation légale de signaler les incidents liés à la cybersécurité à l'OFCS. L'obligation de notification sera introduite lors de la 1 ^{re} révision de la LSI.

Tableau 1: Parties prenantes au niveau fédéral (source AES)

3.2.2 L'Association des entreprises électriques suisses (AES)



(1) L'AES est l'association faîtière de la branche électrique suisse, reconnue au niveau national et international. Elle coordonne et regroupe les intérêts communs et les compétences de ses membres et les représente auprès des milieux politiques, économiques et sociaux. Elle veille ainsi à la mise en place de conditions-cadres fiables pour un approvisionnement en électricité sûr, compétitif sur le marché et durable en Suisse. Ses plus de 400 membres sont répartis sur toute la chaîne de création de valeur (producteurs, gestionnaires de réseau de distribution, entreprises d'interconnexion) et produisent plus de 90 % de l'électricité suisse.

Groupe d'experts de l'AES



(1) Divers groupes de travail sont actifs au sein de l'AES pour traiter les différents thèmes dans le domaine de l'électricité. Des représentants des différents domaines de la branche électrique participent à ces groupes de travail. Un groupe de travail spécial a été créé pour le domaine de la cybersécurité, qui se consacre à tous les thèmes relatifs à la cybersécurité dans la branche électrique. Une équipe d'experts de ce groupe de travail se penche sur le thème «Augmentation de la résilience des TIC dans le secteur de l'électricité».

3.2.3 Entreprise d'approvisionnement en électricité EAE (domaine électrique)



(1) Une entreprise d'approvisionnement en électricité, également appelée fournisseur d'électricité ou entreprise électrique, est une entreprise et une unité organisationnelle qui assure la production, le stockage, le transport et la distribution d'énergie électrique à des clients privés, commerciaux et industriels.

(2) L'économie nationale ne fonctionne pas sans électricité, de sorte que les entreprises d'approvisionnement en électricité sont considérées d'importance systémique. Les réseaux électriques, les centrales électriques et leurs installations de stockage dont le délestage entraîne une menace ou une perturbation importante de la sécurité et de la fiabilité énergétiques du système d'approvisionnement en électricité sont considérés comme d'importance systémique et leurs propriétaires sont tenus par la Confédération de poursuivre leur exploitation.

3.2.4 CERT, CIRT, CSIRT et SOC

(1) CIRT, CERT, CSIRT et SOC sont des termes utilisés dans le monde de la cybersécurité pour décrire différents types d'équipes et d'entités visant à identifier et à gérer les incidents de sécurité. En résumé, CIRT, CERT et CSIRT sont principalement axés sur la réaction aux incidents de sécurité, tandis qu'un SOC vise à surveiller et à protéger l'infrastructure TIC de manière proactive. Le choix de l'approche la plus appropriée dans une organisation dépend des besoins, des objectifs et des risques spécifiques de l'organisation. Toutefois, il arrive souvent que ces équipes travaillent ensemble pour assurer une stratégie de cybersécurité globale.

CERT

(2) Une **Computer Emergency Response Team** (CERT ou équipe d'intervention en cas d'urgence informatique) est une organisation ou un groupe d'experts spécialisés dans la détection, l'évaluation et la réponse aux incidents de cybersécurité. Les CERT visent à renforcer la sécurité des systèmes informatiques et des réseaux, à identifier les menaces et à prendre des mesures efficaces pour faire face aux incidents de sécurité.



- (3) Il existe des CERT privées et publiques, et elles peuvent exister au niveau national, régional ou de l'entreprise. Dans de nombreux pays, il existe également des organisations CERT nationales qui sont spécifiquement responsables de la cybersécurité nationale et qui travaillent en étroite collaboration avec d'autres CERT. L'objectif d'une CERT est de renforcer la cybersécurité, d'augmenter la résilience face aux cyberattaques et de minimiser l'impact des incidents de sécurité. **Il est important de noter que CERT est une marque déposée de l'Université Carnegie Mellon (CMU). Les organisations peuvent utiliser la marque CERT après avoir obtenu une autorisation. Certaines organisations, qui ne savent probablement pas qu'il s'agit d'une marque déposée, l'utilisent néanmoins pour définir leurs équipes de réponse aux incidents.**

CIRT et CSIRT

- (4) La CIRT et la CSIRT sont toutes deux des équipes qui s'occupent de la réponse aux cyberincidents, mais ont des priorités différentes. Globalement, on peut dire qu'une CIRT est davantage axée sur les besoins de sécurité internes d'une entreprise ou d'une unité organisationnelle, tandis qu'une CSIRT a une perspective plus large et peut disposer de ressources plus spécialisées pour répondre à différents types de cybermenaces.

CIRT

- (5) Une **Computer Incident Response Team** (CIRT ou équipe de réponse aux incidents informatiques) est typiquement interne et se concentre sur la réponse aux cyberincidents au sein d'une entreprise ou d'une unité organisationnelle. Elle se compose d'employés de l'entreprise ou des unités organisationnelles responsables de la sécurité, tels que des experts en sécurité IT/OT, des administrateurs réseau et des experts en criminalistique. La tâche principale d'une CIRT est de réagir aux incidents de sécurité qui affectent les systèmes internes, les réseaux ou les données de l'organisation. Une CIRT peut également développer des mesures préventives afin d'éviter de futurs incidents et mettre en œuvre des politiques et des procédures visant à améliorer la sécurité générale de l'organisation.

CSIRT

- (6) Une **Computer Security Incident Response Team** (CSIRT ou équipe de réponse aux incidents de sécurité informatique) peut être interne ou externe et se concentre sur la réponse aux cyberincidents qui peuvent affecter un plus large éventail d'entreprises et d'unités organisationnelles, y compris les agences fédérales, les entreprises et autres institutions. Elle peut être gérée par une organisation ou un groupe sectoriel et peut souvent être spécialisé dans une région, un secteur ou un type de cybermenaces spécifiques. Une CSIRT peut également disposer de ressources et d'une expertise spécialisée pour répondre à des cyberattaques complexes ou de grande envergure, qui peuvent nécessiter des efforts coordonnés. Les tâches d'une CSIRT comprennent souvent aussi la surveillance des menaces, l'analyse des incidents de sécurité et la fourniture d'informations et de recommandations pour améliorer la cybersécurité générale.

SOC

- (7) Un **Security Operation Center** (SOC ou centre d'opération de sécurité) est un établissement ou un service spécialisé, à l'intérieur ou à l'extérieur de l'entreprise ou de l'unité organisationnelle, dont la mission principale est de surveiller et de protéger la sécurité de l'information et de réagir aux incidents de sécurité.
- (8) Un SOC peut être mis en place en interne dans une organisation ou sous la forme d'un service fourni par un prestataire externe (MSSP - Managed Security Service Provider). La mise en place d'un SOC est essentielle pour garantir la sécurité de l'information, identifier les menaces en temps réel et y répondre de manière appropriée. Il s'agit d'un élément essentiel des mesures de sécurité modernes pour les entreprises et les unités organisationnelles afin de se protéger contre les cyberattaques et de s'y préparer.

3.2.5 Fabricants et fournisseurs

- (1) Le rôle des fabricants et des fournisseurs dans l'amélioration de la résilience des TIC (technologies de l'information et de la communication) est essentiel, surtout à une époque où la technologie joue un rôle central dans l'économie et la société:

Fabricant:

- **Innovation de produit:** les fabricants de matériel et de logiciels TIC sont responsables de la conception et de la production de solutions technologiques robustes et résistantes. Cela implique la création



de produits qui résistent aux perturbations et aux pannes, comme le matériel avec une alimentation électrique redondante ou les logiciels avec des fonctions de sécurité intégrées (Security by Design).

- **Contrôle de la qualité:** les fabricants doivent effectuer des contrôles de qualité et des tests rigoureux afin de s'assurer que leurs produits répondent aux exigences en matière de performance et de sécurité. Ceci est essentiel pour garantir la fiabilité des systèmes TIC.
- **Fournir des services de maintenance et de réparation:** les fabricants peuvent proposer des services de maintenance et de réparation pour leurs produits afin d'assurer une récupération rapide en cas de panne ou de défaillance.

Fournisseurs:

- **Chaîne et sécurité d'approvisionnement:** les fournisseurs de matières premières pour les TIC et de composants doivent s'assurer que la chaîne d'approvisionnement est robuste et sûre afin de garantir la disponibilité continue des matériaux critiques. Cela implique l'identification de fournisseurs alternatifs et la diversification des sources d'approvisionnement.
 - **Préparation aux situations d'urgence:** les fournisseurs doivent élaborer des plans d'urgence pour pouvoir réagir aux catastrophes naturelles, aux conflits géopolitiques ou à d'autres crises. Cela peut inclure la mise en place d'entrepôts de secours, le stockage de composants critiques et la mise en œuvre de protocoles de réponse aux crises.
 - **Coopération et communication:** les fournisseurs doivent travailler en étroite collaboration avec leurs clients (les fabricants) et maintenir une communication claire afin d'identifier et de gérer les risques et les défis potentiels de la chaîne d'approvisionnement à un stade précoce.
- (2) La collaboration entre les fabricants et les fournisseurs est essentielle pour renforcer la résilience des TIC. En développant des produits résistants, en sécurisant les chaînes d'approvisionnement et en mettant en œuvre des plans d'urgence, ils peuvent contribuer à minimiser les pannes et les perturbations des technologies de l'information et de la communication et à garantir la continuité des processus commerciaux ainsi que la sécurité des systèmes TIC. Cela est particulièrement important dans les secteurs sensibles tels que la santé, l'énergie et la finance.
- (3) Les fabricants et les fournisseurs jouent un rôle important dans le respect des normes, des règles et des spécifications. Ces règles et normes sont essentielles pour garantir la qualité, la sécurité et les performances des produits et services.

Rôle des producteurs:

- **Respect des normes de qualité:** les fabricants doivent s'assurer que leurs produits sont conformes aux normes et standards de qualité en vigueur. Cela peut inclure des certifications de qualité spécifiques à la branche, des spécifications techniques et des normes de sécurité.
- **Conception et développement de produits:** les fabricants sont responsables de la conception et du développement des produits de manière à ce qu'ils soient conformes aux normes et réglementations applicables. Cela nécessite souvent l'intégration d'exigences spécifiques dans le processus de conception.
- **Contrôle de la qualité et tests:** les fabricants doivent effectuer des contrôles de qualité et des tests rigoureux afin de s'assurer que leurs produits répondent aux spécifications établies. Il peut s'agir de contrôles et de certifications internes ou externes.
- **Documentation et étiquetage:** les fabricants doivent fournir toutes les informations nécessaires, telles que la documentation technique, les fiches de données de sécurité et les déclarations de conformité, et veiller à ce que leurs produits soient correctement étiquetés.

Rôle des fournisseurs:

- **Approvisionnement en matériaux conformes:** les fournisseurs doivent s'assurer que les matières premières, composants et services qu'ils fournissent sont conformes aux normes et réglementations en vigueur. Cela peut impliquer de travailler avec des fabricants et des fournisseurs qualifiés.
- **Des spécifications détaillées:** les fournisseurs doivent fournir des spécifications claires et détaillées pour les matériaux et services qu'ils fournissent afin de s'assurer qu'ils répondent aux exigences.



- **Traçabilité et assurance qualité:** les fournisseurs doivent mettre en œuvre des mécanismes de traçabilité et de contrôle de la qualité afin de s'assurer que les produits livrés répondent aux normes requises.
 - **Certifications et conformité:** les fournisseurs peuvent fournir des certifications et des déclarations de conformité afin d'attester que leurs produits et services sont conformes aux normes et réglementations en vigueur.
- (4) La coopération entre les fabricants et les fournisseurs est essentielle pour garantir que les produits et les services sont conformes aux normes et réglementations pertinentes. Cette coopération contribue à garantir la qualité et la sécurité des produits, à minimiser les risques de non-conformité et à renforcer la confiance des clients et des autorités de réglementation. En outre, le respect des normes et des réglementations permet également aux fabricants et aux fournisseurs d'obtenir des avantages concurrentiels et de faciliter l'accès aux marchés qui imposent des exigences strictes en matière de qualité et de sécurité des produits.



Une gestion active de la chaîne d'approvisionnement (prestataires de services et fabricants) est impérative de la part des entreprises et des unités organisationnelles. C'est précisément dans le domaine de la gestion des risques et des menaces que la chaîne d'approvisionnement doit être activement impliquée.



Il est indispensable d'établir des directives dans le domaine de la gestion des fournisseurs et de les consigner dans un guide de travail. Les directives doivent contenir des exigences de contrôle organisationnel, de gestion des incidents de sécurité de l'information, des exigences de contrôle des personnes ainsi que des exigences de contrôle physique et technologique.



Références à des documents complémentaires:

Modèle: HoP-01-01-03-22 Manuel de travail Domaine ISMS: Gestion des fournisseurs

NIST SP 800-161r1 Pratiques de gestion des risques de la chaîne d'approvisionnement de cyber-sécurité pour les systèmes et les organisations

3.3 Bases légales: lois et règlements obligatoires

- (1) Le résumé suivant donne une vue d'ensemble des bases légales en vigueur sous forme d'articles de loi et d'ordonnance qui doivent être appliqués en relation avec l'augmentation de la résilience TIC chez les fournisseurs d'énergie dans le domaine de l'électricité:

3.3.1 Aperçu des lois, ordonnances et dispositions légales en rapport avec la sécurité de l'approvisionnement et de l'information



Les lois et ordonnances nationales suivantes contiennent des prescriptions en rapport avec la sécurité de l'approvisionnement et de l'information, qui doivent être impérativement respectées:

- Constitution fédérale de la Confédération suisse (Cst.; RS 101): art. 102
- Code des obligations (RS 220): art. 728a, 728b, 754, 961, 961c
- Loi fédérale sur l'approvisionnement économique du pays (loi sur l'approvisionnement du pays LAP; RS 531): art. 4, 31, 32
- Ordonnance sur l'approvisionnement économique du pays (OAEP; RS 531.11): art. 7, 11
- Ordonnance sur l'organisation chargée d'assurer l'approvisionnement économique du pays dans le domaine de l'électricité (OEBE; RS 531.35): art. 1, 1a, 1b, 2
- Loi sur l'énergie (LEne; RS 730.0): art. 7
- Loi fédérale sur l'approvisionnement en électricité (LApEI; RS 734.7): art. 6
- Ordonnance sur l'approvisionnement en électricité (OApEI; RS 734.71): art. 5, 5a
- Loi fédérale sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI; RS 128): art. 5, 74, 76, 77, 78
- Loi fédérale sur la protection des données (loi sur la protection des données, LPD; RS 235.1): art.
- Système de contrôle interne CO 728a, 728b



Les lois et ordonnances internationales suivantes contiennent des prescriptions en rapport avec la sécurité de l'approvisionnement et de l'information, qui doivent impérativement être remplies par les entreprises et unités organisationnelles concernées:

- Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016, p. 1.
- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures relatives à un niveau commun élevé de cybersécurité dans l'Union, modifiant le règlement





La liste ci-dessus n'est pas exhaustive. Il existe encore d'autres articles de lois et d'ordonnances qui ne sont pas explicitement mentionnés, car ils ne peuvent être qu'indirectement liés à la sécurité de l'information.



Les dispositions légales et les ordonnances de la Confédération et des services fédéraux sont contraignantes et doivent être impérativement respectées.



Les entreprises et les unités organisationnelles doivent en partie mettre en œuvre les dispositions légales et les directives internationales. Les entreprises et les unités organisationnelles doivent vérifier quelles directives légales internationales doivent être respectées.



Les articles de loi sont énumérés à l'annexe C.

3.3.2 OFPP Stratégie nationale de protection des infrastructures critiques



(1) La Stratégie nationale de protection des infrastructures critiques (PIC) est un document stratégique important en Suisse, qui se concentre sur la protection et la résilience des installations et services cruciaux. La PIC identifie les secteurs critiques, évalue les risques, encourage les mesures préventives, renforce la sécurité et la capacité de réaction aux menaces et souligne la nécessité d'une collaboration entre le gouvernement, les opérateurs et les autres parties prenantes.

Elle vise à garantir la sécurité nationale et le bien-être de la population et à accroître la résilience face aux crises. Les principaux points de la PIC comprennent:

- **Identification et catégorisation:** la PIC commence par l'identification et la catégorisation des infrastructures critiques en Suisse. Il s'agit de secteurs tels que l'énergie, l'eau, les télécommunications, les transports, la santé et bien d'autres encore, qui sont essentiels au bien-être national et à l'économie.
 - **Évaluation et gestion des risques:** la stratégie met l'accent sur l'évaluation régulière des risques et des menaces auxquels ces infrastructures critiques sont exposées. Cela comprend l'analyse des catastrophes naturelles, des incidents techniques et des attaques intentionnelles. Des mesures de réduction des risques sont élaborées sur la base de ces évaluations.
 - **Coopération coordonnée:** la PIC encourage une étroite collaboration entre différents acteurs, dont les autorités fédérales, cantonales et communales, les exploitants d'infrastructures critiques ainsi que les entreprises et unités organisationnelles privées. L'accent est mis sur une approche coordonnée et partenariale afin de garantir une réponse efficace aux menaces et aux situations d'urgence.
 - **Mesures de sécurité et de prévention:** la stratégie définit des mesures visant à renforcer la sécurité et à prévenir les perturbations et les attaques. Cela comprend l'amélioration de la sécurité physique, le renforcement de la sécurité de l'information et la formation du personnel.
 - **Gestion des urgences et planification des mesures d'urgence:** la PIC souligne la nécessité d'une structure de gestion des urgences complète et d'une planification claire des mesures d'urgence afin de pouvoir réagir de manière appropriée aux perturbations et aux catastrophes.
 - **Communication et sensibilisation:** la stratégie encourage la communication et la sensibilisation auprès du public et des parties prenantes afin de renforcer la compréhension de l'importance de la protection des infrastructures critiques.
- (2) La stratégie PIC est un cadre important pour garantir la sécurité et la résilience de la Suisse en matière d'infrastructures critiques. Elle pose les bases de la collaboration entre les autorités et le secteur privé et souligne l'importance de la prévention, de la protection et de la gestion des urgences.



3.3.3 Guide de l'OFPP sur la protection des infrastructures critiques



(1) Le guide «Protection des infrastructures critiques» montre comment la capacité de résistance (résilience) des infrastructures critiques peut être vérifiée et renforcée. Il contribue à prévenir les défaillances graves des infrastructures critiques et à réduire le temps d'immobilisation en cas d'événement. Sur le plan méthodologique, le guide s'appuie sur des concepts courants et établis de gestion des risques, des crises et de la continuité et combine différents éléments de ces approches dans le sens d'une protection intégrale. Le guide s'appuie sur les planifications et les travaux correspondants dont disposent déjà de nombreuses entreprises et unités organisationnelles. Alors que ces derniers se concentrent généralement sur les risques pour les entreprises et les unités organisationnelles, le guide PIC met l'accent sur la question de savoir dans quelle mesure

les défaillances des infrastructures critiques affectent la population et ses besoins vitaux (économiques). La mise en œuvre du guide PIC nécessite une étroite collaboration entre les exploitants d'infrastructures critiques et les autorités respectives, spécialisées, de surveillance et de régulation, dans les différents domaines des infrastructures critiques (énergie, transports, santé publique, etc.).

(2) Le guide Protection des infrastructures critiques offre un cadre et des recommandations pratiques pour la protection des installations et services importants en Suisse. Voici un résumé des points principaux:

- **Définition des infrastructures critiques:** le guide identifie et définit les secteurs et installations critiques qui sont essentiels au fonctionnement de la Suisse, tels que l'énergie, l'approvisionnement en eau, les télécommunications, les transports et les soins de santé.
- **Évaluation des risques et prévention:** il souligne l'importance de l'évaluation des risques afin d'identifier les menaces et les vulnérabilités potentielles des infrastructures critiques. Des mesures préventives sont recommandées afin de minimiser ces risques.
- **Protection et sécurité:** le guide suggère des mesures pour renforcer la sécurité dans les installations critiques, y compris la sécurité physique, les restrictions d'accès et les systèmes de surveillance.
- **Gestion des situations d'urgence et rétablissement:** des lignes directrices sont fournies pour l'élaboration de plans d'urgence et le rétablissement après un incident, afin de renforcer la résilience des infrastructures critiques.
- **Coopération et échange d'informations:** le guide encourage la coopération entre les services gouvernementaux, les exploitants d'infrastructures critiques, les gouvernements cantonaux et les autres parties prenantes. L'échange d'informations et la coopération sont essentiels pour réagir efficacement aux menaces et aux situations d'urgence.
- **Sensibilisation et formation:** il met l'accent sur la sensibilisation du public et des personnes concernées, en fournissant des formations et des informations afin d'améliorer la préparation et la protection.

(3) Le guide Protection des infrastructures critiques sert d'outil pratique pour promouvoir la protection et la résilience des installations critiques en Suisse et pour s'assurer qu'elles continuent à fonctionner efficacement en cas de menaces ou de crises.

3.3.4 OFAE Norme minimale TIC pour améliorer la résilience des TIC



(1) La sécurité des TIC implique un comportement basé sur les risques et l'utilisation de systèmes sûrs dans le domaine de responsabilité des exploitants respectifs. La mise en œuvre de mesures éprouvées, telles que celles présentées dans la norme minimale TIC sur les améliorations de la résilience des TIC, permet déjà de parer à un grand nombre d'attaques TIC à un coût raisonnable. La présente norme a pour objectif de fournir aux entreprises et aux unités organisationnelles, un outil polyvalent leur permettant d'améliorer individuellement la résilience de leur infrastructure TIC. Grâce à une approche basée sur les risques, la norme permet la mise en œuvre de différents niveaux de protection, adaptés aux besoins de l'organisation.

(2) La norme minimale en matière de TIC a été élaborée par l'Office fédéral pour l'approvisionnement économique du pays en collaboration avec des experts externes du domaine de la sécurité des TIC. Il existe aujourd'hui déjà plusieurs normes internationales reconnues en matière de sécurité des TIC, dont la plupart vont bien au-delà du présent document. La norme minimale TIC ne doit pas être vue comme une concurrence aux normes internationales existantes, mais est compatible avec celles-



ci, tout en ayant une portée réduite. Elle doit permettre de se familiariser plus facilement avec le sujet tout en garantissant un niveau de protection élevé. En complément de la norme minimale TIC, l'Office fédéral pour l'approvisionnement économique du pays a élaboré d'autres normes sectorielles qui présentent un degré de détail (technique) plus élevé. Il est recommandé aux exploitants d'infrastructures critiques de s'orienter, en plus de la norme minimale TIC, vers les directives détaillées spécifiques au secteur dès qu'elles sont disponibles. Si des normes propres à un secteur sont déjà en vigueur ou si des normes internationales telles que l'ISO ou le NIST sont utilisées, les entreprises et les unités organisationnelles peuvent utiliser la liste de contrôle du chapitre «Partie 3 – Mission d'audit» pour déterminer si elles ont déjà couvert la présente norme minimale TIC.

- (3) Il existe dans le monde entier une multitude de normes et de sources d'information différentes pour gérer les risques liés aux TIC. Certaines d'entre elles sont déjà reconnues et utilisées par l'économie. La norme minimale TIC de l'OFAE est basée sur le NIST Cybersecurity Framework Core. Le cas échéant, il est complété par d'autres normes industrielles reconnues au niveau international.

Les principes de la norme minimale TIC pour améliorer la résilience des TIC sont les suivants:

- **Responsabilité individuelle:** les exploitants d'infrastructures critiques sont responsables du maintien de leurs processus TIC critiques.
- **Gestion de la continuité des activités:** tous les aspects de la sécurité des TIC doivent être intégrés dans une gestion globale de la continuité des activités.
- **Gestion des risques:** il incombe aux exploitants d'infrastructures critiques d'évaluer en permanence les risques potentiels liés aux TIC, tels que les atteintes à la disponibilité, à l'intégrité et à la confidentialité. L'entreprise et les unités organisationnelles doivent évaluer quels risques doivent être réduits et lesquels peuvent être supportés.



Le standard minimal TIC pour l'amélioration de la résilience TIC est obligatoire dans l'OApEI et doit donc être appliqué par toutes les entreprises et unités organisationnelles concernées de la branche électrique et mis en œuvre conformément au profil de protection attribué.

- (4) L'objectif du standard minimal TIC est d'augmenter la cyber-résilience pour les entreprises et les unités organisationnelles dans toute la Suisse.

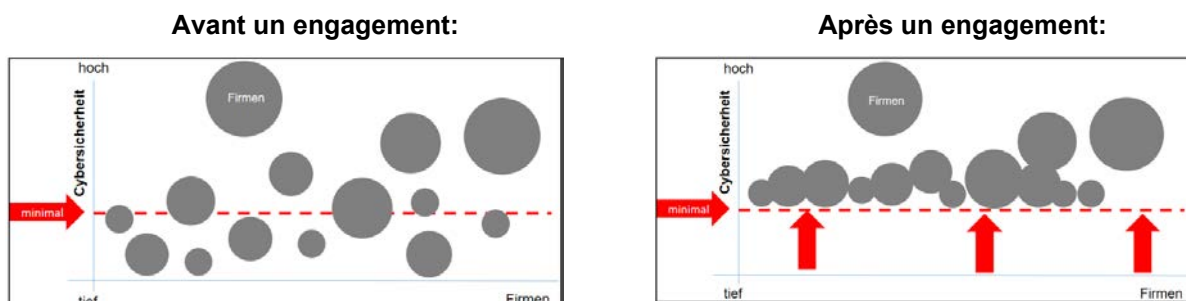


Figure 4: Augmentation de la cybersécurité (source BWL)

3.3.5 OFAE Norme minimale TIC - Outil d'évaluation selon NIST CSF 1.1



- (1) L'OFAE a publié un outil d'évaluation de la norme minimale TIC de l'OFAE afin de déterminer l'emplacement et de vérifier les mesures mises en œuvre. Cet outil est basé sur le NIST Cybersecurity Framework (CSF) version 1.1. Ce cadre est un instrument important qui aide les entreprises et les unités organisationnelles à améliorer leurs pratiques et processus de cybersécurité. Le cadre se compose de plusieurs éléments principaux qui aident les entreprises et les unités organisationnelles à développer et à mettre en œuvre leurs stratégies de cybersécurité.

Structure de base du NIST Cybersecurity Framework (CSF) version 1.1:

1. Framework Core (cœur du framework):

Le cœur du cadre de référence est constitué de cinq fonctions principales ou domaines d'activité qui représentent les objectifs fondamentaux de la cybersécurité. Ces fonctions sont

- **Identifier (Identify):** il s'agit ici d'identifier les actifs, les vulnérabilités et les risques existants et de procéder à une évaluation complète des risques.



- **Protect** (protéger): ce domaine traite des mesures visant à protéger les systèmes et les données contre les cybermenaces. Il s'agit notamment des contrôles d'accès, de la formation et de la sensibilisation.
- **Detect** (Détecter): il s'agit ici de décrire les processus et les technologies permettant de détecter les attaques et les incidents de sécurité à un stade précoce.
- **Respond** (Répondre): ce domaine se concentre sur la réponse appropriée aux incidents de sécurité afin de minimiser les dommages et de favoriser la récupération.
- **Recover** (restauration): il s'agit ici de restaurer les systèmes et les services après un incident de sécurité afin de reprendre un fonctionnement normal.

Chaque fonction principale ou domaine d'activité est divisé en catégories et sous-catégories. Au niveau de la sous-catégorie, il est possible de procéder à l'évaluation (tiers implantés au niveau de la mise en œuvre). De plus, au niveau de la sous-catégorie, les références aux normes, directives et prescriptions sont faites.

2. Framework Implementation Tiers (niveaux de mise en œuvre du cadre):

Le NIST Framework connaît quatre *Implementation Tiers* (en français, niveaux de mise en œuvre). Ceux-ci décrivent le niveau de développement (niveau de protection) qu'une entreprise ou une unité organisationnelle a mis en œuvre. Ils vont de partiel (Tier 1) à dynamique (Tier 4). Pour déterminer son propre niveau de protection (*Tier Level*), une organisation doit connaître précisément ses pratiques de gestion des risques, l'environnement des menaces ainsi que les exigences légales et réglementaires, les objectifs commerciaux et les directives organisationnelles.

3. Framework Profiles (profils cadre):

Un profil cadre est une compilation personnalisable d'activités et de catégories de cybersécurité adaptées aux besoins et objectifs spécifiques d'une entreprise et d'unités organisationnelles. Les entreprises et les unités organisationnelles peuvent créer des profils afin de présenter leurs objectifs de sécurité actuels et souhaités.

4. Framework Implementation Tiers and Profiles Tool (outil pour les niveaux et les profils de mise en œuvre du cadre):

Il s'agit d'un outil permettant aux entreprises et aux unités organisationnelles de déterminer leur position actuelle par rapport aux niveaux d'implémentation du framework et aux profils du framework. Il aide à la planification et à la mise en œuvre des améliorations.

5. Framework Core Informative References (références supplémentaires au noyau du framework):

Ces documents de référence fournissent des informations et des ressources supplémentaires qui peuvent aider les entreprises et les unités organisationnelles à mettre en œuvre le Framework Core.

- (2) Le NIST CSF 1.1 offre une structure flexible qui permet aux entreprises et aux unités organisationnelles d'adapter et d'améliorer leurs besoins individuels en matière de cybersécurité. Il sert de guide pour l'élaboration et la mise en œuvre d'une stratégie de cybersécurité robuste et pour l'amélioration de la résistance aux cybermenaces.

Exécution de la norme minimale TIC de l'OFAE - outil d'évaluation:

- (3) La version actuelle de l'outil d'évaluation de la norme minimale TIC de l'OFAE est basée sur le NIST Cybersecurity Framework (CSF) version 1.1. Les éléments du NIST CSF 1.1 sont reproduits dans l'outil:

Function Funktion Thema	Category Kategorie Catégorie Categoria	Subcategory Aktivität Tâches Missioni	Rating Bewertung Appreciation Stärke	Comments Kommentäre Commentaires Commenti	Empfehlungen DWL Prozessierung	Informative References Referenzen Referenzen Referimenti
		DS.AM-5: Draw up an inventory-taking process which ensures that you have a complete inventory of all your ICT assets at all times. Erarbeiten Sie einen Inventarisierungsprozess welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar aller ICT-Betriebsmittel (Assets) vorhanden ist. Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC (Assets). Definisci una procedura che garantisca la costante presenza di un inventario completo dei vostri strumenti operativi TIC (asset).	alta		Hoch	CIS CSC 1 COBIT 5 BA09.01, BA09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2022 A.5.9 ISO/IEC 27019:2017 7.11.7.12 NERC CIP-002 BSI Standard NIS-2, Kapitel 4.2 Strukturanalyse, M.2.2.25 Zuweisung der Verantwortlichkeit für Informationen, Anwendungen und IT-Komponenten NIST SP 800-53 Rev. 5 CMSS, PMAS

Figure 5: Extrait de l'outil d'évaluation de la norme minimale TIC de l'OFAE (source OFAE)

- **Fonction:** fonctions principales ou domaines d'activité du NIST CSF 1.1
- **Catégorie:** catégorie pour la fonction ou les fonctions principales ou les domaines d'activité du NIST CSF 1.1
- **Activité:** sous-catégorie des fonctions principales ou des domaines d'activité du NIST CSF 1.1
- **Évaluation:** maturités de mise en œuvre (Tier's) selon la description ci-dessous



- **Recommandation de l'OFAE concernant les priorités:** recommandation de l'OFAE concernant les priorités
- **Références:** références aux mesures de mise en œuvre (normes et standards)

Les maturités de mise en œuvre (Tiers) dans le standard minimal TIC de l'OFAE - Assessment Tool:

- (4) Contrairement au CSF 1.1 du NIST, ce ne sont pas les niveaux qui sont utilisés pour évaluer les buts, les objectifs ou le degré de réalisation. Des maturités ont été introduites à cet endroit afin de refléter les critères d'évaluation plus complets et plus précis. La notation suivante est utilisée:

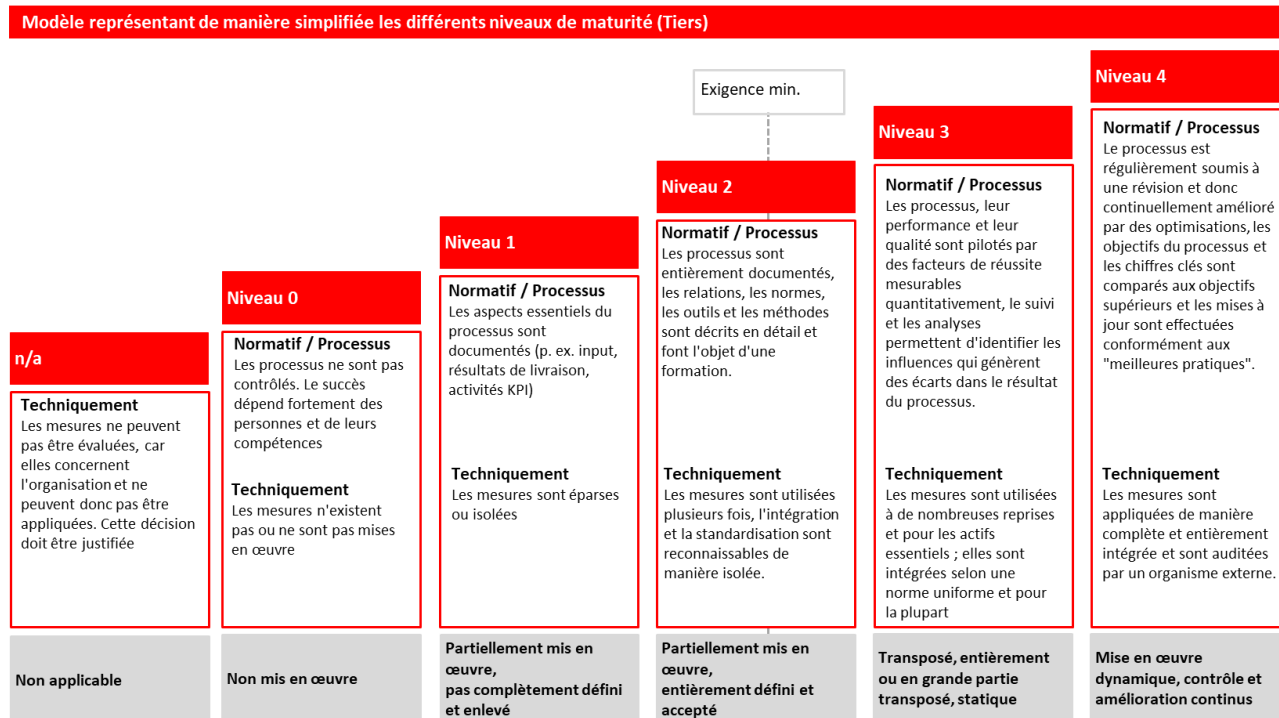


Figure 6: OFAE Standard minimal TIC Maturités (source OFAE)



L'outil d'évaluation de la norme minimale pour les TIC de l'OFAE selon la norme NIST CSF 1.1 est un outil qui peut être créé pour une auto-évaluation. Il s'agit de prendre un instantané de la situation existante. L'outil n'est pas là pour comparer l'état souhaité à l'état réel, et ne permet donc pas non plus de faire une analyse GAP. L'applicabilité ou SoA (Statement of Applicability) ne peut être représentée que de manière limitée, car le contrôle individuel peut certes être évalué comme n/a, mais aucun champ n'est prévu pour la justification.

3.3.6 OFEN Engagement de la norme minimale pour les TIC pour accroître la résilience des TIC

- (1) La révision de l'ordonnance du 14 mars 2008 sur l'approvisionnement en électricité (OApEI; RS 734.71; état au 1er juillet 2024) a pour objectif de déclarer la norme minimale pour les TIC obligatoire pour les principaux fournisseurs d'électricité. Les acteurs ainsi obligés doivent atteindre un certain niveau de protection lors de la mise en œuvre des mesures prévues par le standard. Dans un souci de proportionnalité, plusieurs niveaux de protection (profils de protection) sont prévus avec des exigences échelonnées.
- (2) La norme minimale pour les TIC définit une série de thèmes avec des tâches de la cybersécurité et est un outil important pour garantir la protection contre les cyberattaques. La norme est basée sur le NIST Cybersecurity Framework américain. Elle contient 108 tâches réparties en 23 catégories. La maturité organisationnelle de la cybersécurité dans une entreprise et dans les unités organisationnelles peut être évaluée et améliorée à l'aide de cette structure.
- (3) Les domaines thématiques fondamentaux de la norme minimale pour les TIC de l'OFAE sont pour l'essentiel inchangés par rapport au NIST CSF, mais leur mise en œuvre requiert une certaine flexibilité, une adaptation aux menaces et dangers spécifiques à l'entreprise, à l'unité organisationnelle et nouveaux, des outils techniques et des connaissances spécialisées correspondantes. Aucune solution technique n'est prescrite. Les entreprises et les unités organisationnelles devront les élaborer de manière autonome. Elles peuvent également s'associer dans le cadre des structures associatives existantes et élaborer une norme sectorielle correspondante.





Conformément à l'art. 5a de l'ordonnance sur l'approvisionnement en électricité (OApEI; RS 734.71), la norme minimale pour les TIC est rendu obligatoire par l'OFEN; il doit donc être appliqué par toutes les entreprises et unités organisationnelles concernées de la branche électrique et mis en œuvre en conséquence.

3.3.6.1 Niveau de protection selon l'OFEN

- (1) Le niveau de protection définit les exigences relatives au degré de mise en œuvre des tâches fixées dans la norme minimale TIC (valeurs / tier level selon le chapitre 3 de la norme minimale pour les TIC de l'OFAE). Les gestionnaires de réseau, les producteurs, les exploitants de stockage et les prestataires de services sont classés par catégories en fonction du volume d'électricité ou de la puissance transporté. La catégorie A remplit les exigences (niveaux de protection) les plus élevées, les catégories B et C remplissent chacune des exigences (niveaux de protection) légèrement inférieures. Pour les plus petits acteurs du marché, la catégorie C ne prévoit que des objectifs (niveaux de protection) pour un nombre limité de tâches. Les tâches pour lesquelles aucune valeur correspondante n'est fixée ne doivent pas obligatoirement être mises en œuvre et restent donc des recommandations non contraignantes. Les trois catégories pour les gestionnaires de réseau, les producteurs et les prestataires de services se trouvent dans l'annexe 1a de la révision 24b de l'OApEI. Les valeurs qui y sont consignées (niveaux de protection) ont été définies pour chaque catégorie sur la base de la criticité des entreprises, des unités organisationnelles et en tenant compte des moyens nécessaires à leur mise en œuvre. Les valeurs qui y sont consignées ont été définies pour chaque niveau de protection sur la base de la criticité des entreprises, des unités organisationnelles et en tenant compte des moyens nécessaires à leur mise en œuvre.
- (2) Afin d'attribuer une catégorie (A, B ou C) aux entreprises et unités organisationnelles soumises à l'obligation, les critères correspondants sont définis. Dans la mesure où une entreprise ou une unité organisationnelle répond aux critères d'une catégorie, celle-ci est déterminante pour l'entreprise et l'unité organisationnelle. Par exemple, la catégorie A s'applique aux gestionnaires de réseau qui atteignent une quantité d'électricité transportée d'au moins 450 GWh/an (ch. 1.1, annexe 1a). Les analyses et les pratiques d'autres organismes spécialisés ont été prises en compte lors de la définition des critères. Ainsi, le critère de 450 GWh/an, qui permet d'attribuer la catégorie A aux gestionnaires de réseau, correspond à une valeur fixée par l'Office fédéral de la protection de la population (OFPP) pour les infrastructures critiques d'importance nationale. Le critère de 112 GWh/an pour la catégorie B des gestionnaires de réseau et des prestataires de services correspond pour l'essentiel à la valeur annualisée qui, selon l'AES, caractérise une crise.
- (3) Pour les producteurs et les exploitants de stockage, une puissance de 800 MW pour la catégorie A et de 100 MW pour la catégorie B a été retenue. Cette dernière correspond à la valeur définie dans l'ordonnance sur l'énergie pour les centrales de pompage-turbinage d'intérêt national.
- (4) Les producteurs, les exploitants de stockage et les prestataires de services de ces deux acteurs ne sont pas soumis à l'obligation de respecter la norme minimale pour les TIC en dessous d'une puissance de 100 MW. Une catégorie C n'est pas prévue pour ces derniers. Dans la mesure où la valeur seuil de 100 MW n'est pas atteinte, la norme reste pour eux une simple recommandation. Cela est, d'une part, dû à leur influence sur la sécurité d'approvisionnement qui est moins importante que celle des gestionnaires de réseau qui accèdent directement au réseau via la technologie de commande et, d'autre part, dû au fait qu'ils ne peuvent pas intégrer les coûts de la cybersécurité dans les tarifs, contrairement aux gestionnaires de réseau.
- (5) Dans la mesure où des prestataires de services externes, qui gèrent les systèmes TIC pour le compte d'une entreprise ou d'une unité organisationnelle, ont un accès permanent aux systèmes de contrôle (systèmes de gestion opérationnelle) des donneurs d'ordre, ils doivent respecter les mêmes consignes que ces derniers. La valeur seuil retenue est celle de la quantité d'énergie distribuée ou produite par l'ensemble des clients raccordés au travers d'un même système.



(6) Le champ d'application et la catégorie attribuée sont définis comme suit dans l'annexe 1a de l'Ordonnance sur l'approvisionnement en électricité (OApEI; RS 734.71):

	Niveau de protection pour la catégorie A	Niveau de protection pour la catégorie B	Niveau de protection pour la catégorie C
1.1 Gestionnaires de réseau dont le volume d'électricité transportée au sein de leur zone de desserte est de:	≥ 450 GWh/an	≥ 112 GWh/an et < 450 GWh/an	< 112 GWh/an
1.2 Prestataires qui peuvent durablement piloter des installations de gestionnaires de réseau, s'ils ont de ce fait accès via un seul système à un volume d'électricité transportée de:			
1.3 Producteurs, à l'exception des exploitants de centrales nucléaires, et exploitants de stockage s'ils exploitent et peuvent piloter via un seul système des installations d'une puissance totale de:	≥ 800 MW	≥ 100 MW et < 800 MW	-
1.4 Prestataires qui peuvent durablement piloter des installations de producteurs, à l'exception des exploitants de centrales nucléaires, ou d'exploitants de stockage, s'ils ont de ce fait accès via un seul système à une puissance de:			

Tableau 2: Définition des profils d'entreprises selon l'OApEI (source OFEN/AES)



Conformément à l'annexe 1a de l'Ordonnance sur l'approvisionnement en électricité (OApEI; RS 734.71), toutes les entreprises et unités organisationnelles concernées se voient attribuer une catégorie avec des niveaux de protection définis. Dans les valeurs de niveau de protection de chaque catégorie, elles sont associées aux sous-catégories à traiter (tâches) selon le cadre de référence NIST CSF 1.1 et sont accompagnées d'une maturité minimale à respecter.

3.3.6.2 Attribution des tâches au niveau de la sous-catégorie à chaque catégorie et valeurs de niveau de protection définies pour chaque maturité (tiers)

- (1) Selon l'annexe 1a de l'Ordonnance sur l'approvisionnement en électricité (OApEI; RS 734.71), des valeurs minimales de niveau de protection doivent être atteintes conformément au chapitre 3 de la norme minimale pour les TIC.
- (2) Les valeurs minimales pour le niveau de protection sont définies et mentionnées dans l'annexe 1a de l'Ordonnance sur l'approvisionnement en électricité (OApEI; RS 734.71).



Dans l'annexe 1a de l'Ordonnance sur l'approvisionnement en électricité (OApEI; RS 734.71), les valeurs minimales pour les tiers / maturités sont fixées au niveau de la sous-catégorie (tâches) du CST NIST 1.1 et sont donc obligatoires ou doivent être au moins atteintes.



3.3.7 EICom: suivi de l'approche et des résultats en matière d'amélioration de la résilience des TIC



par l'EICom». Cette directive définit la procédure et les exigences. Les points importants suivants ressortent de la directive:

Surveillance

- (1) En vertu de sa compétence générale (art. 22, al. 1 LApEI), l'EICom surveille la procédure et les résultats des activités visant à augmenter la résilience des TIC, le respect des articles 8a LApEI et 5a OApEI.
- (2) Les activités de surveillance correspondantes sont énumérées dans la directive 1/2024 «Surveillance de la cybersécurité assurée par l'EICom». Cette directive définit la procédure et les exigences. Les points importants suivants ressortent de la directive:
- (3) Dans le cadre de la surveillance, l'EICom suit une approche basée sur les risques en ce qui concerne l'exploitation sûre du réseau électrique suisse. L'objectif de la surveillance est d'augmenter la résilience face aux cybermenaces. Ainsi, les entreprises sont surveillées à différents niveaux en fonction de leur importance et de la situation de risque pour l'exploitation sûre et stable du réseau électrique suisse. Les instruments de surveillance doivent permettre à l'EICom d'évaluer si les mesures prises correspondent aux considérations de l'entreprise en matière de risques et si les prescriptions légales sont respectées. Cela signifie également que l'EICom peut, sur la base de son activité de régulation, émettre des recommandations et/ou ordonner des mesures. Pour faire appliquer les mesures, l'EICom dispose des moyens juridiques habituels. Actuellement, l'EICom prévoit d'utiliser et de combiner trois instruments de surveillance de manière complémentaire.

Sondages

- (4) Après l'entrée en vigueur de l'OAPEI révisée, les entreprises devront remplir certaines exigences minimales. Dans un premier temps, l'EICom les relèvera par le biais d'une auto-évaluation dans le cadre d'un sondage basé sur l'outil d'évaluation OFAE. Les auto-évaluations soumises devront être confirmées par une lettre de leur direction. Cette enquête sera réalisée chaque année auprès de toutes les entreprises concernées selon l'OAPEI révisée. Ce questionnaire permet à l'EICom d'établir une vue d'ensemble de la réalisation des exigences légales, ainsi que de recueillir et d'évaluer des informations sur l'état des mesures de cybersécurité.

Entretiens de sensibilisation

- (5) Les entretiens de sensibilisation sont menés en premier lieu avec des entreprises particulièrement importantes pour l'exploitation sûre et stable du réseau électrique suisse. En complément, des entretiens de sensibilisation sont également possibles sur la base des réponses reçues dans les questionnaires ou sur la base d'un échantillon aléatoire. L'objectif de ces entretiens est de recueillir des informations concrètes sur la mise en œuvre des mesures de cybersécurité et de compléter ainsi qualitativement les résultats de l'enquête. Les entretiens de sensibilisation ont lieu régulièrement sur place auprès des entreprises concernées. Les conclusions de ces entretiens constituent une base pour l'évaluation de la cybersécurité au sein de l'entreprise et pour en déduire d'éventuelles recommandations concernant des mesures à prendre. Leur mise en œuvre peut être vérifiée lors des entretiens de sensibilisation ultérieurs.

Audits

- (6) Comme troisième instrument de surveillance, l'EICom peut procéder à des audits individuels. Ceux-ci visent à approfondir certains aspects techniques sur la base d'anomalies constatées dans le questionnaire ou lors d'entretiens de sensibilisation. De même, des audits peuvent être réalisés sur la base d'indications externes ou d'un échantillon aléatoire. Selon le but et l'objectif, ces audits peuvent être réalisés par l'EICom ou par un auditeur externe.

Transition vers les exigences minimales de l'OAPEI

- (7) L'OAPEI révisée ne prévoit pas de délai transitoire pour atteindre les valeurs cibles minimales exigées. Afin que les auto-évaluations issues de l'enquête auprès des entreprises reflètent le mieux possible la situation actuelle, l'EICom autorise un délai transitoire, de 24 mois au maximum après l'entrée en vigueur de l'OAPEI révisée, pour prouver que les valeurs cibles exigées ont été atteintes. Pour les catégories dans lesquelles les valeurs cibles n'ont pas été atteintes, un plan de mesures et de mise en œuvre validé par la direction doit être présenté avec des objectifs de mise en œuvre concrets et contraignants. Si, de l'avis de l'EICom, les mesures qui y sont proposées ne sont pas mises en œuvre dans les délais, l'EICom



cherche à discuter avec les entreprises concernées. S'il existe des raisons compréhensibles pour lesquelles les valeurs cibles n'ont pas pu être atteintes dans le délai transitoire, l'ECom peut exceptionnellement accorder un délai supplémentaire.

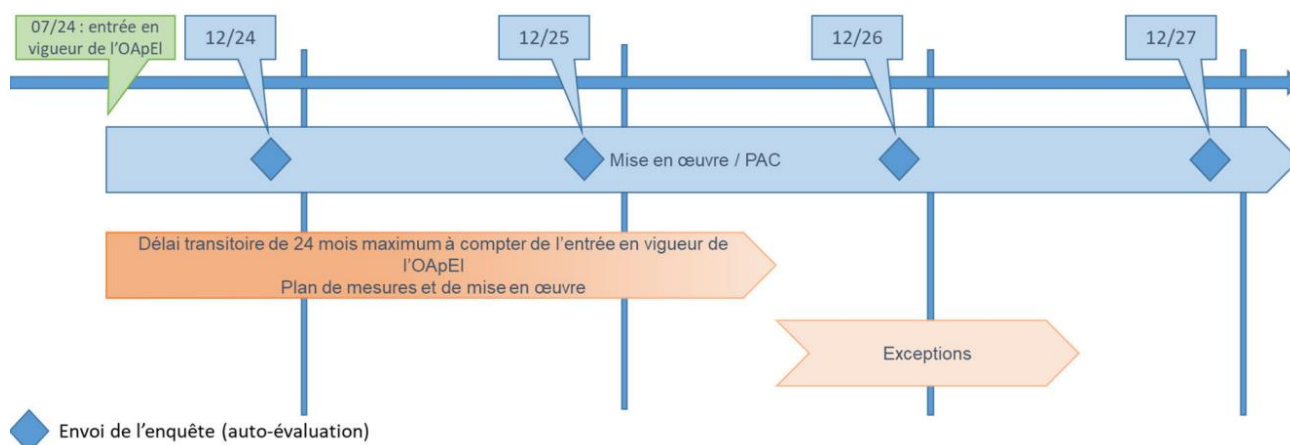


Figure 7: Schéma de déroulement de la mise en œuvre des exigences minimales de cybersécurité (source ECom)



En vertu de sa compétence générale subsidiaire (art. 22, al. 1 LApEI), l'ECom surveille la procédure et les résultats des activités visant à augmenter la résilience des TIC, de même que le respect des articles 8a LApEI et 5a OApEI.

3.3.8 Office fédéral de la cybersécurité (BACS): obligation de signalement et aide



(1) L'Office fédéral de la cybersécurité (OFCS) est le centre de compétences de la Confédération en matière de cybersécurité et donc le premier point de contact pour l'économie, l'administration, les établissements d'enseignement et la population en ce qui concerne les questions cybernétiques. Il est responsable de la mise en œuvre coordonnée de la stratégie nationale de cybersécurité (SNC).

3.3.8.1 Obligation de déclaration pour les infrastructures critiques

- (2) Les cyberattaques réussies peuvent avoir des conséquences importantes pour la disponibilité et la sécurité de l'économie suisse. La population, les autorités et les entreprises sont exposées quotidiennement au risque de cyberattaque. Aujourd'hui, il manque une vue d'ensemble des attaques qui ont eu lieu ainsi que leur localisation, car les déclarations à l'OFCS ne se font que sur une base volontaire. Grâce à une obligation de déclaration, l'OFCS aura à l'avenir une meilleure vue d'ensemble des cyberattaques survenues en Suisse et des modes opératoires des agresseurs. Il sera ainsi possible de mieux évaluer la menace et d'avertir à temps les exploitants d'infrastructures critiques. Par cette obligation de déclaration, le Conseil fédéral veut s'assurer que tous les exploitants d'infrastructures critiques participent à l'échange d'informations et contribuent ainsi à un signalement précoce.

3.3.8.2 Obligation de la Confédération de fournir une assistance en cas de cyberattaque

- (1) Le projet de loi oblige non seulement les entreprises à participer à la protection contre les cyberattaques, mais également l'OFCS, de fournir aux déclarants une assistance subsidiaire pour réagir aux cyberattaques.



3.4 Institutions, cadres, normes, standards, spécifications et lignes directrices pour améliorer la résilience des TIC.

- (1) Ce chapitre décrit de manière synthétique les institutions, les *frameworks*, les normes, les standards et la spécification dans le cadre de ce guide sur l'amélioration de la résilience des TIC. Ces descriptions donnent un aperçu général. Pour augmenter la résilience des TIC, il est recommandé de s'orienter vers des *frameworks*, des normes, des standards et des spécifications actuels, établis et introduits, publiés par des organisations et des institutions reconnues. De nombreuses normes, standards et spécifications servent d'aide à la mise en œuvre. Souvent, les publications ne présentent pas d'exemples d'application, elles servent uniquement à orienter, à définir des mesures et à aider à trouver des solutions.

3.4.1 Frameworks, normes, standards et spécifications

- (1) Les *frameworks*, normes, standards et spécifications jouent un rôle clé dans l'augmentation de la résilience des TIC en fournissant des structures et des directives claires pour la sécurité des technologies de l'information et de la communication. Ces modèles établis servent de points de référence pour définir les bonnes pratiques, identifier les risques et mettre en œuvre des mesures de protection.
- (2) Des cadres tels que ISO/IEC 27001 offrent une structure globale pour la gestion de la sécurité de l'information, tandis que des cadres tels que le NIST Cybersecurity Framework fournissent des étapes et des tâches concrètes pour la réduction des risques. Les normes et les spécifications établissent des critères généralement reconnus pour la sécurité des systèmes TIC, ce qui donne aux entreprises et aux unités organisationnelles une base claire pour leur stratégie de sécurité.
- (3) L'intérêt n'est pas seulement de définir des exigences minimales, mais aussi de promouvoir l'interopérabilité et la comparabilité. L'application de normes communes facilite le partage des bonnes pratiques, l'échange d'expériences et le renforcement de la coopération au sein de la communauté de la sécurité.
- (4) En outre, ces *frameworks*, normes et standards standardisés servent de base aux certifications et aux évaluations, ce qui permet aux entreprises et aux unités organisationnelles d'améliorer leur résilience TIC de manière démontrable. Ils offrent des critères clairs pour l'évaluation des pratiques de sécurité et soutiennent l'amélioration continue des mesures de sécurité.
- (5) Dans l'ensemble, les cadres, normes, standards et spécifications contribuent à renforcer la sécurité et la résilience des systèmes TIC au niveau mondial. Ils offrent un cadre de référence commun qui permet aux entreprises et aux unités organisationnelles de réagir systématiquement aux menaces et de rendre leur infrastructure TIC durablement plus résistante.



Les experts de la Task Force Cyber Security de l'AES recommandent d'appliquer les *frameworks*, normes, standards et spécifications qui sont reconnus et actuels.



Vous trouverez en annexe une liste détaillée des normes, standards et spécifications des *frameworks*.



La liste en annexe n'est pas exhaustive. Seuls les éléments ayant un lien direct avec ce guide ont été mentionnés. Il existe d'autres documents qui peuvent être utilisés pour augmenter la résilience des TIC.



Les outils, *frameworks*, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

3.4.2 Guidelines et publications spéciales

- (1) Les guides et les publications spécifiques contribuent de manière significative à l'augmentation de la résilience des TIC en fournissant des directives claires, des bonnes pratiques et des recommandations spécifiques pour la sécurité et la résilience des technologies de l'information et de la communication. Ces ressources servent de guides précieux pour les entreprises et les unités organisationnelles afin d'identifier les risques potentiels, de mettre en œuvre des mesures de protection appropriées et de réagir de manière adéquate aux menaces actuelles.



- (2) Les Guidelines fournissent des instructions pratiques pour l'élaboration de politiques de sécurité, la mise en œuvre de mécanismes de protection et la formation des employés. Ils aident à créer une base solide pour une stratégie de sécurité TIC complète. Des publications spécifiques abordent souvent plus en détail certains aspects et technologies de sécurité, ce qui permet aux entreprises et aux unités organisationnelles de se préparer spécifiquement aux menaces pertinentes.
- (3) En outre, les guides et les publications contribuent à communiquer l'état actuel des connaissances dans le paysage de la sécurité des TIC, qui évolue rapidement. Ils aident les entreprises et les unités organisationnelles à rester à jour en communiquant les approches innovantes, les menaces actuelles et les bonnes pratiques. Cela favorise une attitude proactive face aux nouveaux défis.
- (4) La communication claire des approches des meilleures pratiques et des recommandations dans ces ressources aide les entreprises et les unités organisationnelles à établir une culture de sécurité robuste et à garantir que toutes les parties prenantes, de la direction aux employés, développent une compréhension commune de l'importance de la résilience des TIC. Dans l'ensemble, les guides et les publications spécifiques contribuent à renforcer la résilience des systèmes TIC et à améliorer la capacité des entreprises et des unités organisationnelles à réagir de manière appropriée aux menaces potentielles.

Les guidelines et publications spéciales suivantes sont utilisées dans ce guide ou sont également utiles à la vue de l'AES:



- Livre blanc BDEW-OE-VSE: Exigences pour des systèmes de commande et de télécommunication sécurisés
- NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security
- AES ICT Continuity
- Manuel de l'AES Protection de base pour les «technologies opérationnelles» (OT) dans l'approvisionnement en électricité
- AES Sécurité physique pour les sous-stations (SPS – CH 2019)
- VSE Business Continuity & Disaster Recovery
- AES Contrôle de sécurité des personnes
- «Politique de données dans la branche énergétique», AES 2022



Les experts de la Task Force Cyber Security de l'AES recommandent d'appliquer les cadres, normes, standards et spécifications en vigueur et actuels.



La liste de cette section n'est pas exhaustive. Seuls les éléments ayant un lien direct avec ce guide ont été mentionnés. Il existe d'innombrables autres documents qui peuvent être utilisés pour augmenter la résilience des TIC.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

3.5 Certifications et formations pour accroître la résilience des TIC

- (1) Les certifications et les formations continues jouent un rôle décisif dans l'augmentation de la résilience des TIC dans les entreprises et les unités organisationnelles. Nous vous expliquons pourquoi ci-après:
 - **Expertise et qualification:** des experts certifiés et des employés bien formés disposent de l'expertise nécessaire pour mettre en œuvre des mesures efficaces en matière de cybersécurité et de résilience des TIC. Cela contribue à réduire la probabilité d'incidents de sécurité et à améliorer la capacité de réaction en cas d'urgence.
 - **Mise à jour des connaissances:** la technologie et le paysage des menaces sont en constante évolution. Grâce à la formation continue et à la certification, les professionnels restent à la pointe des connaissances et sont mieux à même de s'adapter aux exigences en constante évolution.
 - **Mise en œuvre des meilleures pratiques:** les programmes de certification sont souvent basés sur les meilleures pratiques et les normes développées par des experts. Ils fournissent des lignes directrices claires pour la mise en œuvre de mesures de sécurité et pour garantir la résilience des TIC.
 - **Confiance et crédibilité:** les certifications sont un signe d'expertise et de professionnalisme. Les entreprises et les unités organisationnelles qui emploient des employés certifiés signalent à leurs clients et partenaires qu'elles prennent au sérieux la sécurité et la résilience de leurs systèmes TIC.



- **Réduction des risques:** grâce à des employés bien formés et à des experts certifiés, les entreprises peuvent identifier les points faibles, combler les failles de sécurité et prendre des mesures de réduction des risques afin de se protéger contre les cyberattaques et autres dangers liés aux TIC.
 - **Culture de la sécurité:** des employés bien formés dans le domaine de la sécurité TIC augmentent la compréhension des cybermenaces et la capacité à y réagir de manière correcte et appropriée. Cela permet à son tour à une entreprise et à une unité organisationnelle d'établir plus facilement une culture de sécurité vécue.
- (2) Dans l'ensemble, les certifications et les formations continues sont des outils essentiels pour renforcer la résilience des TIC et améliorer la capacité des entreprises et des unités organisationnelles à réagir de manière appropriée aux cybermenaces et aux défaillances techniques. Elles contribuent à garantir la sécurité, la stabilité et l'efficacité des systèmes TIC.

3.5.1 Formations initiales et continues avec certifications

3.5.1.1 Cybersécurité IT/OT de l'AES pour les ingénieurs système



(1) La numérisation et la cybersécurité sont des sujets stimulants pour toutes les entreprises et unités organisationnelles. Le cours modulaire pour les ingénieurs système traite de tous les aspects pertinents concernant l'IT/OT, les vulnérabilités, les fonctions de protection du réseau, la gestion des incidents et la sécurité du système. Il se base sur le manuel de l'AES «Protection de base pour les technologies opérationnelles (OT) dans l'approvisionnement en électricité».

(2) Une compréhension précise des enjeux est au cœur de la formation. Une vision détaillée du sujet est fournie. Le cours montre comment les cyber-risques dans l'infrastructure critique de l'approvisionnement en électricité peuvent être réduits à un niveau acceptable.



Recommandation des experts de la Task Force Cyber Security de l'AES:
il est recommandé de suivre la formation dans son intégralité.

3.5.1.2 Offre de formation de l'AES dans le cadre du guide

- (1) Des formations et des instructions dans le cadre de ce guide sont en cours de planification à l'AES. L'AES s'efforce de faire en sorte que les EAE puissent suivre les formations et les instructions nécessaires auprès de l'association pour augmenter la résilience des TIC et respecter les prescriptions légales en matière de cybersécurité.

3.5.1.3 Autres possibilités de formation et de perfectionnement

- (1) L'AES s'efforce de faire en sorte que les formations nécessaires soient disponibles pour ses membres dans une qualité, un volume et un contenu appropriés. Les EAE disposent ainsi d'un bagage optimal pour comprendre les exigences réglementaires et pouvoir mettre en œuvre les mesures nécessaires conformément au présent guide. L'offre de formation actuelle, pour les spécialistes du secteur de l'énergie qui répondent à ces exigences, est aujourd'hui minimale, voire inexistante. Il manque des formations spécifiques pour les responsables de la sécurité OT et les spécialistes, qui puissent transmettre le contenu de la formation nécessaire en fonction des groupes cibles.
- (2) Pour cette raison, l'AES introduit une liste de formations et de formations continues recommandées dans le domaine de la mise en œuvre de la norme minimale pour les TIC en mettant l'accent sur l'augmentation de la résilience des TIC dans la branche électrique. Les prestataires de cours, de formations et de formations continues ont la possibilité de demander à figurer sur cette liste. Les experts de la Task Force Cybersécurité de l'AES examineront les demandes selon des critères définis et donneront ensuite leur aval pour l'inscription sur la liste. Les cours, stages et formations/perfectionnements correspondants sont répertoriés par l'AES sur la «Liste des formations et perfectionnements recommandés en cybersécurité» et peuvent être consultés sur le site internet.





Il existe de nombreux cours, formations et formations continues dans le domaine de la cybersécurité, qui ne sont que partiellement adaptés au domaine de la mise en œuvre de la norme minimale pour les TIC axée sur l'amélioration de la résilience TIC dans le secteur de l'électricité ou qui ne fournissent pas le savoir-faire nécessaire à cet effet. Une grande prudence est donc de mise dans le choix des cours, des formations et des formations continues. Souvent, on exploite l'ignorance des personnes qui ont besoin de telles formations.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Seuls les cours, stages, formations et formations continues figurant sur la «Liste AES des formations/formations continues recommandées en matière de cybersécurité» dans le domaine de la mise en œuvre de la norme minimale pour les TIC avec focalisation sur l'augmentation de la résilience TIC dans la branche électrique doivent être suivis.

3.5.2 Certifications de sécurité pour les entreprises et les unités organisationnelles

3.5.2.1 Certification de l'ISMS selon la norme ISO 27001

- (1) La certification ISO 27001 se réfère à un système de gestion de la sécurité de l'information (ISMS). Cette norme spécifie les exigences pour l'établissement, la mise en œuvre, le maintien et l'amélioration continue d'un ISMS documenté au sein d'une organisation. Le processus comprend l'analyse du contexte et des risques, la définition du champ d'application, la mise en œuvre de mesures de sécurité, le suivi des performances et des évaluations régulières. La certification est effectuée par un organisme indépendant et atteste de la conformité de l'ISMS à la norme ISO 27001, ce qui indique une protection efficace des informations et des données.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

3.5.2.2 Certification de l'application du cadre de cybersécurité du NIST

- (1) La certification pour l'application du NIST Cyber Security Framework ne se fait pas directement par un organisme de certification standardisé, comme c'est le cas pour certaines autres normes (par ex. ISO 27001). Le Cyber Security Framework (CSF) NIST est un cadre avec des tâches et non une norme de certification avec des mesures concrètes. Les entreprises et les unités organisationnelles peuvent toutefois démontrer leur conformité au cadre de différentes manières:
 - **Auto-évaluation:** les entreprises et les unités organisationnelles peuvent procéder à une auto-évaluation afin de vérifier avec quelle maturité leur entreprise et leurs unités organisationnelles satisfont aux catégories ou sous-catégories du CSF NIST.
 - **Audits de tiers:** les entreprises et les unités organisationnelles peuvent demander à des prestataires de services de sécurité ou à des auditeurs externes de vérifier leurs pratiques de sécurité par rapport au CSF NIST et de formuler des recommandations appropriées.
 - **Exigences spécifiques à certains secteurs:** dans certains secteurs, il existe des prescriptions ou des règlements spécifiques en matière de cybersécurité. Le respect de ces réglementations peut servir de preuve indirecte pour l'application du CSF NIST.
 - **Confirmation par les fournisseurs ou les partenaires:** les entreprises et les unités organisationnelles peuvent demander à leurs fournisseurs ou partenaires de prouver qu'ils ont mis en œuvre leurs pratiques de sécurité conformément au CSF NIST.
- (2) En lui-même, le NIST encourage les entreprises et les unités organisationnelles à adapter et à mettre en œuvre le cadre afin de répondre aux besoins et aux risques individuels. Par conséquent, dans ce contexte, la certification peut être axée sur l'efficacité et la maturité des pratiques de sécurité d'une entreprise et des unités organisationnelles conformément au CSF NIST, plutôt que sur une certification formelle et normalisée.



En collaboration avec les organismes de certification nationaux officiels, l'OFAE s'efforce de proposer à l'avenir une certification pour l'application du NIST Cyber Security Framework.



4. Base de l'efficacité pour améliorer la résilience des TIC

4.1 Le système de gestion intégré SGI



Figure 8: Système de gestion intégré SGI (Source TÜV Süd)

(1) Le système de gestion intégré (SGI) sert de cadre global pour accroître la résilience des technologies de l'information et de la communication (TIC). L'utilisation d'un SGI dans ce contexte vise à créer une approche holistique et coordonnée de la gestion des ressources TIC afin de répondre efficacement aux défis, aux menaces et aux perturbations. Voici différents aspects qui englobent l'utilisation du SGI pour accroître la résilience des TIC:

- **Intégration de systèmes de gestion:** le SGI intègre différents systèmes de gestion, tels que la gestion de la qualité (ISO 9001), la gestion de l'environnement (ISO 14001), la gestion de la sécurité de l'information (ISO 27001) et les systèmes de gestion de la sécurité et de la santé au travail (ISO 45001). Cette intégration permet une gestion cohérente et efficace des ressources TIC en reliant différents aspects de l'organisation.
 - **Gestion des risques:** le SGI permet une gestion intégrée des risques pour les TIC. Les risques liés à la sécurité, à la conformité, à l'impact environnemental et à la qualité peuvent être analysés et évalués. Cela permet d'identifier de manière proactive les risques pour les TIC et de mettre en œuvre des mesures de réduction des risques.
 - **Amélioration continue:** grâce au cycle PDCA (Plan-Do-Check-Act), le SGI favorise une culture d'amélioration continue. Cela est essentiel pour renforcer la résilience des TIC à long terme. Les entreprises et les unités organisationnelles peuvent optimiser en permanence leurs processus et leurs mesures sur la base des expériences et des changements dans le paysage des menaces.
 - **Gestion des urgences et de la continuité:** le SGI permet d'intégrer les processus de gestion des urgences et de la continuité dans tous les systèmes de gestion d'une entreprise et des unités organisationnelles. Cela comprend l'élaboration de plans d'urgence, le contrôle régulier de l'efficacité de ces plans et la formation du personnel à la gestion des incidents liés aux TIC ou à la sécurité.
 - **Approche globale:** le SGI favorise une approche globale de la gestion des TIC. Il prend en compte non seulement les aspects technologiques, mais aussi les facteurs organisationnels et humains. Cette approche est essentielle pour améliorer la résilience des TIC dans un contexte global.
 - **Gestion de la conformité:** l'intégration de la gestion de la conformité dans le SGI permet de garantir que les ressources TIC sont conformes aux réglementations en vigueur. Ceci est important pour répondre aux exigences légales dans le domaine de la sécurité des TIC et renforcer ainsi la résilience.
 - **Formation et sensibilisation:** le SGI soutient les programmes de formation et de sensibilisation du personnel à l'utilisation des ressources TIC. Un personnel bien informé et formé contribue largement à renforcer la résilience des TIC.
- (2) En résumé, l'utilisation du SGI comme base pour accroître la résilience des TIC offre une approche structurée et intégrée permettant de répondre aux défis et aux perturbations tout en garantissant des performances durables des TIC.



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'introduction d'un système de gestion intégré (SGI) offre une approche structurée et globale qui constitue une base incontournable pour accroître la résilience des TIC. Il est donc recommandé d'utiliser un SGI ou une structure similaire.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.





Ce guide se base sur les principes d'un système de gestion intégré (SGI). Il ne traite toutefois en premier lieu que des domaines de la sécurité de l'information. Ceci à l'aide de la mise en place et de la réalisation d'un système de gestion de la sécurité de l'information (ISMS). Les liens avec d'autres systèmes de gestion sont traités ponctuellement et mis en évidence lorsque cela est nécessaire.

4.2 La gestion de la sécurité de l'information (GSI) comme base pour accroître la résilience des TIC

- (1) L'application de la gestion de la sécurité de l'information (GSI) en tant que base pour accroître la résilience des technologies de l'information et de la communication (TIC) joue un rôle crucial dans l'environnement moderne des entreprises. La GIS est une approche globale qui vise à garantir la sécurité, l'intégrité et la disponibilité des informations. Dans le contexte de la résilience des TIC, la GIS contribue à différents aspects clés:
- (2) La GSI permet d'identifier et d'évaluer systématiquement les risques pour la sécurité de l'information. L'analyse des menaces et des vulnérabilités permet de prendre des mesures préventives afin de minimiser l'impact potentiel sur les TIC.
- (3) L'élaboration de plans et de processus d'urgence fait partie intégrante de la GSI. Ceux-ci garantissent une réaction structurée aux incidents de sécurité et aux perturbations des TIC. Les plans d'urgence garantissent que l'organisation est en mesure de réagir rapidement et efficacement aux situations de crise.
- (4) La GSI encourage une surveillance et une amélioration continues des processus de sécurité grâce au cycle PDCA (*Plan Do Check Act*). L'identification des faiblesses permet de prendre des mesures appropriées afin de renforcer continuellement la résilience des TIC.
- (5) La GSI veille à ce que les objectifs de sécurité soient en phase avec les objectifs commerciaux globaux. Cela garantit que la résilience des TIC contribue directement à la continuité des activités et soutient les objectifs stratégiques de l'entreprise.
- (6) La GSI soutient les programmes de formation et de sensibilisation des employés à la sécurité de l'information. Des employés bien informés sont essentiels au maintien de la résilience des TIC.
- (7) La GSI encourage la communication et la collaboration entre les différents services et parties prenantes. Une approche coordonnée est essentielle pour garantir une réponse efficace aux incidents de sécurité et renforcer la résilience des TIC.
- (8) La GSI facilite le respect des exigences de conformité et des dispositions légales dans le domaine de la sécurité de l'information. Cela minimise les risques juridiques et renforce la résilience des TIC face aux défis réglementaires.
- (9) Grâce à la mise en œuvre de systèmes de surveillance et d'alerte précoce, l'ISM peut identifier les menaces potentielles à un stade précoce. Cela permet de réagir de manière proactive afin de minimiser les dommages et de renforcer la résilience des TIC.
- (10) En résumé, la GSI propose une méthodologie structurée pour accroître la résilience des TIC. Elle se concentre sur les mesures préventives, la planification d'urgence, l'amélioration continue et le respect des normes afin de créer un environnement TIC robuste et résistant.



La gestion de la sécurité de l'information (GSI) peut être opérationnalisée et exploitée à l'aide d'un système de gestion de la sécurité de l'information (ISMS). Ce guide décrit en 8 phases la mise en place et l'exploitation d'un ISMS selon la norme ISO27001.



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'introduction de la gestion de la sécurité de l'information (GSI) offre une approche structurée et globale qui permet d'augmenter la résilience des TIC. Il est donc recommandé d'introduire une GIS.

4.3 Système de gestion de la sécurité et de la santé au travail pour soutenir l'augmentation de la résilience des TIC

- (1) Le système de gestion de la sécurité et de la santé au travail offre un soutien important pour accroître la résilience des technologies de l'information et de la communication (TIC). Ce système de gestion établit un cadre structuré pour garantir la sécurité et la santé des employés sur le lieu de travail, ce qui contribue à son tour à renforcer la résilience des TIC.
- (2) Un aspect central du système de gestion de la sécurité et de la santé au travail est l'identification et l'évaluation systématiques des risques liés à la sécurité et à la santé au travail. Cela inclut non seulement les



risques physiques sur le lieu de travail, mais aussi les dangers potentiels dans le domaine des TIC. L'analyse des processus, des environnements et des conditions de travail permet d'identifier les points faibles potentiels qui pourraient avoir une incidence sur les TIC.

- (3) Le système de gestion encourage également le développement de politiques et de procédures claires pour les situations d'urgence et la gestion des urgences. Cela est essentiel pour pouvoir réagir de manière appropriée aux événements imprévus ou aux incidents de sécurité dans le domaine des TIC. Un plan d'urgence bien élaboré permet de prendre rapidement des mesures et de minimiser l'impact des perturbations.
- (4) Le système de gestion aide également à intégrer les aspects de sécurité et de santé dans la planification et la mise en œuvre des stratégies TIC. Cela contribue à garantir que les considérations de sécurité sont intégrées dès le début dans le développement et la mise en œuvre des systèmes TIC. Le lien entre la sécurité au travail et la sécurité des TIC est ainsi renforcé.
- (5) En outre, le système de gestion accorde une grande importance à l'amélioration continue des mesures de sécurité et de santé. Cette approche permet aux entreprises et aux unités organisationnelles non seulement de réagir aux risques actuels, mais aussi de prendre des mesures proactives afin de renforcer la résilience des TIC à long terme. Des vérifications et des adaptations régulières permettent de réagir à l'évolution des menaces dans le paysage TIC.
- (6) La formation et les programmes de sensibilisation du personnel, encouragés par la norme ISO 45001, jouent un rôle important dans le renforcement de la résilience des TIC. Des employés bien informés et formés sont mieux à même de comprendre et de mettre en œuvre les aspects liés à la sécurité en ce qui concerne les TIC.
- (7) En résumé, la norme ISO 45001, en tant que système de gestion de la sécurité et de la santé au travail, offre une approche holistique qui non seulement protège la santé physique des employés, mais contribue également à renforcer la résistance et la résilience de l'infrastructure TIC. Cela passe par une évaluation systématique des risques, des directives claires en cas d'urgence, l'intégration des aspects de sécurité dans les stratégies TIC, l'amélioration continue et la formation des employés.



Ce guide n'aborde pas entièrement le système de gestion de la sécurité et de la santé au travail. Seuls les éléments qui contribuent à l'écoute de la résilience des TIC sont utilisés et décrits.



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'introduction d'un système de gestion de la sécurité et de la santé au travail devrait être mise en place et exploitée par les entreprises et les unités organisationnelles. Ce système aide les entreprises et les unités organisationnelles à accroître leur résilience aux TIC.

4.4 Gestion des processus, des risques, de la continuité des activités et des urgences comme bases supplémentaires pour augmenter la résilience des TIC



La gestion des processus, des risques, de la continuité des activités et des urgences constitue d'autres piliers importants pour accroître la résilience des TIC. Ce sont des outils puissants et complets pour une gestion solide et efficace de l'entreprise et des unités organisationnelles. Ils fournissent des directives et des éléments importants pour l'efficacité de l'amélioration de la résilience des TIC. La description, l'introduction et l'exploitation de ces systèmes de gestion de base ne sont abordées que de manière limitée dans ce guide.

4.4.1 Gestion des processus

- (1) La gestion des processus se réfère à la planification systématique, à la conception, à la mise en œuvre, au suivi et à l'amélioration continue des processus commerciaux au sein d'une organisation. Les processus commerciaux sont des opérations répétitives et structurées qui se produisent dans les entreprises et les unités organisationnelles afin d'atteindre des objectifs spécifiques, tels que la fourniture de produits ou de services, l'optimisation des flux de travail ou la satisfaction des exigences des clients.
- (2) La gestion des processus vise à rendre ces processus plus efficaces, plus efficaces et plus orientés vers le client. Voici quelques aspects importants de la gestion des processus:
 - **Identification des processus:** il faut d'abord identifier les processus au sein d'une organisation. Cela implique de reconnaître quels processus ont lieu, comment ils sont structurés et qui en est responsable.



- **Conception des processus:** une fois identifiés, les processus sont analysés et, le cas échéant, reconçus. L'objectif est d'optimiser les processus de manière à ce qu'ils fournissent les résultats souhaités de manière efficiente et efficace.
 - **Mise en œuvre des processus:** les processus révisés sont mis en œuvre dans les entreprises et les unités organisationnelles. Cela implique l'utilisation d'indicateurs de performance (KPI) et de systèmes de reporting.
 - **Surveillance des processus:** les processus sont surveillés en permanence afin de s'assurer qu'ils se déroulent correctement et qu'ils produisent les résultats souhaités. Cela implique l'utilisation d'indicateurs de performance (KPI) et de systèmes de reporting.
 - **Contrôle des processus:** si nécessaire, des mesures sont prises pour adapter les processus ou résoudre les problèmes. Cela peut inclure l'adaptation des ressources, la formation ou d'autres mesures d'amélioration des processus.
 - **Optimisation des processus:** la gestion des processus vise une amélioration continue. Les entreprises et les unités organisationnelles cherchent constamment des moyens de rendre les processus plus efficaces et plus efficaces. Cela peut être réalisé en utilisant les méthodes Lean, Six Sigma, Total Quality Management (TQM) et d'autres méthodes d'optimisation des processus.
 - **Orientation client:** la gestion des processus met fortement l'accent sur les exigences des clients. La conception et l'amélioration des processus visent à augmenter la satisfaction des clients et à répondre à leurs besoins et attentes.
- (3) La gestion des processus est essentielle, car elle peut contribuer à accroître l'efficacité, à réduire les coûts, à améliorer la qualité et à accroître la compétitivité. Il s'agit d'un processus continu qui nécessite de s'adapter aux conditions changeantes et de tenir compte des commentaires des clients.

4.4.2 Gestion des risques

- (1) La gestion des risques est un processus systématique d'identification, d'analyse, d'évaluation, de maîtrise ainsi que de communication et de surveillance des risques pouvant affecter une entreprise et ses unités organisationnelles. L'objectif principal de la gestion des risques est de minimiser ou de contrôler les risques afin de réduire la probabilité d'événements négatifs tout en saisissant les opportunités pour atteindre les objectifs de l'entreprise. Voici les étapes et les principes de base de la gestion des risques:
- **Identification des risques:** cette étape consiste à identifier tous les risques potentiels qui peuvent affecter une organisation. Cela comprend les risques internes et externes, tels que les risques financiers, les risques opérationnels, les risques juridiques, les risques technologiques ou les risques liés à la concurrence.
 - **Évaluation des risques:** une fois les risques identifiés, ils sont évalués afin de déterminer leur impact et leur probabilité d'occurrence. Cela permet de classer les risques par ordre de priorité et de décider sur quels risques l'organisation doit concentrer son attention.
 - **Gestion des risques:** après l'évaluation des risques, des stratégies de traitement des risques sont élaborées. Il existe différentes manières de traiter les risques, notamment:
 - Éviter les risques: prendre des mesures pour éliminer complètement le risque.
 - Réduction des risques: prendre des mesures pour réduire la probabilité d'occurrence ou l'impact d'un risque.
 - Transfert du risque: le risque est transféré à des tiers, tels que des compagnies d'assurance ou des partenaires contractuels.
 - Acceptation du risque: le risque est accepté en connaissance de cause, par exemple lorsque le coût du traitement du risque est plus élevé que le dommage potentiel.
 - **Contrôle des risques:** mise en œuvre de mesures et de contrôles afin de garantir que les stratégies de gestion des risques définies sont effectivement appliquées. Cela comprend la surveillance des risques en cours d'exploitation, la vérification des processus et l'adaptation des mesures si nécessaire.
 - **Communication des risques:** communiquer efficacement les risques et les stratégies de gestion des risques au sein de l'organisation et aux parties prenantes telles que les clients, les investisseurs et les autorités de réglementation.



- **Rapports sur les risques:** rapports réguliers sur l'état du traitement des risques et sur les progrès réalisés dans la mise en œuvre des mesures.
 - **Culture du risque:** créer une culture d'entreprise dans laquelle la gestion des risques joue un rôle important et dans laquelle les employés comprennent l'importance de la réduction et du contrôle des risques.
 - **Suivi et évaluation:** suivi permanent du paysage des risques et évaluation de l'efficacité des stratégies de gestion des risques.
- (2) La gestion des risques est essentielle dans les entreprises et les unités organisationnelles de toutes tailles et de tous secteurs, car elle contribue à minimiser les pertes financières, à maintenir les activités commerciales et à garantir la stabilité et la durabilité à long terme. Il s'agit d'un processus continu qui doit s'adapter à l'évolution des risques et des conditions afin de garantir que l'organisation puisse faire face avec succès aux incertitudes.



En tant qu'exploitant d'infrastructures critiques, l'identification et l'évaluation des risques doivent être effectuées non seulement du point de vue d'une gestion sûre des affaires, mais aussi du point de vue des infrastructures critiques et de leur impact sur la société suisse.



Références à des documents complémentaires:

- NIST Risk Management Framework
- ISO 31000:2018 - Risk management
- Norme BSI 200-3

4.4.3 Gestion de la continuité des activités (BCM)

- (1) La gestion de la continuité des activités (BCM ou Business Continuity Management) est une approche globale de planification et de préparation aux perturbations, aux crises et aux catastrophes afin d'assurer la continuité des activités et la résilience d'une organisation. Dans le contexte de l'augmentation de la résilience des TIC, le BCM joue un rôle crucial, car les technologies de l'information et de la communication (TIC) constituent souvent l'épine dorsale des processus commerciaux modernes. Le BCM et la résilience TIC sont étroitement liés et l'intégration de la résilience TIC dans le BCM est d'une grande importance. Voici quelques aspects importants du BCM en rapport avec la résilience TIC:
- **Évaluation et identification des risques:** le BCM commence par l'identification et l'évaluation des risques qui pourraient mettre en danger l'infrastructure et les systèmes TIC d'une organisation. Cela comprend les menaces telles que les cyberattaques, les catastrophes naturelles, les défaillances techniques et les erreurs humaines.
 - **Analyse d'impact sur les activités (BIA):** dans le cadre du BCM, une analyse d'impact sur les activités est effectuée afin de comprendre les effets des perturbations sur les processus commerciaux. Cela implique d'identifier les systèmes et applications TIC critiques dont la défaillance pourrait avoir des répercussions importantes sur l'entreprise.
 - **Plans d'urgence et de récupération:** sur la base de l'évaluation des risques et de la BIA, l'organisation développe des plans d'urgence et de récupération pour ses systèmes TIC. Ces plans contiennent des étapes et des procédures visant à maintenir la continuité des activités et à restaurer les systèmes TIC en cas de défaillance.
 - **Tests et exercices:** le BCM comprend des tests et des exercices réguliers afin de s'assurer que les plans d'urgence et de récupération sont efficaces. Cela inclut des tests de restauration des systèmes TIC et des simulations de scénarios d'urgence et de crise.
 - **Formation et sensibilisation:** les employés et le personnel informatique sont formés à leur rôle dans le BCM et la récupération des systèmes TIC, afin de s'assurer qu'ils peuvent réagir de manière appropriée en cas d'urgence.
 - **Réponse aux incidents:** le BCM comprend des procédures claires de réponse aux incidents, qui définissent comment réagir aux incidents de sécurité et aux perturbations des systèmes TIC.
 - **Surveillance et adaptation:** le BCM nécessite une surveillance continue des mesures de résilience des TIC et une adaptation aux nouvelles menaces, technologies et exigences commerciales.



- **Intégration de la résilience des TIC:** le BCM et la résilience des TIC doivent être mutuellement intégrées de manière transparente. Cela signifie que la sécurité et la résilience des systèmes TIC doivent être intégrées dans l'ensemble du processus BCM.
- (2) L'intégration de la résilience des TIC dans le BCM est essentielle, car les TIC jouent un rôle central dans de nombreuses entreprises et unités organisationnelles. Une panne ou un dysfonctionnement des systèmes TIC peut avoir un impact considérable sur la continuité de l'activité et la capacité à fournir des services. En prenant en compte la résilience des TIC dans le BCM, les entreprises et les unités organisationnelles peuvent s'assurer qu'elles peuvent réagir efficacement aux risques liés aux TIC et augmenter leur résilience en cas de perturbation.



Références à des documents complémentaires:

- Norme BSI 200-4
- ISO 22301: Business Continuity Management
- NIST SP 800-34

4.4.3.1 Analyse d'impact sur les activités (BIA)

- (1) L'analyse d'impact sur les activités (BIA) est une étape importante dans l'amélioration de la résilience des TIC dans le cadre d'une gestion globale des risques. La BIA est un processus par lequel les entreprises et les unités organisationnelles analysent et évaluent l'impact potentiel des perturbations et des pannes TIC sur leurs processus et fonctions commerciales. Elle aide à identifier les composants et les applications TIC critiques et à déterminer comment les perturbations dans ces domaines pourraient affecter la continuité des activités. Dans le contexte de l'augmentation de la résilience des TIC, la BIA joue un rôle central:
- **Identification des composants TIC critiques:** la BIA aide à identifier les systèmes TIC, les applications et l'infrastructure qui sont essentiels au bon fonctionnement des processus d'entreprise et à la fourniture de services. Il s'agit par exemple des bases de données critiques, des systèmes de communication, des plateformes de commerce électronique ou des applications logicielles spécifiques.
 - **Évaluation de l'impact:** la BIA évalue l'impact potentiel des perturbations des TIC sur les processus et fonctions de l'entreprise. Il peut s'agir d'un impact financier, de la perte de clients, de conséquences juridiques, d'une atteinte à la réputation et plus encore.
 - **Hierarchisation de la restauration:** la BIA aide à hiérarchiser les systèmes et applications TIC qui doivent être restaurés en premier afin d'assurer la continuité des activités. Cela permet une allocation ciblée des ressources et des calendriers pour la restauration.
 - **Planification d'urgence et de récupération:** les résultats de la BIA sont intégrés dans les plans d'urgence et de récupération. Ils fournissent des instructions et des procédures claires pour la restauration des systèmes et applications TIC critiques afin de minimiser l'impact des perturbations.
 - **Évaluation des risques et amélioration:** la BIA aide à identifier les points faibles et les risques dans les systèmes TIC et permet de mettre en œuvre des mesures pour améliorer la résilience des TIC. Cela peut inclure l'implémentation de mesures de sécurité, la mise à jour des systèmes et l'introduction de systèmes redondants.
 - **Formation et sensibilisation:** les résultats de la BIA peuvent contribuer à l'élaboration de programmes de formation et de sensibilisation des employés afin de s'assurer qu'ils comprennent l'importance de la résilience des TIC et qu'ils sachent comment réagir en cas d'urgence.
- (2) La BIA est un outil essentiel pour garantir que les mesures de résilience des TIC soient ciblées et efficaces. En identifiant les composants TIC critiques et en évaluant leur impact sur les processus commerciaux, les entreprises et les unités organisationnelles peuvent investir de manière ciblée dans des mesures qui augmentent la résistance aux perturbations TIC. Cela contribue à garantir la continuité des activités et à mieux préparer l'organisation à la gestion des risques liés aux TIC.



Références à des documents complémentaires:

- Norme BSI 200-4
- ISO 22301: Business Continuity Management
- NIST SP 800-34



4.4.4 Gestion des situations d'urgence

- (1) La gestion des situations d'urgence joue un rôle crucial dans l'augmentation de la résilience des technologies de l'information et de la communication (TIC). Elle désigne le processus structuré par lequel les entreprises et les unités organisationnelles réagissent à des événements ou des perturbations imprévus, les gèrent et se rétablissent par la suite. Dans le contexte des TIC, une gestion efficace des situations d'urgence vise à minimiser l'impact des perturbations et à garantir que les systèmes TIC fonctionnent de manière optimale, même dans des circonstances défavorables.
- (2) Tout commence par l'élaboration d'un plan de gestion des situations d'urgence clair, qui définit la structure, les responsabilités et les procédures d'action. Ce plan doit être spécifiquement adapté à l'infrastructure TIC et prendre en compte différents scénarios, notamment les cyberattaques, les catastrophes naturelles, les pannes techniques ou d'autres incidents liés à la sécurité.
- (3) Une évaluation complète des risques constitue la base du plan de gestion des situations d'urgence. Il s'agit d'identifier les menaces potentielles pour les TIC et d'évaluer leur impact sur la continuité des activités. Cette analyse permet de développer des mesures ciblées afin de renforcer la résilience des TIC face aux risques identifiés.
- (4) Pendant une crise, une communication claire est essentielle. Le plan de gestion des situations d'urgence devrait établir des directives claires pour la communication interne et externe, tant au sein de l'organisation qu'avec les parties prenantes concernées. Cela contribue à minimiser les incertitudes et à optimiser l'efficacité de la réaction.
- (5) Un autre aspect important de la gestion des situations d'urgences est la mise en place d'équipes d'intervention d'urgence spécialement conçues pour gérer les perturbations dans le domaine des TIC. Ces équipes doivent non seulement disposer d'un savoir-faire technique, mais aussi être en mesure de collaborer efficacement et de prendre des décisions éclairées sous pression.
- (6) Des formations et des simulations régulières sont essentielles pour s'assurer que l'équipe de gestion des situations d'urgence est bien préparée. En jouant différents scénarios, il est possible d'identifier les points faibles du plan et d'y apporter des améliorations.
- (7) Le suivi d'une situation d'urgence est tout aussi important que la réaction immédiate. Une analyse complète des mesures prises, de l'efficacité de la gestion des situations d'urgence et des effets d'apprentissage obtenus conduit à des améliorations continues pour les événements futurs.
- (8) Dans l'ensemble, une gestion des situations d'urgence bien conçue contribue considérablement à accroître la résilience des TIC. Elle permet de gérer efficacement les perturbations, mais elle favorise aussi la capacité à se remettre des situations d'urgence et à en ressortir plus fort.



Références à des documents complémentaires:

- NIST SP 800-34 «Contingency Planning Guide for Information Technology Systems»
- Norme BSI 100-4 «Gestion des cas d'urgence»

4.5 Stratégie de cybersécurité selon le principe Defense in Depth

- (1) La stratégie de cybersécurité «Defense in Depth» (en français: défense en profondeur) est une approche qui vise à créer un système de défense complet et multicouche pour protéger les systèmes et les données TIC contre les cybermenaces. Cette stratégie part du principe qu'aucune mesure de sécurité unique n'est suffisante pour contrer toutes les menaces potentielles. Au lieu de cela, plusieurs niveaux de protection sont mis en œuvre afin de garantir une protection complète.
- (2) Voici les principaux composants et principes de la stratégie de cybersécurité de *Defense in Depth* pour accroître la résilience des TIC:
 - **Prévention:** la première couche de la défense se concentre sur la prévention des attaques. Cela comprend des mesures de sécurité telles que des pare-feux, des systèmes de détection/prévention d'intrusion (IDS/IPS), des logiciels antivirus et des configurations sécurisées des réseaux et des terminaux.
 - **Détection:** lorsque les mesures préventives échouent, la détection des incidents de sécurité est cruciale. Cela implique la mise en œuvre de systèmes de surveillance de la sécurité, de la journalisation et d'outils de gestion des informations et des événements de sécurité (SIEM) afin d'identifier les activités suspectes.



- **Réaction:** en cas de violation de la sécurité ou d'incident, une réaction rapide est essentielle. Cela implique la mise en place de plans d'urgence et la formation d'équipes de réponse aux incidents afin de réagir de manière appropriée aux incidents, de les isoler et de les éliminer.
 - **Authentification et contrôle d'accès:** l'accès aux systèmes et aux données doit être réservé aux utilisateurs autorisés. Pour ce faire, il convient de mettre en œuvre des méthodes d'authentification forte telles que l'authentification à deux facteurs (2FA) et d'utiliser des autorisations et des listes de contrôle d'accès.
 - **Sécurité du réseau:** les approches de sécurité basées sur les couches, telles que la segmentation du réseau, les VLAN et les zones de sécurité, aident à protéger le réseau contre les mouvements latéraux des attaquants.
 - **Sécurité des terminaux:** la sécurisation des terminaux tels que les ordinateurs, les smartphones et les appareils IoT est un élément essentiel de la stratégie de défense en profondeur. Cela comprend des mises à jour régulières des logiciels, des politiques de sécurité et des solutions de protection des points finaux.
 - **Cryptage:** le cryptage des données protège les informations aussi bien pendant la transmission qu'au repos. Cela est essentiel pour protéger les données contre tout accès non autorisé.
 - **Formation et sensibilisation:** un personnel bien informé est un facteur important pour la sécurité. Les formations et les campagnes de sensibilisation peuvent encourager les employés à agir en étant conscients de la sécurité et à reconnaître les attaques de phishing.
 - **Gestion des correctifs:** la mise à jour régulière des logiciels et des systèmes d'exploitation afin de combler les failles de sécurité connues est un mécanisme de protection essentiel.
 - **Surveillance et audit:** la surveillance permanente et les audits de sécurité et tests d'intrusion réguliers permettent d'identifier les failles de sécurité et d'y remédier.
- (3) La stratégie de défense en profondeur est flexible et peut être adaptée aux exigences et aux risques spécifiques d'une organisation. Elle souligne l'importance du fait qu'aucune mesure de sécurité ne suffit à elle seule pour lutter efficacement contre les cybermenaces de plus en plus complexes. Au lieu de cela, elle mise sur une combinaison de couches de protection pour garantir un niveau de sécurité plus élevé.



Références à des documents complémentaires:

- Protection de base AES pour l'OT dans l'approvisionnement en électricité
- NIST SP 800-82
- BSI ICS-Security-Kompendium



Le présent guide n'aborde pas plus en détail la stratégie de cybersécurité selon le principe de *Defense in Depth*. Vous trouverez suffisamment d'explications et de références dans d'autres documents.

5. Les bases pour augmenter la résilience des TIC



Dans ce chapitre, les experts de la Task Force Cyber Security de l'AES présentent les principes de base permettant d'accroître la résilience des TIC.

5.1 Compréhension fondamentale de la démarche

- (1) Il existe souvent un malentendu selon lequel les directives, les prescriptions, les normes, les standards, les cadres, etc. décrivent un mode d'emploi ou la solution pour la mise en œuvre de mesures visant à accroître la résilience des TIC. Or, dans la plupart des cas, ce n'est pas le cas. Souvent, seuls sont décrits les contrôles et les tâches qui doivent être considérés ou pris en compte dans les différents domaines et points pour améliorer la résilience des TIC. Chaque entreprise et chaque unité organisationnelle doit analyser, développer et mettre en œuvre de manière autonome les solutions proprement dites et les mesures effectives pour l'exécution.
- (2) Ces documents contiennent souvent des instructions et des exemples d'application qui aident les entreprises et les unités organisationnelles à trouver des solutions et à les mettre en œuvre. Il s'agit



généralement d'exemples pratiques spécifiques qui ne peuvent pas être appliqués tels quels dans les entreprises et unités organisationnelles concernées.



Les directives, prescriptions, normes et standards, frameworks, etc. ne sont pas des instructions et ne contiennent pas d'exemples d'application pouvant être mis en œuvre 1:1. Ils ne contiennent que des contrôles, des tâches et des descriptions de mesures possibles à mettre en œuvre. Chaque entreprise et chaque unité organisationnelle est responsable de la recherche de solutions pour la mise en œuvre des contrôles et des mesures. Des exemples d'application tirés des documents susmentionnés peuvent toutefois aider à trouver des solutions.

5.2 Complexité et portée de la sécurité de l'information pour accroître la résilience des TIC

- (1) La complexité et la portée de la sécurité de l'information dans le contexte du renforcement de la résilience des TIC sont extrêmement exigeantes et étendues. La sécurité de l'information s'étend sur un large éventail de dimensions, couvrant à la fois les aspects techniques et organisationnels.
- (2) D'un point de vue technique, la sécurisation de l'infrastructure TIC implique la protection des réseaux, des systèmes, des applications et des données contre les accès non autorisés, les manipulations ou les pannes. Cela nécessite des mesures de sécurité avancées telles que des pare-feux, des systèmes de détection d'intrusion, le cryptage et des mises à jour régulières de la sécurité afin de pouvoir faire face à des menaces en constante évolution.
- (3) La complexité continue de croître avec la diversité des technologies et des plateformes utilisées dans les entreprises et les unités organisationnelles modernes. Le Cloud Computing, les appareils mobiles, l'internet des objets (IoT) et les systèmes en réseau élargissent considérablement le vecteur d'attaque et nécessitent une stratégie de sécurité globale.
- (4) Au niveau organisationnel, des politiques et des procédures de sécurité claires doivent être développées et mises en œuvre. La sensibilisation et la formation de tous les employés aux pratiques liées à la sécurité sont essentielles, car le facteur humain constitue souvent un réel point faible.
- (5) La gestion des identités et des droits d'accès est un autre défi complexe. S'assurer que seules les personnes autorisées peuvent accéder aux informations sensibles nécessite des systèmes et des processus d'authentification et d'autorisation avancés.
- (6) Un aspect crucial est la capacité à détecter et à réagir en temps réel aux incidents de sécurité. Cela nécessite des systèmes de gestion des informations et des événements de sécurité (SIEM) performants, capables de détecter les irrégularités ou les anomalies à un stade précoce.
- (7) L'adaptation constante aux nouvelles menaces et technologies rend le périmètre de la sécurité de l'information dynamique. Il nécessite des évaluations régulières des risques, des audits de sécurité et une amélioration continue des mesures de sécurité.
- (8) En résumé, la sécurité de l'information dans le cadre de l'augmentation de la résilience des TIC est une démarche très complexe qui ne comprend pas seulement des mesures de protection techniques, mais qui nécessite également la mise en place d'une culture de la sécurité à l'échelle de l'entreprise, la réalisation de formations et l'introduction de processus organisationnels. Une stratégie de sécurité globale est indispensable pour garantir la résilience des technologies de l'information et de la communication face à de multiples menaces.



La complexité et l'ampleur de la sécurité de l'information pour accroître la résilience des TIC ne doivent pas être sous-estimées.

5.3 Efforts en matière de sécurité de l'information pour accroître la résilience des TIC

- (1) L'effort à fournir en matière de sécurité de l'information dans le cadre de l'augmentation de la résilience des TIC est considérable et couvre une multitude d'aspects. En commençant par les investissements technologiques, la mise en œuvre de mesures de sécurité robustes nécessite un effort financier considérable. Cela inclut l'achat et la mise à jour de logiciels de sécurité, l'implémentation de pare-feux, de systèmes de détection d'intrusion, de technologies de cryptage et d'autres infrastructures de sécurité.
- (2) La formation et la sensibilisation du personnel constituent un autre élément essentiel. Le développement de la sensibilisation à la sécurité nécessite des formations régulières afin de maintenir le personnel à jour sur les menaces actuelles, les meilleures pratiques et les politiques de sécurité. Ce processus nécessite non seulement des moyens financiers, mais aussi du temps et des ressources en personnel.



- (3) La création et la mise en œuvre de politiques et de procédures de sécurité claires nécessitent une forte implication de la direction de l'entreprise. L'élaboration, la mise à jour et le suivi de ces politiques représentent un travail administratif considérable pour s'assurer qu'elles répondent aux menaces actuelles et aux exigences réglementaires.
- (4) Les progrès technologiques et l'évolution continue du paysage des menaces signifient qu'un effort considérable de recherche et de développement est nécessaire. Les entreprises et les unités organisationnelles doivent se tenir constamment au courant des nouvelles menaces de sécurité et des contre-mesures afin d'assurer l'efficacité de leur infrastructure de sécurité.
- (5) Le recours à un Security Operation Center (SOC), qui réagit 24 heures sur 24 aux incidents de sécurité, est un autre investissement que les entreprises et les unités organisationnelles doivent faire pour assurer la détection et la réaction aux attaques potentielles 24 heures sur 24.
- (6) L'amélioration continue de la sécurité de l'information implique un effort permanent. Cela implique des audits de sécurité réguliers, des évaluations des risques et des adaptations des mesures de sécurité en fonction de l'évolution des menaces et des exigences commerciales.
- (7) L'effort à fournir en matière de sécurité de l'information pour accroître la résilience des TIC est souvent sous-estimé, car la complexité et les exigences multiples de cette tâche ne sont pas toujours immédiatement évidentes. L'une des raisons est le développement rapide de la technologie et le paysage des menaces en constante évolution. Les entreprises et les unités organisationnelles doivent non seulement rester à la pointe de la technologie, mais aussi être en mesure de réagir de manière proactive aux nouvelles menaces.
- (8) L'intégration de la sécurité de l'information dans la culture d'entreprise nécessite un changement culturel qui prend du temps et demande des efforts. Cet aspect n'est souvent pas suffisamment pris en compte lorsque l'on considère l'effort à fournir pour la sécurité de l'information.
- (9) En résumé, l'effort à fournir en matière de sécurité de l'information pour accroître la résilience des TIC est sous-estimé, car les défis sont à la fois vastes et spécifiques. Il nécessite non seulement des investissements financiers et des ressources supplémentaires, mais aussi une orientation stratégique, une adaptation continue et l'intégration de la sécurité dans l'ensemble de l'organisation.



L'effort à fournir en matière de sécurité de l'information pour accroître la résilience des TIC est considérable et ne doit en aucun cas être sous-estimé.

5.4 Les bases d'une augmentation réussie de la résilience des TIC

5.4.1 Éléments nécessaires à une augmentation réussie de la résilience des TIC

Figure 9: Les éléments nécessaires pour réussir à augmenter la résilience des TIC (source AES)

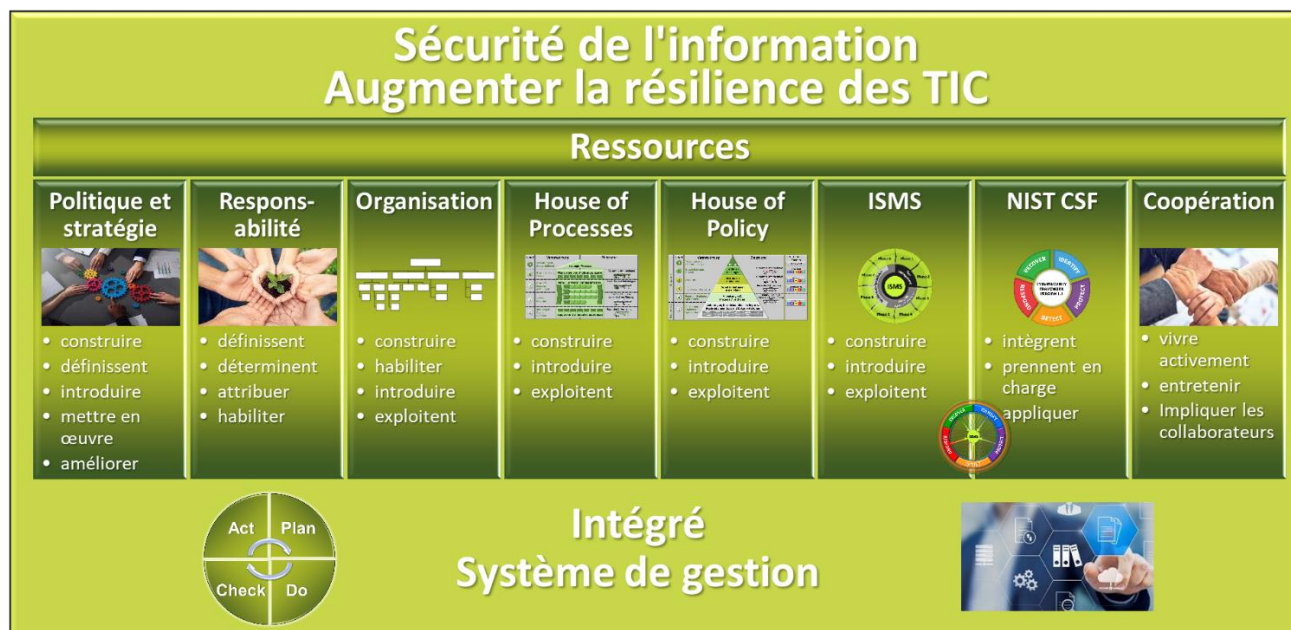
- (1) Les éléments fondamentaux pour une augmentation réussie de la résilience des TIC doivent être abordés de manière globale. Ils interagissent entre eux et ne sont donc pas clairement délimités. Selon l'entreprise et les unités organisationnelles, des domaines spécifiques peuvent également être exécutés par des prestataires de services externes. L'ensemble des étapes de planification, d'introduction, de mise en œuvre et d'exploitation ultérieure de la gestion de la sécurité de l'information (SGI/IMS) doivent se faire selon le cycle PDCA (*Plan, Do, Check, Act*).

5.4.2 Des ressources suffisantes pour accroître la résilience des TIC

- (1) Il est essentiel d'allouer des ressources suffisantes à la sécurité de l'information pour accroître la résilience des TIC. L'allocation des ressources est une tâche exigeante qui est souvent sous-estimée. Il est important de noter que les ressources limitées ne sont pas seulement utilisées pour des mesures techniques, mais aussi

po





ur des mesures organisationnelles.

- (2) La nécessité d'investissements continus est souvent sous-estimée. La dynamique du paysage des menaces exige des mises à jour régulières de l'infrastructure de sécurité pour rester en phase avec les nouvelles méthodes d'attaque. Cela exige non seulement des ressources financières, mais aussi une volonté constante d'adaptation.
- (3) La mise en œuvre et le suivi des politiques de sécurité nécessitent non seulement des ressources financières, mais aussi du temps. Il est important de s'assurer que les directives, en plus d'exister, soient également communiquées, enseignées et respectées de manière efficace. Cela nécessite un effort organisationnel et une surveillance continue.
- (4) L'intégration de la sécurité de l'information dans la culture d'entreprise est un processus à long terme qui nécessite également un engagement au niveau de la direction. Ce changement culturel est essentiel pour garantir que la sécurité ne soit pas considérée comme une tâche isolée des départements IT/OT, mais qu'elle soit perçue comme un élément central de toute organisation.
- (5) Globalement, l'importance de disposer de ressources suffisantes pour la sécurité de l'information n'est souvent pleinement reconnue que lorsque des incidents de sécurité surviennent. Une stratégie globale nécessite un investissement approprié dans les technologies, la formation, les politiques et le changement culturel afin de renforcer la résilience de l'infrastructure TIC et d'être prêt à faire face aux menaces en constante évolution.



L'effort à fournir en matière de sécurité de l'information pour accroître la résilience des TIC est considérable et ne doit en aucun cas être sous-estimé.

5.4.3 Système de gestion intégré (SGI)



Figure 10: SGI (source TÜV NORD)

(1) Le système de gestion intégré (SGI) joue un rôle crucial dans l'augmentation de la résilience des TIC en permettant une approche globale et coordonnée de différents aspects de la gestion. L'importance du SGI réside dans le fait qu'il intègre différentes normes et systèmes de gestion dans une structure unique, notamment la gestion de la qualité, la gestion de l'environnement ou la gestion de la sécurité de l'information.

(2) L'intégration de différents systèmes de gestion permet une utilisation plus efficace des ressources, car des processus et des procédures communs peuvent être mis en

place. Il en résulte une mise en œuvre cohérente et coordonnée des mesures visant à accroître la



résilience des TIC. Le SGI permet d'éviter les redondances et d'exploiter les synergies entre les différents systèmes de gestion.

- (3) L'utilité du SGI pour accroître la résilience des TIC réside dans l'approche globale des risques et des opportunités. En intégrant les aspects de la qualité, de l'environnement et de la sécurité de l'information, les entreprises et les unités organisationnelles peuvent concevoir leurs processus de manière à garantir non seulement la protection des technologies de l'information, mais aussi le maintien de procédures efficaces et de normes de qualité élevées.
- (4) Un autre avantage du SGI réside dans l'optimisation des audits et des surveillances. Étant donné que différents standards et normes sont liés entre eux, les audits peuvent être réalisés plus efficacement, ce qui permet d'économiser les ressources en matière de surveillance. Cela permet une évaluation globale des performances et du respect des différents aspects de la gestion.
- (5) La structure cohérente du SGI permet aux entreprises et aux unités organisationnelles de réagir de manière plus flexible aux conditions changeantes. Cela est essentiel pour réagir rapidement aux nouveaux défis et exigences dans un environnement TIC en constante évolution.
- (6) Dans l'ensemble, le système de gestion intégré favorise une approche systématique et efficace pour accroître la résilience des TIC. En associant la gestion de la qualité, la gestion de l'environnement et la gestion de la sécurité de l'information, non seulement les aspects de sécurité sont renforcés, mais la performance globale et la durabilité d'une organisation sont également améliorées.



Le présent guide ne traite pas explicitement d'un système de gestion intégré. Les méthodologies, les principes et les éléments sont toutefois utilisés comme base.



Recommandation des experts de la Task Force Cyber Security de l'AES:
Les systèmes de gestion intégrés (SGI) devraient être mis en place et appliqués par les entreprises et les unités organisationnelles.

5.4.4 Augmenter la résilience des TIC selon le cycle de Deming

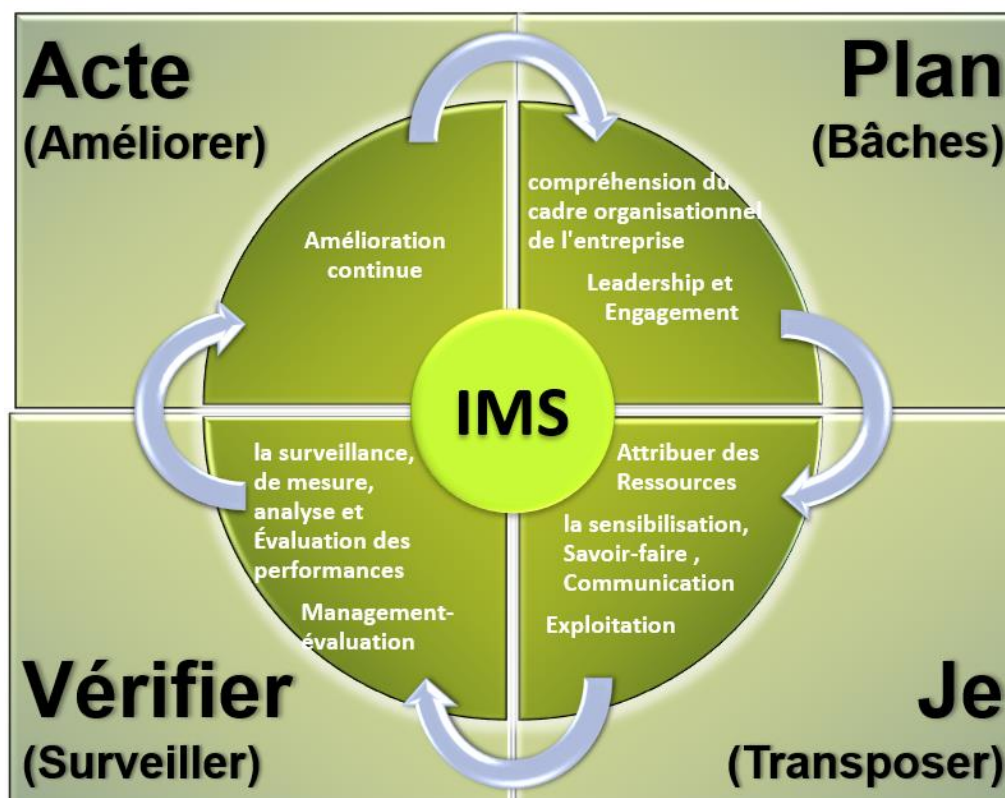


Figure 11: Cycle de Deming PDCA (source AES)

- (1) Le cycle de Deming, également appelé cycle PDCA, est un processus éprouvé de gestion de la qualité et d'amélioration continue. Le cycle PDCA se compose de quatre phases récurrentes:



- **1. Planifier (Plan):** au cours de cette phase, les objectifs et les processus sont identifiés et planifiés. Cela implique la définition d'objectifs clairs, l'identification des problèmes ou des points faibles, l'analyse des données et des informations, la définition des mesures à prendre et la planification des ressources nécessaires pour atteindre les objectifs.
 - **2. Mettre en œuvre (Do):** une fois la phase de planification terminée, les mesures prévues sont mises en œuvre. Il peut s'agir d'introduire de nouveaux processus, de former des employés ou de modifier des processus de travail existants. Au cours de cette phase, la planification est mise en pratique.
 - **3. Vérifier (Check):** cette phase permet de vérifier les résultats et les progrès réalisés. Des données sont collectées et analysées afin de s'assurer que les mesures fonctionnent comme prévu. La vérification permet d'identifier les problèmes ou les écarts par rapport aux objectifs et donne des indications sur la nécessité de procéder à des ajustements supplémentaires.
 - **4. Agir (Act):** cette phase consiste à agir sur la base des résultats de la vérification. Si des problèmes ou des écarts ont été constatés, des mesures appropriées sont prises pour y remédier. Cela peut signifier que la planification est adaptée, que de nouvelles mesures sont prises ou que les processus sont encore optimisés afin d'améliorer la qualité et l'efficacité.
- (2) Une fois la phase «agir» terminée, le cycle recommence. Ce processus de planification, de mise en œuvre, de vérification et d'action contribue à l'amélioration continue d'une entreprise et de ses unités organisationnelles. Le cycle PDCA est un élément important de la gestion de la qualité totale (TQM) et a fait ses preuves en tant que méthode efficace pour améliorer la qualité, l'efficacité et la compétitivité.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Le PDCA, ou cycle de Deming, est un processus d'amélioration continue et doit être appliqué pour augmenter la résilience des TIC dans les différents domaines.



5.4.5 Sécurité de l'information: politique et stratégie

5.4.5.1 Politique de sécurité de l'information (PSI)

- (1) Une politique globale de sécurité de l'information (PSI) est un document central dans toute organisation qui définit les principes et les procédures de base pour assurer la sécurité des informations et des données au sein de l'organisation. Une PSI est essentielle pour garantir que les informations confidentielles et critiques sont correctement protégées. Les éléments clés d'une politique globale de sécurité de l'information sont énumérés ci-dessous:
- **Objectif et but:** la PSI doit expliquer l'objectif stratégique global et le but de la sécurité de l'information dans l'organisation. Il peut s'agir de la protection de l'information, de la protection des données, de la continuité de l'activité et de la conformité aux exigences légales.
 - **Champ d'application:** la PSI doit indiquer clairement les domaines, systèmes et données auxquels elle s'applique. Cela inclut également les partenaires et prestataires de services externes qui entrent en contact avec les informations de l'entreprise et des unités organisationnelles.
 - **Principes et valeurs:** la PSI doit contenir une déclaration claire des principes et valeurs que l'organisation promeut en matière de sécurité de l'information. Cela peut inclure l'éthique, l'intégrité, la confidentialité, la disponibilité et la résilience.
 - **Responsabilités:** la PSI doit définir les rôles et les responsabilités pour la mise en œuvre des politiques et des procédures de sécurité de l'information au sein de l'organisation. Cela peut inclure la désignation d'un Chief Information Security Officer (CISO) ou d'un responsable de la sécurité de l'information (CISO).
 - **Gestion des risques:** La PSI doit décrire l'approche de l'organisation en matière de gestion des risques liés à la sécurité de l'information. Cela comprend l'identification, l'évaluation et le traitement des risques de sécurité.
 - **Protection des informations:** le fournisseur d'accès à internet doit fournir des instructions claires sur la manière de protéger les informations. Cela inclut l'accès, le cryptage, la sauvegarde, la récupération, le stockage sécurisé et l'élimination des documents et des informations.
 - **Notification des incidents de sécurité:** Les politiques devraient définir les procédures et les délais de notification des incidents de sécurité et des violations de données afin de garantir une réaction et une enquête rapides.
 - **Formation et sensibilisation:** la PSI doit définir des exigences en matière de formation et de sensibilisation du personnel à la sécurité de l'information afin de renforcer la prise de conscience et les compétences.
 - **Conformité et législation:** la PSI doit s'assurer que l'organisation respecte les exigences légales et réglementaires pertinentes en matière de sécurité de l'information.
 - **Amélioration continue:** la PSI doit souligner l'importance de l'amélioration continue des mesures de sécurité de l'information et fournir des mécanismes de révision et de mise à jour de la politique.
 - **Révision et approbation:** la PSI doit définir la manière dont la politique est revue, approuvée et mise à jour afin de s'assurer qu'elle répond à l'évolution des besoins et des menaces.
- (2) La PSI doit être comprise et suivie par l'ensemble du personnel et des parties prenantes de l'organisation. Elle constitue un élément essentiel d'un système global de gestion de la sécurité de l'information (ISMS) et sert de base à l'élaboration et à la mise en œuvre de mesures et de procédures de sécurité concrètes.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Chaque entreprise et chaque unité organisationnelle doit élaborer une politique de sécurité de l'information (PSI) qui lui est propre. Cette politique doit être approuvée, introduite, formée et mise en œuvre par la direction et adaptée si nécessaire. Elle constitue la pierre angulaire de l'amélioration de la résilience des TIC. Il est important que la politique de sécurité de l'information soit ancrée dans la culture d'entreprise et qu'elle soit vécue.



5.4.5.2 Stratégie de sécurité de l'information (SSI)



Figure 12: Responsabilité (source weka.ch)

(1) Une stratégie de sécurité de l'information (SSI) est une approche stratégique visant à sécuriser les informations et les données au sein d'une organisation. Elle définit les principes de base, les objectifs et les mesures nécessaires pour garantir la confidentialité, l'intégrité et la disponibilité des informations tout en assurant le respect des dispositions légales et des normes spécifiques à la branche. Une analyse de l'état actuel de la sécurité de l'information mise en œuvre sert de base à la stratégie de sécurité de l'information.

(2) Les éléments clés d'une stratégie de sécurité de l'information sont énumérés ci-dessous:

- **Objectifs et priorités:** la SSI devrait définir des objectifs clairs et mesurables pour la sécurité de l'information dans l'organisation. Il peut s'agir de réduire les incidents de sécurité, de protéger les données sensibles ou d'améliorer les capacités de réponse aux incidents.
 - **Évaluation des risques:** une évaluation complète des risques auxquels l'entreprise et les unités organisationnelles sont exposées en ce qui concerne leurs informations et leurs données est une première étape essentielle. Cela permet d'identifier les menaces et les vulnérabilités les plus importantes.
 - **Conformité:** le respect des lois et des directives spécifiques au secteur doit être pris en compte dans la stratégie.
 - **Lignes directrices et guidelines de sécurité de l'information:** il est essentiel de développer et de mettre en œuvre des politiques et des procédures de sécurité de l'information auxquelles les employés et les parties prenantes doivent se conformer. Cela comprend par exemple les politiques d'accès, les politiques de mots de passe ou les normes de cryptage.
 - **Mesures techniques de sécurité:** le choix et la mise en œuvre de technologies de sécurité telles que les pare-feux, les systèmes de détection/prévention d'intrusion (IDS/IPS), les logiciels antivirus, les solutions de cryptage et les méthodes d'authentification devraient être intégrés dans la stratégie.
 - **Formation et sensibilisation:** la sensibilisation des employés à l'importance de la sécurité de l'information et la formation à la conscience de la sécurité sont indispensables pour éviter les erreurs humaines et les attaques d'ingénierie sociale réussies.
 - **Plan de réponse aux incidents:** la stratégie doit inclure l'élaboration d'un plan de réponse aux incidents optimisé pour l'entreprise et les unités organisationnelles afin de garantir une réponse efficace aux incidents de sécurité.
 - **Surveillance et audits:** une surveillance continue de la situation en matière de sécurité ainsi que des audits de sécurité et des tests d'intrusion réguliers sont nécessaires pour s'assurer que les contrôles de sécurité sont efficaces et pour détecter d'éventuelles vulnérabilités.
 - **Allocation des ressources:** l'allocation du budget, du personnel et d'autres ressources pour la mise en œuvre de la stratégie de sécurité de l'information est essentielle.
 - **Amélioration continue:** une stratégie de sécurité de l'information devrait inclure le principe d'amélioration continue. Cela signifie que la stratégie doit être régulièrement revue et adaptée afin de réagir aux nouvelles menaces et aux évolutions du paysage de la cybersécurité.
- (3) Une stratégie de sécurité de l'information efficace est essentielle pour prévenir les pertes de données, les incidents de sécurité et les atteintes à la réputation. Elle doit être étroitement liée aux objectifs commerciaux de l'organisation et adopter une approche globale de la sécurisation des informations et des données.



5.4.6 Sécurité de l'information: Responsabilité



Figure 13: Responsabilité (source meine-krankenkasse.de)

(1) La définition des responsabilités est d'une grande importance dans les entreprises et les unités organisationnelles, en particulier dans le contexte de l'augmentation de la résilience des TIC, et ce pour de nombreuses raisons:

- **Clarté et transparence:** la définition des responsabilités permet de savoir clairement qui est responsable de quelles tâches et activités. Cela permet d'éviter les malentendus et d'assurer la transparence au sein de l'organisation.

- **Efficacité et productivité:** l'attribution claire des responsabilités augmente l'efficacité, car les employés savent ce que l'on attend d'eux. Il en résulte une plus grande productivité, car le temps et les ressources sont utilisés plus efficacement.

- **Responsabilisation:** les responsabilités garantissent la responsabilisation. Si certaines tâches et objectifs sont attribués à une personne ou un groupe spécifique, ils peuvent être tenus responsables de l'accomplissement de ces tâches.
 - **Contrôle de qualité:** l'attribution claire des responsabilités permet de surveiller et de contrôler les processus et les activités. Cela contribue à garantir des normes de qualité élevées.
 - **Gestion des risques:** dans des domaines tels que la sécurité de l'information et la conformité, la définition des responsabilités est essentielle pour identifier et minimiser les risques. Elle contribue à combler les failles de sécurité et à satisfaire aux exigences légales.
 - **Résolution des conflits:** en cas de désaccord ou de conflit, une répartition claire des responsabilités peut aider à les résoudre. Il est clairement indiqué qui a le pouvoir de décision en dernier ressort.
 - **Délégation et développement:** la définition des responsabilités permet aux cadres de déléguer des tâches et des responsabilités de manière ciblée. Cela contribue au développement professionnel des employés et favorise leur apprentissage et leur croissance.
 - **Confiance et engagement des employés:** les employés qui savent que leurs responsabilités sont clairement définies ont généralement plus confiance en l'organisation et sont plus engagés, car ils sont conscients de leur rôle et de leur importance.
 - **Continuité:** des responsabilités claires garantissent la continuité au sein de l'entreprise et des unités organisationnelles. Si une personne quitte l'entreprise ou s'absente temporairement, une autre peut reprendre ses fonctions sans interruption.
 - **Respect des normes et des réglementations:** dans les secteurs réglementés ou dans les domaines où des normes élevées doivent être respectées, il est essentiel de définir clairement les responsabilités afin de garantir que toutes les exigences sont respectées.
- (2) Globalement, la définition des responsabilités est un élément important de la gestion efficace d'une organisation. Elle permet d'éliminer les ambiguïtés et les inefficacités, favorise la responsabilisation et contribue à améliorer la performance et le succès globaux d'une organisation. Une communication claire des responsabilités est le signe d'une organisation bien gérée.
- (3) L'augmentation de la résilience des TIC nécessite des responsabilités et des rôles clairs au sein d'une organisation. Cela garantit que les mesures visant à se défendre contre les cybermenaces et à maintenir la continuité de l'activité sont planifiées, mises en œuvre et contrôlées efficacement.
- (4) La définition claire de ces responsabilités garantit que tous les aspects de la cyber-résilience des TIC sont couverts, de l'élaboration de la stratégie à la mise en œuvre technique, en passant par la surveillance quotidienne et la réaction aux incidents de sécurité. Elle permet également une coordination efficace entre les différentes équipes et les différents départements afin de garantir que la cybersécurité soit perçue comme une responsabilité partagée.



Les cadres supérieurs de chaque entreprise doivent être conscient de leurs responsabilités (CO 754 Responsabilité des organes).

Lors de l'attribution des responsabilités, il faut veiller à ce qu'un remplaçant soit désigné pour toutes les personnes attribuées. Et celle-ci doit être en mesure d'assumer à tout moment et sans faille la responsabilité qui lui a été attribuée.



5.4.6.1 Responsabilités selon le modèle RASCI

- (1) Le modèle RASCI (également appelé modèle RACI) est un cadre permettant de définir les responsabilités et les rôles au sein des projets, des processus ou des entreprises et des unités organisationnelles. Il permet de clarifier les tâches et les responsabilités des différentes parties prenantes afin de garantir une collaboration efficace et d'augmenter la probabilité de réussite. L'acronyme «RASCI» désigne les cinq rôles principaux du modèle.

Index	Désignation	Description / principes
R	Responsable (Responsable)	La personne ou le groupe responsable de l'exécution effective d'une tâche ou d'une activité. Cette personne exécute les étapes nécessaires à la réalisation de la tâche et à l'obtention du résultat souhaité. Il peut y avoir plusieurs «responsables» pour une tâche, en fonction de son ampleur et de sa complexité.
A	Accountable (Responsable / redevable)	La personne qui porte la responsabilité ultime d'une tâche ou d'un processus. La «personne responsable» est chargée de veiller à ce que la tâche soit menée à bien. Il ne peut y avoir qu'une seule «personne responsable» pour une tâche. Cette personne est responsable de la réception finale, de la garantie de la qualité et du respect des délais.
S	Supportive (Exécutant / soutenant)	Personnes ou groupes qui aident le «responsable» à mener à bien la tâche. Ils peuvent fournir des ressources, des compétences, des outils ou des informations, permettant ainsi le bon déroulement de la tâche. Les «personnes de soutien» travaillent en étroite collaboration avec les «responsables».
C	Consulted (Consulté)	Personnes ou groupes qui doivent être consultés avant que des décisions ne soient prises ou des mesures prises. Ils possèdent des connaissances spécifiques ou une expertise pertinente pour la tâche ou le processus et offrent des conseils ou un retour d'information. Toutefois, ce ne sont pas eux qui détiennent la compétence décisionnelle finale, mais la «personne responsable».
I	Informed (Informé)	Personnes ou groupes qui doivent être informés de l'avancement, du résultat ou des décisions relatives à la tâche ou au processus. Ces personnes doivent être tenues informées, mais ne sont généralement pas directement impliquées dans la tâche.

Tableau 3: Responsabilités selon RASCI (source AES)

- (2) Le modèle RASCI est souvent représenté sous forme de matrice, avec les tâches ou les processus sur l'axe horizontal et les cinq rôles sur l'axe vertical. Chaque tâche ou activité est ensuite abrégée par les lettres correspondantes afin d'attribuer les rôles. Le modèle RASCI favorise la clarté et la transparence dans l'attribution des responsabilités et des rôles. Il permet d'éviter les malentendus et les doublons, d'accroître l'efficacité, d'améliorer la communication et de faciliter la coordination au sein d'un projet, d'un processus ou d'une organisation. C'est un outil précieux pour la gestion des tâches et la garantie d'une collaboration efficace.



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'utilisation du modèle RASCI pour l'attribution des responsabilités aide les entreprises et les unités organisationnelles à avoir une compréhension commune et devrait donc être introduite de manière globale.



5.4.7 Sécurité de l'information: organisation et organigramme

- (1) La sécurisation des informations et des systèmes est essentielle pour résister aux menaces. Une organisation de la sécurité bien structurée, avec des responsabilités et une hiérarchie claire, est indispensable. L'organigramme de la sécurité de l'information devrait comprendre un département de sécurité dédié, directement subordonné à la direction de l'entreprise. Au sein de ce département, des équipes spécialisées dans la sécurité du réseau, la protection des données, la réponse aux incidents et la conformité sont créées et travaillent en étroite collaboration. Une organisation structurée favorise une culture de la sécurité dans laquelle tous les employés comprennent leurs responsabilités en matière de protection de l'information.
- (2) La collaboration avec des partenaires externes est également importante pour obtenir des informations sur les menaces. L'organigramme doit présenter des interfaces claires avec d'autres organisations de sécurité afin de renforcer la résilience des TIC. L'organisation de la sécurité planifie, met en œuvre et surveille les mesures de sécurité afin de garantir l'intégrité, la confidentialité et la disponibilité des informations et des systèmes informatiques. Elle coordonne différentes fonctions de sécurité et développe des stratégies, des politiques et des procédures adaptées aux besoins de l'entreprise et des unités organisationnelles.
- (3) L'organigramme de sécurité visualise cette structure et montre les hiérarchies, les responsabilités et les interactions. Il définit les interfaces et met en évidence le flux d'informations au sein de l'organisation. Les fonctions peuvent être multiples, de la sécurité du réseau à la gestion des risques. La clarté des responsabilités garantit une communication efficace. Les interfaces entre les équipes permettent une collaboration transparente, notamment entre la sécurité du réseau et la sécurité physique.
- (4) L'organisation de la sécurité est étroitement liée à d'autres départements tels que l'informatique, le service juridique et la gestion des risques, ce qui permet une approche globale des risques de sécurité. Globalement, l'organisation de la sécurité joue un rôle central dans la création d'une infrastructure de sécurité complète et coordonnée. La définition claire des responsabilités, la collaboration efficace et l'intégration dans la structure globale de l'entreprise renforcent la sécurité de l'information et augmentent la résilience face aux menaces.

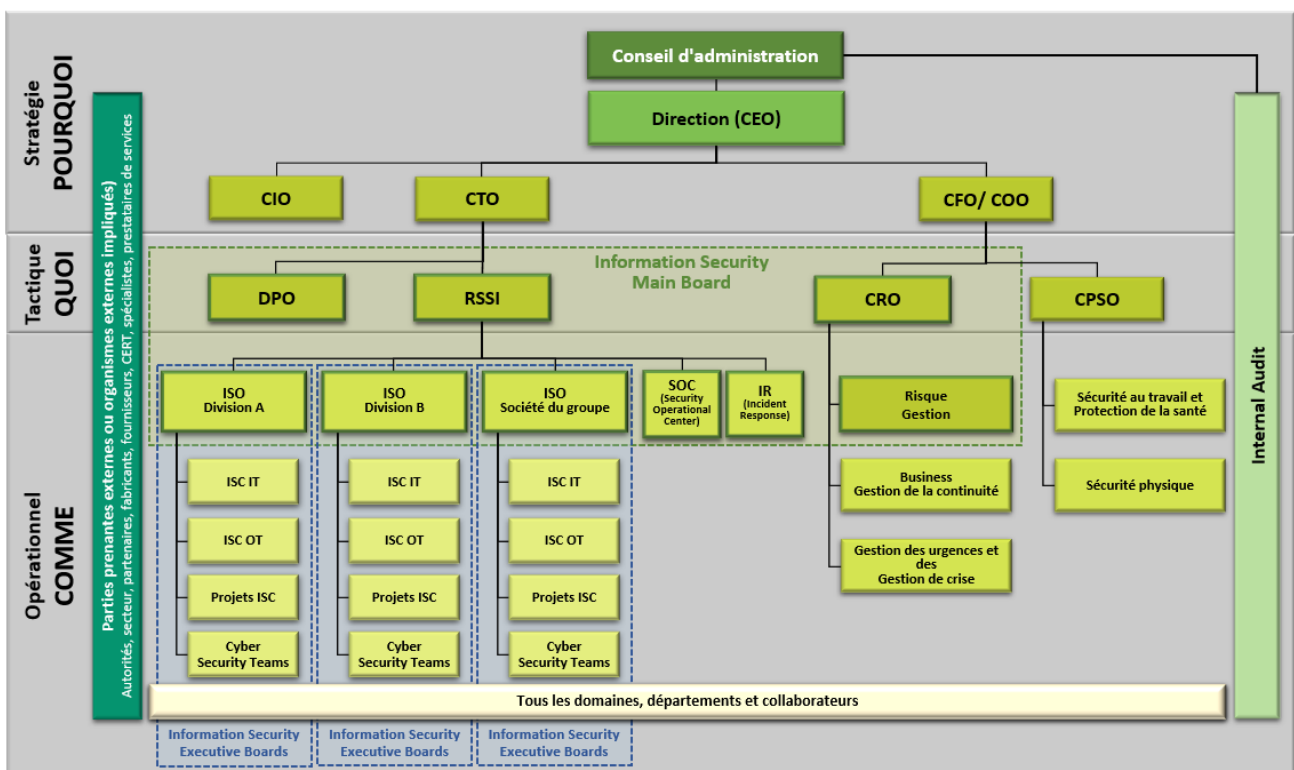


Figure 14: Structure de principe d'un organigramme de sécurité possible (source AES)

- (5) L'organigramme de sécurité pour la sécurité de l'information à l'échelle de l'entreprise varie en fonction de la taille, de la complexité et des besoins de l'entreprise. Il est important de s'assurer qu'une séparation entre les niveaux stratégique, tactique et opérationnel est garantie. En outre, il convient d'établir une séparation claire entre les responsabilités relatives aux directives et à l'exécution, avec les preuves qui s'ensuivent (celui qui donne des directives ne peut pas en plus les exécuter → Segregation of Duties). La



structure exacte et les responsabilités peuvent varier en fonction des exigences et des ressources spécifiques de l'organisation. L'objectif est de créer une structure de sécurité globale afin de pouvoir mettre en œuvre et exploiter une gestion efficace et appropriée de la sécurité de l'information.



La structure d'une organisation de sécurité pour la sécurité de l'information varie en fonction de la taille, de la complexité et des besoins d'une entreprise et des unités organisationnelles. Il est important de faire une distinction entre les niveaux stratégique, tactique et opérationnel. En outre, une séparation claire doit être maintenue entre les responsabilités concernant les directives et l'exécution avec les preuves qui s'ensuivent (celui qui donne des directives ne peut pas exécuter en même temps que le personnel).



Recommandation des experts de la Task Force Cyber Security de l'AES:

La mise en place d'une organisation de la sécurité est impérative pour accroître la résilience des TIC. Celle-ci doit être consignée par écrit, soutenue et communiquée par la direction. Tous les services et personnes impliqués doivent être conscients de leurs fonctions, droits et obligations.

- (6) L'image ci-dessus montre un exemple de structure possible d'un organigramme de sécurité, qui comprend les éléments suivants:

5.4.7.1 Fonctions de l'organigramme de sécurité au niveau stratégique:

- **Conseil d'administration:** le conseil d'administration définit la sécurité de l'information au plus haut niveau et en assume donc aussi la responsabilité globale.
- **Direction, (C-Level ou niveau C):** la direction est un élément fondamental de l'organisation de la sécurité. Elle doit définir la stratégie de sécurité et est responsable de l'ensemble de la mise en œuvre de la sécurité de l'information, et donc aussi de l'augmentation de la résilience des TIC.

5.4.7.2 Fonctions de l'organigramme de sécurité au niveau tactique:

- **DPO (responsable de la protection des données ou responsable de la conformité et de la protection des données):** ces responsables sont chargés de garantir le respect des dispositions légales et des normes industrielles en matière de protection et de sécurité des données. Ils aident à respecter les prescriptions telles que la loi suisse sur la protection des données et son ordonnance ainsi que d'autres prescriptions légales pertinentes dans le domaine de la protection des données et de la conformité.
- **CISO (Chief Information Security Officer):** le CISO est responsable de la gestion de la sécurité de l'information et est le leader de la stratégie de cybersécurité de l'organisation. Il rapporte directement à la direction. Il dirige l'Information Security Main Board, au sein duquel toutes les exigences (directives et instructions de travail) sont établies et surveillées. Souvent, dans les petites et moyennes entreprises et unités organisationnelles, le rôle du CISO est délégué à une personne externe à l'entreprise.
- **Information Security Main Board:** l'Information Security Main Board joue un rôle décisif dans la garantie de la sécurité de l'information au sein d'une entreprise et de ses unités organisationnelles. Ce conseil est responsable sur le plan opérationnel du développement, de la mise en œuvre et du contrôle de la stratégie de sécurité de l'information ainsi que de toutes les directives et mesures visant à garantir l'intégrité, la confidentialité et la disponibilité des informations et des ressources informatiques.

L'une des tâches principales de l'Information Security Main Board est de formuler des stratégies et des objectifs de sécurité complets qui correspondent aux objectifs commerciaux de l'entreprise et aux unités organisationnelles. Cela implique notamment la conception d'une architecture de sécurité robuste pour les systèmes et les infrastructures TIC afin de minimiser les risques potentiels.

Un autre domaine central est la collaboration avec la gestion des risques, qui comprend l'identification, l'évaluation et la hiérarchisation des risques de sécurité. Dans ce contexte, l'Information Security Main Board développe des stratégies de réduction et de contrôle des risques afin de renforcer la résistance de l'entreprise et des unités organisationnelles face aux menaces.

Il joue également un rôle important dans la mise en place de processus et de plans permettant de réagir efficacement aux incidents de sécurité. Cela comprend la réponse aux incidents et l'interface avec la gestion des urgences et des crises afin de garantir une réponse rapide et coordonnée aux incidents de sécurité.



En outre, l'Information Security Main Board joue un rôle crucial dans la surveillance et l'analyse des événements de sécurité en temps réel. Il initie la mise en place de systèmes de surveillance de la sécurité et analyse les menaces afin de pouvoir réagir de manière proactive aux risques de sécurité potentiels.

Il est également responsable des programmes de formation et de sensibilisation afin de renforcer la conscience de la sécurité des employés. Cela inclut la fourniture de formations sur les pratiques de sécurité et la sensibilisation aux menaces actuelles.

Il veille à ce que l'entreprise et les unités organisationnelles respectent les exigences légales et les réglementations spécifiques au secteur en matière de sécurité de l'information.

La protection des données est un domaine partiel de la sécurité de l'information. Elle est toutefois placée sous la responsabilité du DPO. Les mesures sont commandées et contrôlées par le Main Board selon les directives du DPO.

L'évaluation technologique de nouvelles solutions et la recommandation de technologies de sécurité sont également des tâches importantes. À cet égard, l'Information Security Main Board évalue en permanence les nouvelles technologies afin de s'assurer qu'elles répondent aux normes de sécurité.

L'étroite collaboration avec d'autres secteurs, départements, cadres et partenaires externes est un élément essentiel du travail du Information Security Main Board. La communication au niveau C permet de sensibiliser aux risques de sécurité et d'encourager la collaboration pour atteindre des objectifs de sécurité communs.

Enfin, l'Information Security Main Board accorde une grande importance à l'amélioration continue en vérifiant et en actualisant les consignes et les processus de sécurité et en mettant en œuvre des mesures visant à optimiser en permanence la sécurité de l'information.

- **CRO (Chief Risk Officer):** le Chief Risk Officer (CRO) est responsable de la gestion des risques à l'échelle de l'entreprise et rapporte directement à la direction. Ses tâches comprennent, outre la gestion des risques à l'échelle de l'entreprise, le soutien de l'Information Security Main Board et d'autres fonctions dans l'identification, l'évaluation et le contrôle des risques dans les sous-domaines respectifs. Le CRO développe des stratégies de réduction et de contrôle des risques, garantit le respect des lois et des réglementations et joue un rôle clé dans la gestion de la continuité des activités, des urgences et des crises. Grâce à une surveillance et une évaluation continues, le CRO veille à ce que l'entreprise et les unités organisationnelles réagissent de manière appropriée aux risques de sécurité, permettant ainsi une sécurité de l'information plus résiliente.
- **CPSO (Chief Physical Safety Officer):** le Chief Physical Safety Officer (CPSO) est responsable de la sécurité et de la santé au travail ainsi que de la sécurité physique. Dans le domaine de la sécurité et de la santé au travail, le CPSO développe des stratégies et des mesures afin de garantir que les employés puissent travailler dans un environnement sûr et sain. Cela inclut la mise en œuvre de programmes de formation et de politiques visant à prévenir les accidents et à protéger la santé des employés.

Dans le domaine de la sécurité physique, le CPSO est responsable de la protection des installations et des ressources de l'entreprise. Cela comprend la mise en œuvre de contrôles d'accès, de systèmes de surveillance et d'autres mesures de sécurité afin d'empêcher les accès non autorisés et de minimiser les menaces physiques. Le CPSO joue un rôle central dans l'élaboration des plans de sécurité afin d'assurer la sécurité physique de l'entreprise et des unités organisationnelles.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Les moyennes et petites entreprises et unités organisationnelles doivent examiner si la fonction de CISO et les domaines du Information Security Main Board doivent être confiés à un prestataire de services «as a service». En effet, la mise en place de ressources internes disposant des compétences nécessaires prendra du temps.

5.4.7.3 Fonctions de l'organigramme de sécurité au niveau opérationnel:

- **ISO (Information Security Officer):** cette fonction est membre de l'Information Security Main Board et est responsable de la sécurité de l'information pour une ou plusieurs divisions au sein de l'entreprise. Il est l'interface entre le CISO et les divisions concernées. L'ISO établit et surveille les instructions de travail et les publie dans les différentes divisions. En outre, il s'assure, avec l'Information Security Coordinator (ISC), que les consignes de sécurité sont appliquées.



- **ISC (Information Security Coordinator):** il est le lien entre les différents domaines organisationnels dans les divisions et l'Information Security Main Board ou l'ISO. En fonction de l'entreprise et des unités organisationnelles, le CSI coordonne les intérêts de la sécurité de l'information dans l'IT, l'OT et les projets.
- **SOC (Security Operation Center):** le Security Operation Center (SOC) est une composante essentielle et coordonnée par l'Information Security Main Board. Il joue un rôle central dans le domaine de la réponse aux incidents d'une entreprise et des unités organisationnelles. Les principales tâches du SOC consistent à surveiller, détecter et réagir de manière proactive aux incidents de sécurité. L'une des fonctions centrales du SOC consiste à surveiller en permanence l'infrastructure IT-OT pour détecter les menaces de sécurité potentielles. Pour ce faire, des systèmes de surveillance et des technologies avancées sont utilisés afin de détecter rapidement les anomalies et les activités suspectes.

Le SOC signale les incidents de sécurité détectés au CSIRT pour analyse détaillée et traitement des alertes. L'intégration de la Threat Intelligence est une autre tâche du SOC. Il s'agit d'utiliser des informations actualisées sur les menaces provenant de différentes sources afin de renforcer la défense de l'entreprise et des unités organisationnelles face aux menaces nouvelles et évolutives.

Globalement, le SOC fait office de centre nerveux pour la surveillance et la réaction aux incidents de sécurité. Grâce à une collaboration efficace avec les autres départements de sécurité et le CISO, le SOC contribue à garantir la sécurité globale des systèmes d'information et à rendre l'organisation plus résistante aux cybermenaces.



Pour les entreprises et les unités organisationnelles, il est logique que le SOC (Security Operation Center) soit loué «as a service» auprès d'un fournisseur tiers.

- **IR (Incident Response):** l'Incident Response (IR) joue un rôle important dans le domaine de la sécurité de l'information en se concentrant sur la détection et la gestion d'incidents de sécurité complexes qui ne peuvent pas être gérés de manière autonome par le CSIRT interne. La tâche principale de l'Incident Response est de réagir efficacement aux incidents de sécurité complexes afin de minimiser les dommages potentiels et de protéger l'intégrité, la confidentialité et la disponibilité des informations et des ressources.



Dans les petites et moyennes entreprises et unités organisationnelles, il est souvent judicieux de recourir à un IR (Incident Response) «as a service» auprès d'un fournisseur tiers.



Lors de la souscription d'une cyberassurance, certains fournisseurs incluent un service de réponse aux incidents.

- **Les équipes de cybersécurité:** sous l'ISO, il y a généralement une équipe de spécialistes qui se concentre sur différents aspects de la cybersécurité. Cette équipe peut comprendre les rôles suivants:
 - **CSIRT:** les analystes de la sécurité au sein du CSIRT jouent un rôle crucial dans l'évaluation des alertes et la distinction entre les événements opérationnels normaux et les attaques potentielles. C'est là qu'intervient également l'étroite collaboration avec l'Information Security Main Board et d'autres équipes de cybersécurité au sein de l'entreprise et des unités organisationnelles.

Lorsqu'un incident de sécurité se produit, le CSIRT est chargé d'agir rapidement. Cela commence par l'identification et la vérification immédiates de l'incident. Pour ce faire, différents outils et technologies sont utilisés afin de comprendre la nature et l'ampleur de l'incident. Une fois les menaces potentielles identifiées, l'équipe de cybersécurité, y compris le CSIRT, est responsable de l'enquête et de l'analyse de ces incidents. Cela implique de déterminer la nature et l'ampleur de la menace et d'évaluer son impact potentiel sur les différents secteurs d'une entreprise et les unités organisationnelles. Un autre aspect important réside dans la réaction efficace aux incidents de sécurité.

Le CSIRT élabore et met en œuvre des procédures et des plans clairs pour la gestion des incidents de sécurité, y compris la coordination avec les autres équipes et services concernés. L'endiguement efficace de l'incident est au cœur des préoccupations du CSIRT. L'équipe s'efforce de stopper la propagation de l'attaque et de prévenir d'autres dommages. Il peut s'agir



d'isoler des systèmes, de désactiver des comptes d'utilisateurs ou de prendre d'autres mesures pour endiguer l'incident.

Parallèlement, une analyse médico-légale peut être effectuée avec l'Incident Respond Team afin de comprendre les causes de l'incident et de rassembler des preuves pour prendre des mesures supplémentaires. Cette analyse permet également d'identifier les points faibles qui pourraient être à l'origine de l'incident, afin de prendre des mesures préventives pour renforcer la sécurité.

La communication joue un rôle crucial au sein du CSIRT. L'équipe est chargée d'informer les parties prenantes concernées, y compris les cadres, le personnel et, le cas échéant, les parties externes. Cela favorise une communication transparente et permet une réponse coordonnée à l'incident.

Enfin, on procède à la documentation de l'ensemble de l'incident et des mesures prises. Cette documentation est importante non seulement pour l'analyse et l'amélioration internes, mais aussi pour les exigences légales ou réglementaires ainsi que pour la collaboration avec les autorités externes.

En résumé, le CSIRT est indispensable pour garantir la capacité de réaction d'une entreprise et des unités organisationnelles aux incidents de sécurité. En réagissant rapidement, de manière coordonnée et bien documentée, l'équipe contribue à minimiser l'impact des incidents de sécurité et à renforcer la résilience de l'organisation.

En cas d'incidents de sécurité complexes, le CSIRT peut faire appel à l'équipe (externe) de réponse aux incidents pour l'assister et poursuivre le traitement ou l'analyse.

Le CSIRT joue également un rôle déterminant dans l'amélioration continue de la situation en matière de sécurité. En analysant les incidents de sécurité et en identifiant les points faibles, le CSIRT contribue à développer des mesures préventives afin d'éviter de futures attaques.

- **Security Awareness and Training Team:** ce groupe s'occupe de la formation du personnel et augmente la sensibilisation aux risques de sécurité et aux bonnes pratiques.
 - **Architectes de sécurité:** ces experts sont responsables de la planification et de la conception d'architectures et de solutions TIC sécurisées.
 - **Analystes de sécurité:** ces analystes surveillent les événements de sécurité, enquêtent sur les incidents, réalisent des audits de sécurité et aident à identifier les vulnérabilités.
 - **Network Security Team:** ce groupe se concentre sur la sécurité des réseaux et des systèmes de communication. Elle comprend des administrateurs de pare-feu, des ingénieurs en sécurité réseau et des experts en segmentation réseau.
 - **Équipe de sécurité serveur et client:** cette équipe se concentre sur la sécurité du serveur et du client. Elle comprend des auditeurs de sécurité, des développeurs d'applications sécurisées et des experts en tests de sécurité.
 - **Application Security Team:** cette équipe se concentre sur la sécurité des applications et des développements logiciels. Elle comprend des auditeurs de sécurité internes, des spécialistes et des experts en tests de sécurité.
 - **Équipe de sécurité physique:** outre la sécurité numérique, la sécurité physique de l'infrastructure TIC est également importante. Cette équipe est responsable de la protection des centres de données, des salles de serveurs et d'autres ressources physiques.
 - **Gestion des risques des tiers et de la chaîne d'approvisionnement:** cette équipe est chargée de surveiller la sécurité des prestataires de services, des tiers et des fournisseurs et de s'assurer qu'ils respectent les normes de sécurité de l'organisation.
- **Tout les employés:** chaque utilisateur de moyens TIC doit être conscient des cybermenaces potentielles et être en mesure d'agir de manière adéquate dans son propre domaine d'action. Il doit pouvoir signaler en temps réel les incidents de sécurité présumés aux services de sécurité concernés et agir ainsi en tant que capteur de la sécurité de l'information. Chaque employé contribue ainsi de manière déterminante et continue à l'augmentation de la résilience des TIC et est donc également coresponsable, dans son activité quotidienne, de la protection de l'entreprise et des unités organisationnelles.
- La sécurité des informations concerne tous les employés de la même manière. Chacun d'entre eux peut contribuer à éviter les dommages et à contribuer au succès en agissant de manière responsable et en privilégiant la qualité. Une sensibilisation à la sécurité de l'information ainsi que des formations pour les employés et les cadres sont donc fondamentales pour la sécurité des informations. Pour mettre en œuvre efficacement les mesures de sécurité, les employés doivent non seulement posséder



les connaissances nécessaires sur l'utilisation des mécanismes de sécurité, mais aussi comprendre le sens et l'objectif de ces mesures. L'ambiance de travail, les valeurs communes et l'engagement des employés influencent considérablement la sécurité de l'information.

En cas d'embauche ou de modification des tâches, une initiation complète et, le cas échéant, une formation sont nécessaires. Les aspects relatifs à la sécurité du poste de travail concerné doivent être pris en compte. En cas de départ ou de modification des responsabilités des employés, ce processus doit être accompagné de mesures de sécurité appropriées, telles que le retrait des autorisations et la restitution des clés et des badges.

Il est important que les employés s'engagent à respecter toutes les lois, règles et réglementations en vigueur. Pour ce faire, il est nécessaire de les familiariser avec les règles existantes en matière de sécurité de l'information tout en les incitant à les respecter. En outre, les employés doivent être informés du fait que tout incident de sécurité identifié ou suspecté doit être immédiatement signalé au management de la sécurité, et ils doivent savoir comment et à qui ce signalement doit être effectué.

- **Conseils exécutifs de la sécurité de l'information:** Les Information Security Executive Boards jouent un rôle central dans le cadre de la sécurité de l'information au niveau opérationnel, qui implique différents acteurs et fonctions clés au sein d'une entreprise et des unités organisationnelles. Cet organe est composé de cadres supérieurs, dont le responsable de la sécurité de l'information (ISO), le coordinateur de la sécurité de l'information (ISC) pour l'IT, l'OT et les projets, ainsi que de représentants des équipes de cybersécurité. Il agit comme un lien avec les multiples domaines, départements et employés qui sont tous impliqués dans la sécurisation des informations et des systèmes informatiques.

Le responsable de la sécurité de l'information (Information Security Officer, ISO) assume le rôle de responsable suprême au sein de l'Information Security Executive Board. L'ISO est responsable de la mise en œuvre de stratégies de sécurité complètes et de la garantie du respect des dispositions légales et des directives internes.

Le coordinateur de la sécurité de l'information (Information Security Coordinator, ISC) joue un rôle crucial dans la coordination des efforts de sécurité dans différents domaines clés, y compris l'informatique, l'OT et les projets. L'ISC est responsable de l'intégration des pratiques de sécurité dans ces différents contextes et veille à ce que les aspects de sécurité soient intégrés dans toutes les activités de l'entreprise et de l'unité organisationnelle.

Les équipes de cybersécurité, qui comprennent des groupes spécialisés de professionnels, sont directement impliquées dans la mise en œuvre des mesures de sécurité et la gestion des incidents de sécurité. Elles travaillent en étroite collaboration avec l'Information Security Executive Board afin d'évaluer les menaces actuelles, de développer des contre-mesures appropriées et de s'assurer que l'ensemble de l'organisation est résiliente face aux cybermenaces.

L'Information Security Executive Board crée une approche coordonnée et cohérente de la sécurité de l'information en impliquant les différents acteurs dans le développement et la mise en œuvre des stratégies de sécurité. Il promeut une culture de la sécurité qui englobe tous les secteurs, départements et employés d'une entreprise et des unités organisationnelles. Grâce à une communication régulière, à des formations et à des politiques de sécurité claires, le conseil contribue à sensibiliser aux questions de sécurité et à garantir que la sécurité de l'information reste une priorité à tous les niveaux de l'organisation.

- (7) La structure exacte et les responsabilités peuvent varier en fonction des besoins et des ressources spécifiques de l'organisation. L'objectif est de mettre en place une structure de sécurité globale qui protège l'organisation contre les cybermenaces et garantit que les systèmes TIC fonctionnent de manière sûre et conforme.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Étant donné que le domaine d'activité d'un Security Operation Center (SOC) et d'Incident Respond est très vaste et nécessite un savoir-faire spécifique, les entreprises et les unités organisationnelles doivent examiner attentivement si elles ne souhaitent pas acquérir ce domaine auprès d'un prestataire de services «As a Service».



Il est très important que tous les employés soient impliqués dans la sécurité d'une entreprise et des unités organisationnelles. Ils contribuent de manière déterminante et continue à l'augmentation de la résilience des TIC et est donc également coresponsable dans son activité quotidienne.



5.4.7.4 Éléments transversaux de l'organigramme de sécurité à tous les niveaux:

- **Internal Audit (audit interne):** l'audit interne du conseil d'administration joue un rôle crucial dans le cadre de la sécurité de l'information, notamment lorsqu'il s'agit d'accroître la résilience des TIC. L'audit interne se concentre sur l'assurance que les mesures et les contrôles de sécurité sont appropriés et efficaces pour protéger les informations et les systèmes TIC de l'organisation. L'audit interne examine et évalue la mise en œuvre des politiques, procédures et normes de sécurité de l'information. Il prend en compte aussi bien les aspects technologiques que les processus et la conformité réglementaire. L'audit vise à identifier les vulnérabilités et les risques potentiels dans l'infrastructure de sécurité.

En outre, l'audit interne examine l'efficacité des mesures de sécurité afin de s'assurer qu'elles résistent aux menaces et aux exigences actuelles. Cela implique une évaluation des contrôles d'accès, des procédures de cryptage, des systèmes de surveillance de la sécurité et d'autres solutions technologiques. L'examen porte également sur le respect des normes de sécurité et des réglementations. L'audit interne veille à ce que l'organisation respecte les exigences légales et suive les meilleures pratiques spécifiques au secteur afin d'assurer la sécurité de l'information.

Un autre aspect important est l'évaluation de la résilience des TIC face aux menaces et perturbations potentielles. L'audit interne examine les plans et les mesures de récupération après des incidents de sécurité ou des catastrophes afin de s'assurer que l'organisation peut réagir rapidement et efficacement à de tels événements.

Les résultats de l'audit interne sont consignés dans des rapports qui sont transmis au conseil d'administration et à la direction de l'organisation. Ces rapports donnent un aperçu de l'état actuel de la sécurité de l'information, identifient les domaines d'amélioration potentiels et aident à définir des mesures pour augmenter la résilience des TIC.

Globalement, l'audit interne joue un rôle clé pour garantir que la sécurité de l'information est gérée de manière adéquate au sein de l'entreprise et des unités organisationnelles. Par ses vérifications et ses recommandations, elle contribue à accroître la résistance des TIC aux menaces et à assurer ainsi la continuité des processus d'entreprise.

- **Parties prenantes externes ou organismes externes impliqués:** Les autorités, le secteur, p. ex. l'AES, les partenaires, p. ex. d'autres EAE, les fabricants, les fournisseurs, les spécialistes et les prestataires de services font partie des parties prenantes externes ou des organismes externes impliqués. Les parties prenantes externes et les organismes impliqués jouent un rôle crucial dans le cadre global de la sécurité de l'information, qui vise à accroître la résilience des TIC.

En tant que parties prenantes externes, les autorités représentent une source importante de cadres juridiques et de réglementations qui influencent la sécurité de l'information. Il est essentiel de travailler en étroite collaboration avec elles pour s'assurer que les entreprises et les unités organisationnelles respectent les exigences légales, tout en bénéficiant d'un soutien et de directives sur les meilleures pratiques.

Les organisations de la branche jouent un rôle clé dans la rédaction de normes sectorielles et de bonnes pratiques en matière de sécurité de l'information. La collaboration avec ces organisations permet aux entreprises et aux unités organisationnelles de bénéficier de connaissances spécifiques au secteur et de s'assurer que leurs pratiques de sécurité sont conformes aux normes actuelles du secteur.

Le partenariat avec des partenaires externes, des fabricants et des fournisseurs est essentiel, car leurs produits et services sont souvent intégrés dans l'infrastructure TIC. Une coordination étroite garantit non seulement la sécurité de ces produits et services, mais favorise également un échange transparent d'informations sur la sécurité et entraîne une amélioration de la sécurité globale.

Des experts techniques externes peuvent apporter des perspectives supplémentaires et des connaissances spécialisées pour aider les entreprises et les unités organisationnelles à développer et à mettre en œuvre des stratégies de sécurité efficaces.

Les prestataires de services spécialisés dans la sécurité offrent des ressources et une expertise supplémentaires. Des tests d'intrusion aux services de réponse aux incidents en passant par la formation à la sécurité, ils contribuent à renforcer les capacités de sécurité d'une organisation et à garantir qu'elle est prête à répondre à un large éventail d'exigences en matière de sécurité.



Les interfaces entre ces parties prenantes externes sont essentielles pour garantir un échange d'informations sans faille et travailler ensemble au renforcement de la résilience des TIC. En travaillant de manière coordonnée avec ces acteurs externes, les entreprises et les unités organisationnelles peuvent élaborer une stratégie globale, proactive et résiliente pour relever les défis du paysage des menaces en constante évolution.



La collaboration constructive avec les parties prenantes externes et les organismes externes est essentielle pour accroître la résilience des TIC. Les interfaces doivent être clairement définies et attribuées. Il faut s'assurer que tous les postes nécessaires sont impliqués et que ces interfaces sont gérées activement.

5.4.8 Sécurité de l'information: Maison des processus (House of Processes)

- (1) Une «maison des processus» sert de structure organisationnelle permettant de hiérarchiser et de visualiser les processus d'une entreprise et de ses unités organisationnelles. L'intérêt d'une maison des processus réside dans plusieurs aspects importants:
 - **Structuration et vue d'ensemble:** une maison des processus offre une hiérarchie claire qui permet de structurer la multitude de processus dans une entreprise et des unités organisationnelles. Cela favorise la clarté et la compréhension du paysage des processus.
 - **Représentation transparente des processus:** elle permet une représentation transparente et facilement compréhensible des processus, en commençant par les processus stratégiques et de gestion et en terminant par les processus de base et de soutien. Cela favorise la compréhension du fonctionnement de l'entreprise et de l'unité organisationnelle par les employés et les parties prenantes.
 - **Identification des interactions:** la disposition des processus dans une maison des processus permet de mettre en évidence les interactions entre différents processus. Cela favorise une vision globale et permet une meilleure coordination entre les unités organisationnelles.
 - **Optimisation et amélioration:** la maison des processus sert de base à l'identification des potentiels d'optimisation et des possibilités d'amélioration. Elle facilite l'analyse ciblée et l'adaptation des processus afin d'augmenter l'efficacité et l'efficacité.
 - **Intégration des technologies de l'information:** une maison des processus sert de guide pour l'intégration des technologies de l'information afin de soutenir et d'automatiser efficacement les processus. Cela favorise la numérisation et améliore les processus de travail.
 - **Communication et collaboration:** elles facilitent la communication interne et externe en fournissant une structure claire pour la transmission des informations et la collaboration entre les différentes unités organisationnelles et les parties prenantes.
- (2) En résumé, une maison des processus aide l'entreprise et les unités organisationnelles à mieux organiser, comprendre, optimiser et concevoir efficacement leurs processus. C'est un outil qui permet de maîtriser la complexité des processus de l'entreprise et des unités organisationnelles et d'améliorer la performance globale d'une entreprise et des unités organisationnelles.

5.4.8.1 Structure de la Maison des processus

- (1) Le concept de maison des processus dans le contexte de la gestion de l'information peut être spécifiquement adapté aux exigences des entreprises et d'unités organisationnelles électriques. Dans les entreprises et les unités organisationnelles, les différents processus sont organisés dans une maison des processus afin de garantir une gestion efficace et transparente de toutes les activités. La structure de base suivante s'applique à une maison des processus:



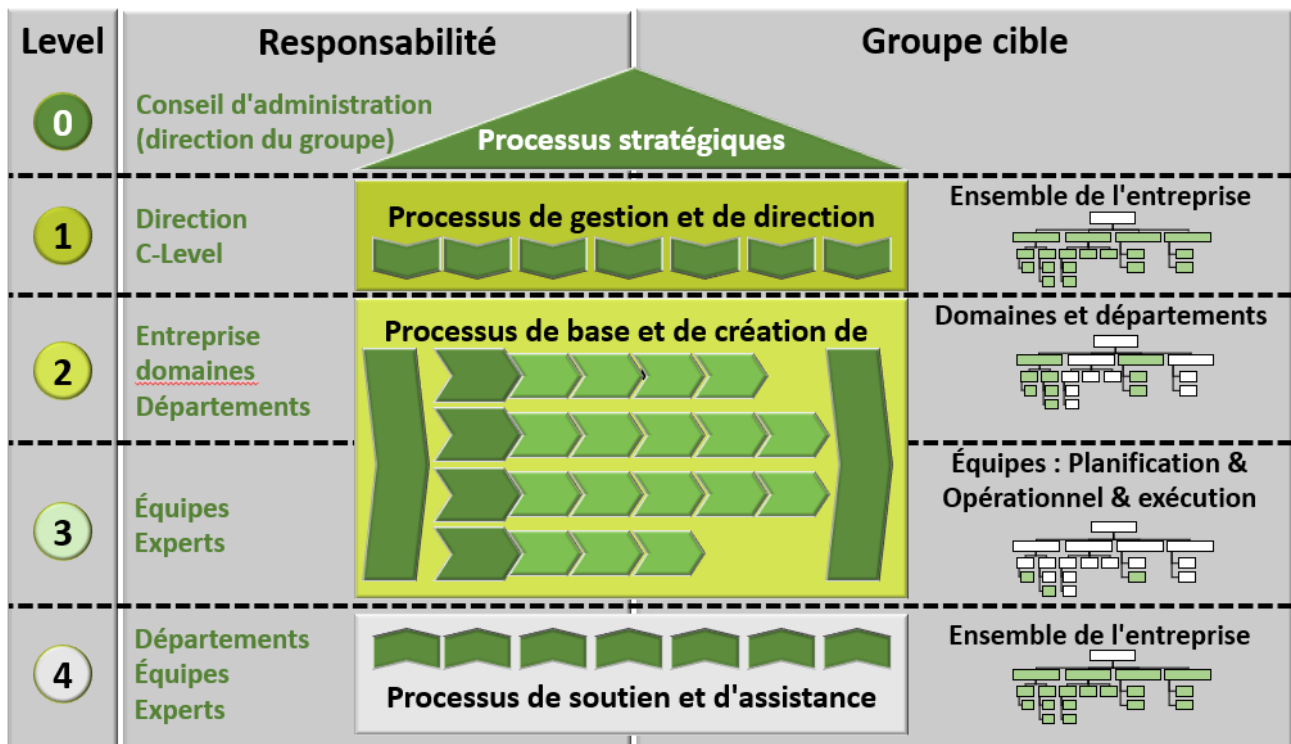


Figure 15: Structure dans la Maison du processus (source AES)

(2) La liste suivante décrit les principaux processus liés à la sécurité de l'information:

- **Niveau 0 (toit):** Processus stratégiques
 - **Politique énergétique et développement de stratégies:** Développement d'objectifs et de stratégies à long terme en tenant compte des aspects environnementaux, des directives politiques et des exigences du marché.
- **Niveau 1 (dernier étage):** processus de gestion et de direction

Les processus de gestion et de direction sont des éléments décisifs dans l'organisation et la direction des entreprises. Voici une liste des principaux processus de gestion et de direction:

 - **Planification:** formulation de plans concrets et de directives d'action. Planification des ressources, y compris les ressources humaines, financières et technologiques. Établissement de budgets et de prévisions financières.
 - **Organisation:** définition des structures organisationnelles et des hiérarchies. Attribution des tâches et des responsabilités. Mise en place de mécanismes de communication et de coordination.
 - **Prise de décision:** analyse des informations et des données. Identification des options d'action. Sélection des meilleures alternatives en tenant compte des risques et des opportunités.
 - **Leadership et motivation:** développement de principes et de styles de leadership. Motiver les employés pour qu'ils atteignent leurs objectifs. Promotion d'une culture d'entreprise positive.
 - **Communication:** définition de politiques et de plans de communication; diffusion d'informations pertinentes aux employés. Promotion d'une communication ouverte et efficace au sein de l'organisation.
 - **Mise en œuvre:** transformation des plans et des stratégies en actions concrètes. Utilisation des ressources selon les priorités définies. Suivi des progrès et adaptation si nécessaire.
 - **Suivi et contrôle:** définition d'indicateurs de performance clés (KPI) pour le suivi. Évaluation continue des processus et des résultats. Mise en œuvre de mesures correctives en cas d'écarts.
 - **Gestion des risques:** identification et évaluation des risques. Développement de stratégies pour minimiser les risques. Intégration de la gestion des risques dans les processus de décision et de planification.
 - **Gestion de l'innovation:** promotion d'une culture de l'innovation. Identification des opportunités d'innovation de produits et de processus. Mise en œuvre de stratégies d'innovation.



Les processus de gestion et de direction sont souvent liés et interagissent afin de garantir que les entreprises sont gérées et dirigées efficacement. Le succès d'une entreprise dépend en grande partie de sa capacité à intégrer et à adapter ces processus de manière judicieuse.

■ **Niveau 2 (étage supérieur):** processus clés de la chaîne de valeur

- **Production d'électricité:** comprend les différentes méthodes de production d'électricité, qu'il s'agisse de centrales électriques conventionnelles, d'énergies renouvelables ou d'autres sources.
- **Gestion du réseau:** planification, développement et entretien du réseau électrique afin de garantir un approvisionnement énergétique fiable.
- **Exploitation réseau:** responsable du bon fonctionnement du réseau électrique, de la gestion des flux d'énergie et de la garantie de la stabilité du réseau.
- **Gestion de la charge:** surveillance et adaptation de la production d'énergie à la demande actuelle afin d'éviter les goulets d'étranglement ou les surcapacités.

■ **Niveau 3 (rez-de-chaussée):** sous-processus dans la chaîne de création de valeur

- **Sous-processus de production d'électricité:** comprend les différentes méthodes de production d'électricité, que ce soit par des centrales électriques conventionnelles, des énergies renouvelables ou d'autres sources.
- **Sous-processus pour l'exploitation du réseau:** responsable du bon fonctionnement du réseau électrique, de la gestion des flux d'énergie et de la garantie de la stabilité du réseau.
- **Sous-processus pour la gestion de la charge:** surveillance et adaptation de la production d'énergie à la demande actuelle afin d'éviter les goulets d'étranglement ou les surcapacités.

■ **Niveau 4 (étage supérieur):** processus de soutien

- **Gestion financière:** gestion des aspects financiers de l'entreprise et des unités organisationnelles, y compris la budgétisation, la comptabilité et la facturation.
- **Gestion du personnel:** recrutement, formation et gestion du personnel, y compris les politiques de sécurité et de santé.
- **Gestion informatique:** gestion des technologies informatiques nécessaires au fonctionnement et au contrôle du système d'approvisionnement en énergie.
- **Communication avec la clientèle:** communication avec les clients finaux sur les tarifs d'électricité, les informations sur la consommation et les demandes spécifiques des clients.
- **Partenariats et communication avec les fournisseurs:** communication avec d'autres entreprises et unités organisationnelles, les autorités de réglementation et les fournisseurs pour une collaboration et une conformité efficaces.

- (3) La maison des processus d'une entreprise et d'unités organisationnelles de distribution électriques offre une représentation hiérarchique des principaux processus et permet de comprendre les interactions entre les différents niveaux. Elle sert également de base à l'intégration des technologies de l'information afin de soutenir et de gérer efficacement ces processus. Il est important de noter que la structure spécifique d'une Maison des processus peut varier en fonction des exigences et des conditions individuelles de chaque entreprise et unité d'organisation de l'approvisionnement en électricité.
- (4) Exemple de Maison des processus pour une entreprise et des unités organisationnelles dans le domaine de l'approvisionnement en électricité:



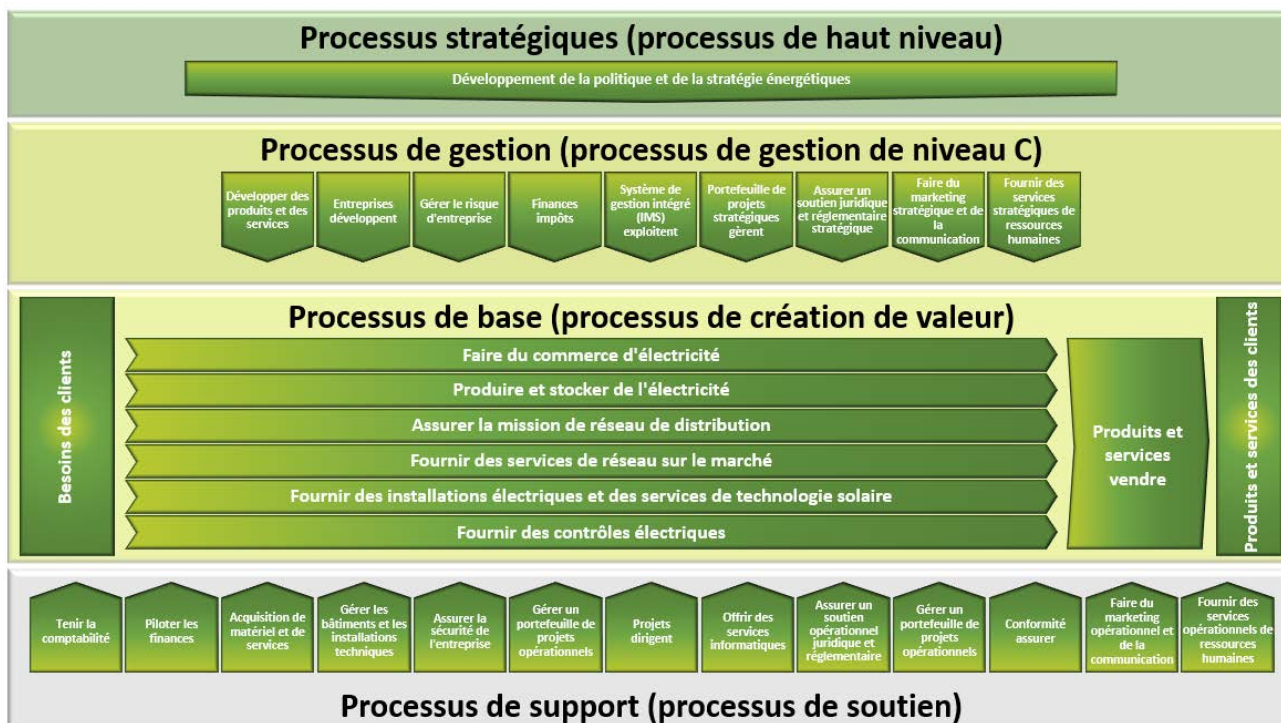


Figure 16: Processus dans la Maison des processus (source AES)



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'implication de la maison des processus de l'entreprise et de l'unité d'organisation permet, dans différents processus de sécurité de l'information, d'obtenir des procédures, des évaluations et une compréhension appropriée des exigences en matière de résilience des TIC. Par exemple, lors de l'évaluation des risques ou de la mise en place d'un registre des actifs.



5.4.8.2 Responsabilités et compétences au sein de la Maison des processus

- (1) Les responsabilités au sein de la Maison des processus sont précisément définies. Il est défini qui ou quel rôle dans l'entreprise et dans les unités organisationnelles est compétent ou responsable de l'élaboration et de l'approbation des différents processus.

Niveau	Responsable	Type de processus	Groupe cible	Approbation par
0	Conseil d'administration (direction du groupe)	Processus stratégiques	Groupe Ensemble de l'entreprise	
1	Direction de l'entreprise, C-Level	Processus de gestion et de direction	Ensemble de l'organisation / entreprise	Conseil d'administration et/ou direction du groupe
2	Responsable d'unité et de département	Principaux processus de base dans la chaîne de création de valeur	Divisions et départements	Direction, niveau C
3	Équipes et experts	Sous-processus dans la chaîne de création de valeur	Équipes d'exécution opérationnelles, y compris la planification, les ingénieurs experts et les spécialistes	Responsable d'unité et de département
4	Départements, équipes et experts	Processus de soutien et d'assistance	Spécifique	Direction, C-Level, responsables de division et de département

Tableau 4: Responsabilités et compétences dans la Maison des processus (source AES)

5.4.9 Sécurité de l'information: Maison des politiques (House of Policies)

5.4.9.1 Structure de la Maison des politiques

- (1) La Maison des politiques, dans le contexte d'un système de gestion de la sécurité de l'information (ISMS), décrit la structure et les processus des directives relatives à la sécurité de l'information. Un ISMS est une approche globale de la gestion de la sécurité de l'information au sein d'une organisation. La Maison des politiques constitue le fondement de cette approche et se compose de plusieurs niveaux:
- **Niveau 0 (toit):** le niveau le plus élevé de la Maison des politiques représente le conseil d'administration et la direction du groupe (le cas échéant). Une déclaration claire sur la sécurité de l'information doit être faite à ce niveau. La direction reçoit ainsi des instructions claires concernant l'augmentation de la résilience des TIC. C'est à ce niveau que les objectifs stratégiques sont définis et qu'il est question du «pourquoi».
 - **Niveau 1 (dernier étage):** le niveau 1 de la Maison des politiques représente la direction de l'entreprise ou le top management (niveau C) de l'entreprise. C'est ici que sont définis les principes de base et les objectifs stratégiques de la sécurité de l'information. Cela peut inclure l'importance de la sécurité de l'information pour l'entreprise, le budget qui lui est alloué et les responsabilités et compétences existantes. A ce niveau, les objectifs stratégiques sont concrétisés et consignés sur l'entreprise. Il s'agit de savoir «pourquoi». Toutes les fonctions de la sécurité de l'information doivent être représentées.
 - **Niveau 2 (duplex):** ce niveau est responsable de l'élaboration de politiques et de procédures de sécurité concrètes au niveau tactique. C'est à ce niveau que sont établies les directives tactiques générales au moyen de politiques et de lignes directrices concernant la sécurité de l'information et, par conséquent, l'amélioration de la résilience des TIC, sur la base de l'orientation stratégique de la man-sarde. En principe, le cadre et le champ d'application sont définis à ce niveau. Il s'agit de savoir «CE QUI» doit être fait en principe. Les catégories pour la sécurité de l'information sont ainsi constituées et définies.
 - **Niveau 3 (dernier étage):** à ce niveau, des instructions de travail et des instructions opérationnelles sont élaborées. Tous les domaines et thèmes spécifiques de la sécurité de l'information sont abordés de manière spécifique. Ils couvrent des sujets tels que la protection des données, le contrôle d'accès,



les mots de passe, la sauvegarde des données et autres aspects fondamentaux de la sécurité. Le principe est de savoir «comment» faire quelque chose. Les sous-catégories nécessaires sont ainsi définies avec les tâches pour la sécurité de l'information.

- **Niveau 4 (rez-de-chaussée):** c'est à ce niveau que sont développés les instructions concrètes, les processus et les guides qui permettent la mise en œuvre des instructions de travail et des Instructions. C'est à ce niveau que sont définies les mesures spécifiques issues des tâches, telles que la mise en œuvre de pare-feu, de systèmes de détection des intrusions, de cryptage, l'élaboration et la mise en œuvre de plans d'urgence, la formation des employés, la sécurisation des ressources physiques et la surveillance des événements de sécurité, etc. En principe, c'est à ce niveau que l'on définit «comment» quelque chose doit être fait concrètement.
 - **Niveau 5 (sous-sol):** la base ou niveau 5 de la Maison des politiques représente les mesures techniques et les solutions de sécurité nécessaires pour mettre en œuvre les objectifs de sécurité et en apporter la preuve. Cela comprend par exemple l'implantation de pare-feu, de systèmes de détection d'intrusion, le cryptage et d'autres mesures techniques de sécurité.
- (2) Les niveaux 0 à 4 établissent et décrivent les directives. Ces directives peuvent également contenir des preuves qui attestent que les directives du niveau supérieur sont comprises et mises en œuvre. Au niveau 5, on trouve les preuves de la mise en œuvre ainsi que la documentation technique pour la mise en œuvre.
- (3) La Maison des politiques représente une structure hiérarchique qui garantit que les objectifs de l'organisation en matière de sécurité de l'information sont poursuivis et mis en œuvre de bout en bout, depuis le niveau supérieur de la direction jusqu'à la mise en œuvre technique dans l'infrastructure IT/OT. Les différents niveaux sont étroitement liés et s'appuient les uns sur les autres afin de garantir une stratégie de sécurité de l'information cohérente et efficace.

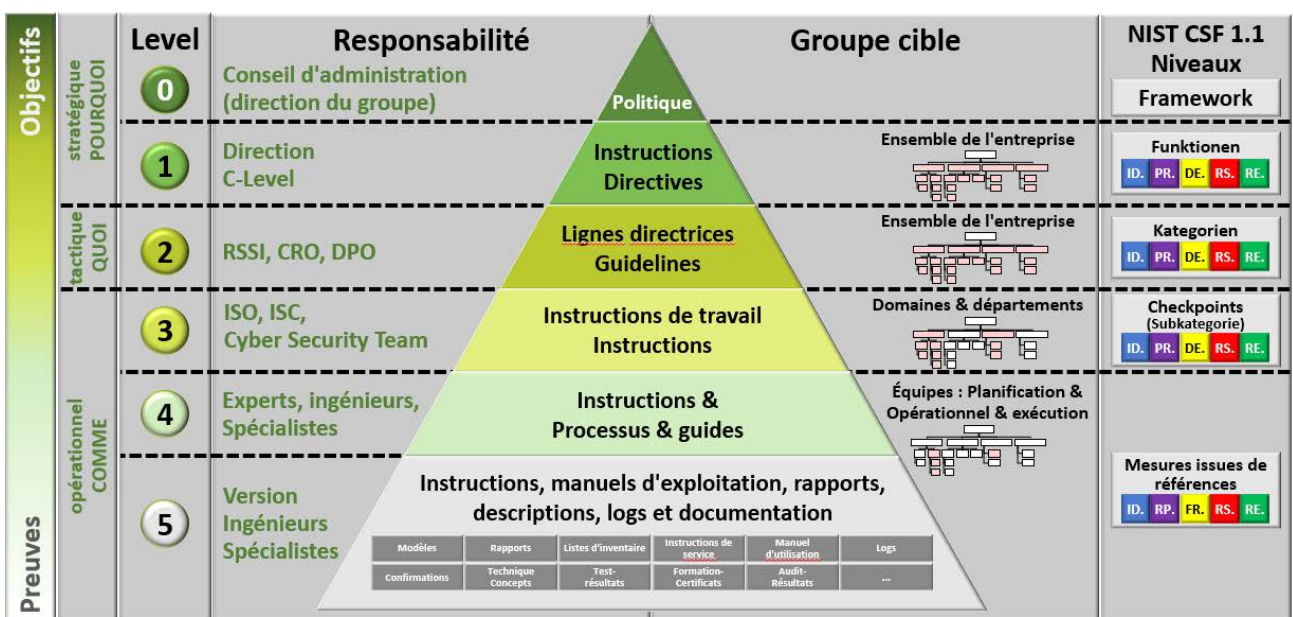


Figure 17: Structure de principe de la Maison des politiques avec le mapping vers le CSF NIST 1.1 (source AES)



Recommandation des experts de la Task Force Cyber Security de l'AES:

Pour accroître la résilience des TIC, il est impératif de mettre en place et d'exploiter une Maison des politiques.



5.4.9.2 Responsabilités et compétences au sein de la Maison des politiques

- (1) Les responsabilités au sein de la Maison des politiques sont précisément définies. Il est défini qui, quel rôle ou quelle fonction au sein de l'entreprise et des unités organisationnelles est responsable de l'élaboration et de l'approbation des différents documents.

		Ni- veau	Responsable	Type de poli- tique	Groupe cible	Approbation par
Vorgaben	Stratégique	0	Conseil d'administration (direction du groupe)	Politique	Groupe Ensemble de l'entreprise	
		1	Direction de l'entreprise, C-Level	Instructions, Directives	Ensemble de l'organisation / entreprise	Conseil d'adminis- tration et/ou direc- tion du groupe
	Tactique	2	Chief Information Secu- rity Officer (CISO), Chief Risk Officer (CRO), Responsable de la pro- tection des données (DPO)	Directives, Lignes direc- trices	Ensemble de l'organisation / entreprise	Direction, niveau C
Nachweise	Opérationnel	3	Responsable de la sécu- rité de l'information (ISO), coordinateur de la sécurité de l'information (ISC), équipe de cyber- sécurité	Instructions de travail, Instructions	Domaines et départements	CISO, CRO, DPO
		4	Experts, ingénieurs, spé- cialistes	Instructions, pro- cessus et guides	Équipes d'exécution opéra- tionnelles, y compris la plani- fication, les ingénieurs experts et les spécialistes	ISO, ISC, équipe de cybersécurité
		5	Utilisateurs, ingénieurs, spécialistes	Instructions, descriptions et documentation, etc.	Spécifique	Révision par des experts, des ingé- nieurs ou des spé- cialistes

Tableau 5: Responsabilités et compétences au sein de la Maison des politiques (source AES)

5.4.9.3 Objectifs et preuves



Figure 18: Objectifs et preuves avec transition fluide (source AES)

- (1) Il n'y a pas de limite claire entre les exigences et les preuves. En effet, dans l'ensemble de la Maison des politiques, une consigne d'un niveau est confirmée par un niveau inférieur ou la preuve est apportée que la consigne est comprise et que sa mise en œuvre est décrite. Un niveau de détail granulaire doit être appliqué. En principe, les directives sont toujours plus détaillées dans le document de base, ce qui prouve qu'elles sont comprises et mises en œuvre.

5.4.9.4 Maîtrise des documents à la Maison des politiques

- (1) La maîtrise des documents est un élément important du système de gestion de la qualité (Quality Management System, QMS) dans les entreprises et les unités organisationnelles. Elle se réfère au processus de création, de mise à jour, d'approbation, de distribution et de gestion des documents afin de garantir qu'ils sont exacts, à jour et accessibles. Voici une description étape par étape de la maîtrise des documents:

- **Création et modification de documents:** la première étape consiste à créer ou à mettre à jour des documents afin de s'assurer qu'ils répondent aux exigences et aux normes actuelles. Il peut s'agir de politiques, de directives, de lignes directrices, d'instructions, de processus, de guides, de procédures, d'instructions de travail, de directives de qualité, de formulaires, de rapports et d'autres types de documents.



- **Marquage et identification:** chaque document doit être clairement marqué et identifié afin d'éviter toute confusion. Cela implique l'attribution d'un nom de document, d'un numéro de version et de dates de création ou de modification.
- **Approbation et autorisation:** les documents, en particulier ceux qui sont critiques pour l'organisation, doivent être approuvés. Cela est généralement fait par des rôles ou des fonctions définis qui sont responsables du contenu du document.
- **Distribution et contrôle d'accès:** les documents approuvés doivent être communiqués au personnel concerné et, si nécessaire, faire l'objet d'une formation. Des droits et des contrôles d'accès sont définis afin de garantir que seules les personnes autorisées peuvent accéder aux documents.
- **Stockage et conservation:** les documents sont stockés de manière sécurisée afin de garantir leur intégrité et leur confidentialité. Il peut s'agir d'un stockage physique (par exemple dans des classeurs) ou d'un stockage électronique dans un système de gestion de documents (QMS).
- **Suivi des modifications:** les modifications apportées aux documents font l'objet d'un suivi afin de documenter l'historique et l'évolution des documents. Cela comprend l'indication des raisons des modifications et le suivi des versions.
- **Processus de retrait:** lorsque les documents ne sont plus nécessaires ou sont obsolètes, ils doivent être retirés et archivés ou éliminés de manière appropriée.
- **Révision et suivi:** des révisions régulières des documents sont nécessaires pour s'assurer qu'ils restent à jour et pertinents. Cela peut se faire dans le cadre d'audits internes ou de contrôles de qualité.
- **Formation et sensibilisation:** les employés doivent être informés et formés sur les procédures de contrôle des documents afin de s'assurer qu'ils comprennent et respectent les processus.
- **Communication:** les modifications apportées aux documents et les mises à jour doivent être communiquées afin que toutes les parties concernées soient informées.

(2) La maîtrise des documents contribue à garantir la qualité, la conformité et l'efficacité au sein d'une organisation. Un système de gouvernance documentaire efficace garantit que les bonnes informations sont mises à la disposition des bonnes personnes au bon moment et que ces informations sont à jour et précises.

5.4.9.5 Aperçu des documents de la Maison des politiques sur l'augmentation de la résilience des TIC aux niveaux 0 à 3

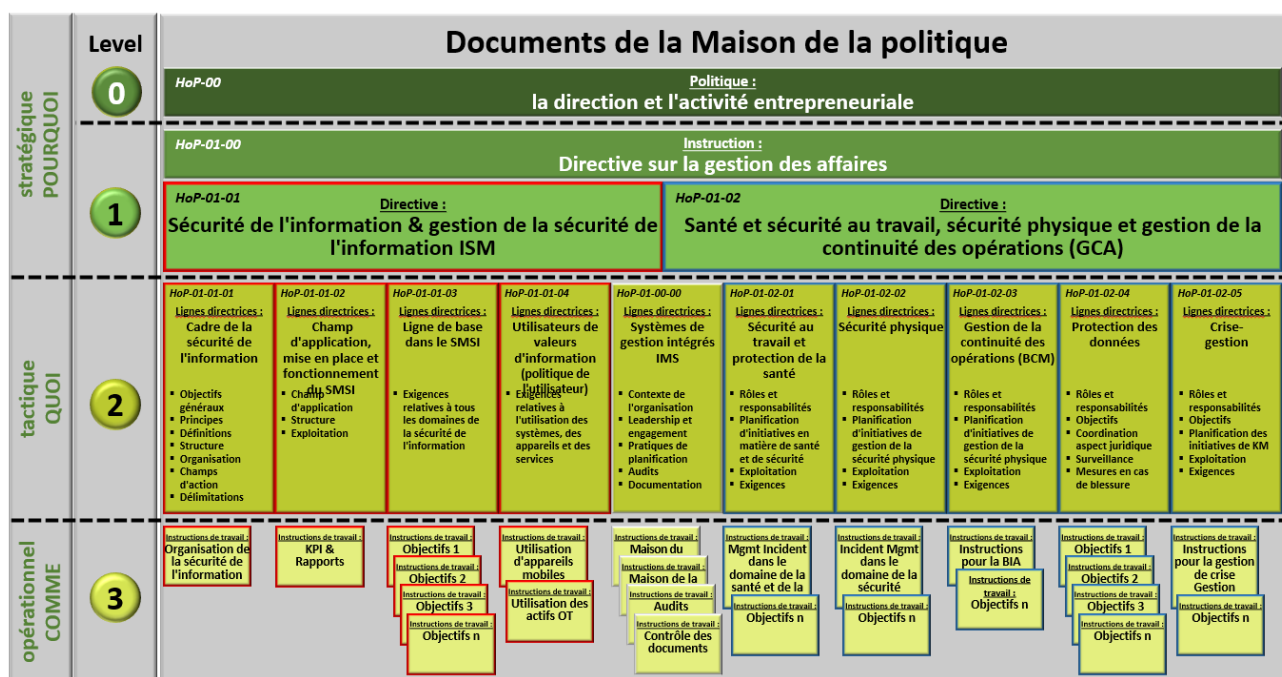


Figure 19: Documents de la Maison de la politique aux niveaux 0 à 3 (source AES)





Dans ce guide, la Maison des politiques décrit les niveaux 0 à 3. En annexe se trouve une description des directives nécessaires du point de vue de l'AES ainsi que des exemples pour l'entreprise ELECTRICITÉ SA, qui peuvent être utilisés comme modèles ou comme aide à l'élaboration des documents.



Dans les annexes, il y a des exemples types qui peuvent être appliqués.

5.4.9.6 Cartographie de la Maison des politiques avec le CSF NIST CSF 1.1

- (1) Le cadre de cybersécurité NIST comprend quatre niveaux qui représentent systématiquement l'amélioration de la résilience des TIC de manière plus ou moins détaillée. Plus les niveaux sont bas, plus les différentes mesures visant à accroître la résilience des TIC sont détaillées et concrètes.

	Niveau	Responsable	Type de politique	Niveaux CSF NIST CSF 1.1	
Vorgaben	Stratégiquement « POURQUOI »	0 Conseil d'administration (direction du groupe)	Politique	Framework	En principe, la politique de sécurité de l'information doit stipuler qu'un cadre tel que le CSF NIST 1.1 doit être utilisé pour accroître la résilience des TIC.
		1 Direction de l'entreprise, C-Level	Lignes directrices, Instructions	Funktionen ID. PR. DE. RS. RE.	La stratégie de sécurité de l'information et les instructions spécifiques doivent faire référence aux différentes fonctions du CSF NIST 1.1 (ID=Identify, PR=Protect ; DE=Detect, RS = Response et RE=Recover). Il faut s'assurer que toutes les fonctions sont traitées de manière adéquate et que les directives correspondantes sont intégrées.
	Tactique « QUOI »	2 Chief Information Security Officer (CISO), Chief Risk Officer (CRO), Responsable de la protection des données (DPO)	Directives, Guidelines	Kategorien ID. PR. DE. RS. RE.	Dans les directives et les guidelines, tous les points doivent être traités au niveau de la catégorie dans le NIST CST. Il peut être fait référence au niveau de la fonction. Il est impératif que tous les points soient décrits et définis au niveau de la catégorie.
		3 Responsable de la sécurité de l'information (ISO), coordinateur de la sécurité de l'information (ISC), équipe de cybersécurité	Instructions de travail, Instructions	Checkpoints (Subkategorie) ID. PR. DE. RS. RE.	Les manuels de travail et les instructions doivent être détaillés au moins jusqu'à la sous-catégorie du niveau CSF NIST 1.1. Il est possible de faire référence aux niveaux supérieurs ou inférieurs si cela facilite la compréhension.
Nachweise	Opérationnel « COMMENT »	4 Experts, ingénieurs, spécialistes	Instructions, processus et guides	Massnahmen aus Referenzen ID. PR. DE. RS. RE.	Les références du CSF NIST 1.1 doivent être utilisées pour les justifications. Il est également possible de se référer aux niveaux supérieurs du CSF NIST 1.1. Il existe également d'innombrables documents utiles. Ce guide en donne quelques exemples.
		5 Utilisateurs, ingénieurs, spécialistes	Instructions, descriptions et documentation, etc.		

Tableau 6: Mapping Maison des politiques avec les niveaux dans le CSF NIST 1.1

- (2) En principe, chaque point du CSF NIST 1.1 doit être représenté dans les documents de référence de la Maison des politiques aux niveaux 0 à 3. Cela doit se faire au moins jusqu'au niveau de la tâche (sous-catégorie). En outre, des références ou des points des références mentionnées peuvent également être intégrés.





L'outil «VSE-NIST-CSF-1.1_HoP-Mapping-Tool» permet d'attribuer les différents éléments du CSF NIST 1.1 aux documents de la Maison des politiques en amont de la création des documents.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Le mapping des éléments du CSF NIST 1.1 avec les documents de la Maison des politiques permet de garantir que tous les points sont attribués et traités.

5.4.9.7 Mapping de l'ISO 27001:2022 Annexe A avec les documents de la Maison de la politique

- (1) En principe, selon ISO 27001:2022 Annexe A, chacun doit être représenté dans un document de référence de la Maison des politiques aux niveaux 0 à 3. Cela doit se faire au moins jusqu'au niveau de la sous-catégorie. En outre, des références ou des points des mesures énumérées selon ISO 27002:2022 peuvent également être intégrés.



Dans l'outil «VSE-ISO27002-Annex-A_HoP-Mapping-Tool», les différents éléments de l'ISO27001:2022 Annexe A peuvent être attribués aux documents de la Maison des politiques en amont de la création des documents.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Le mappage de l'Annexe A de la norme ISO 27001 avec les documents de la Maison des politiques permet de garantir que tous les points sont attribués et traités.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

5.4.9.8 Listes des objectifs et des preuves dans la Maison des politiques



Dans ce guide, seules les directives et les preuves qui sont en rapport direct avec la Maison des politiques pour la sécurité de l'information sont énumérées. Cette énumération n'est pas exhaustive et peut être complétée à tout moment par des documents supplémentaires. La définition des noms et la désignation des différents types de documents s'inspirent des directives actuelles de différents cadres et normes, mais peuvent varier selon les entreprises ou les unités organisationnelles et leurs définitions. Il est toutefois important que la désignation et la fonction des types de documents soient appliquées dans l'ensemble de l'entreprise et des unités organisationnelles.

5.4.10 Système de gestion de la sécurité de l'information (ISMS)

- (1) Un système de gestion de la sécurité de l'information (ISMS) est un cadre structuré et global qui sert à gérer la sécurité de l'information dans une entreprise et dans les unités organisationnelles. Il comprend des directives, des processus, des technologies et des mesures qui visent à garantir la confidentialité, l'intégrité et la disponibilité des informations. L'ISMS prend en compte les aspects technologiques et organisationnels et s'inspire de normes internationales telles que ISO/IEC 27001. L'objectif est d'identifier, d'évaluer et de traiter les risques afin de rendre l'infrastructure TIC plus résistante aux menaces. Grâce à une surveillance continue, à des formations et à des adaptations, l'ISMS contribue à garantir la sécurité de l'information à un niveau approprié et à assurer la protection des données sensibles.

5.4.10.1 Raisons de la mise en place d'un ISMS:

- (1) Un système de gestion de la sécurité de l'information (Information Security Management System, ISMS) est d'une importance capitale pour les entreprises et les unités organisationnelles, car il sert à garantir et à améliorer la sécurité de l'information. Voici quelques raisons pour lesquelles un ISMS est important:
 - **Protection des informations sensibles:** un ISMS aide à protéger les informations confidentielles et sensibles contre l'accès non autorisé, le vol ou la perte de données. C'est d'autant plus important que les données font aujourd'hui partie des actifs les plus précieux de nombreuses entreprises et unités organisationnelles.
 - **Respect des dispositions légales:** dans de nombreux pays et secteurs, il existe des dispositions légales et des règles de protection des données auxquelles les entreprises et les unités



organisationnelles doivent se conformer. Un ISMS permet de se conformer à ces exigences et d'éviter les conséquences juridiques.

- **Confiance de la clientèle:** une sécurité de l'information robuste inspire confiance à la clientèle et aux partenaires. Les entreprises et les unités organisationnelles qui font preuve d'une sécurité des données avérée peuvent gagner de la clientèle et la conserver.
 - **Gestion des risques:** un ISMS aide à identifier, évaluer et atténuer les risques de sécurité. Cela permet à l'organisation de gérer les menaces potentielles de manière proactive.
 - **Continuité et résilience:** le ISMS favorise l'élaboration de plans d'urgence et de récupération afin de garantir que l'organisation puisse continuer à fonctionner après un incident de sécurité ou une catastrophe.
 - **Efficacité et productivité:** la mise en œuvre de politiques et de procédures de sécurité peut améliorer l'efficacité de l'organisation, car les employés savent comment traiter les informations en toute sécurité.
 - **Réduction des coûts:** en prévenant les incidents de sécurité et les pertes de données, les entreprises et les unités organisationnelles peuvent réaliser des économies considérables sur les coûts liés à la gestion des incidents et au rétablissement de la réputation et de la confiance.
 - **Bonnes pratiques et normes:** un ISMS peut être basé sur des normes internationales telles que l'ISO 27001, ce qui offre des bonnes pratiques et un cadre pour la sécurité de l'information.
 - **Amélioration continue:** le ISMS favorise l'amélioration continue de la sécurité de l'information. Les entreprises et les unités organisationnelles peuvent développer en permanence leurs mesures de sécurité en se basant sur les données et les expériences recueillies.
 - **Avantage en termes de réputation et de compétitivité:** les entreprises et les unités organisationnelles qui ont démontré qu'elles mettaient en œuvre des pratiques de sécurité robustes peuvent améliorer leur réputation et leur compétitivité, car elles sont considérées comme des partenaires fiables.
- (2) À une époque où les cyberattaques et les violations de la protection des données sont monnaie courante, un ISMS est un élément important de la stratégie commerciale. Il permet de minimiser les risques, de maintenir les activités et de gagner la confiance des parties prenantes.

5.4.10.2 Mise en place d'un ISMS

- (1) Un système de gestion de la sécurité de l'information (ISMS) est une approche systématique et structurée de la gestion et de la sécurisation des informations au sein d'une organisation. La mise en place d'un ISMS se fait en plusieurs étapes, un cadre éprouvé étant le cycle Plan-Do-Check-Act (PDCA) décrit dans la norme ISO 27001. Vous trouverez ci-dessous un aperçu de la mise en place d'un ISMS:
- **Définition du cadre:** commencez par définir le champ d'application et les objectifs du ISMS. Déterminez quelles informations doivent être protégées et identifiez les exigences légales et réglementaires pertinentes.
 - **Leadership et soutien:** la direction générale doit soutenir le ISMS et définir les responsabilités en matière de sécurité de l'information.
 - **Évaluation des risques:** identifiez et évaluez les risques pour la sécurité de l'information. Cela implique l'analyse des menaces, des vulnérabilités et de l'impact potentiel sur l'organisation.
 - **Planification:** élaborer des politiques, des objectifs et des procédures de sécurité pour traiter les risques identifiés. Élaborez également un plan de mise en œuvre du ISMS.
 - **Mise en œuvre et exploitation:** mettre en œuvre les politiques et procédures de sécurité dans l'ensemble de l'organisation. Cela comprend la formation, les mesures de sécurité et la définition des responsabilités.
 - **Surveillance et évaluation:** surveillez en permanence l'efficacité de l'ISMS. Enregistrez les incidents de sécurité, réalisez des audits internes et externes et évaluez les mesures mises en œuvre.
 - **Amélioration continue:** sur la base des résultats de la surveillance et de la mesure, prenez des mesures pour améliorer continuellement l'ISMS. Cela peut inclure l'adaptation des politiques, des procédures et des formations.
 - **Évaluation par la direction:** la direction générale doit examiner régulièrement l'ISMS afin de s'assurer qu'il est efficace et qu'il répond aux besoins de l'entreprise.

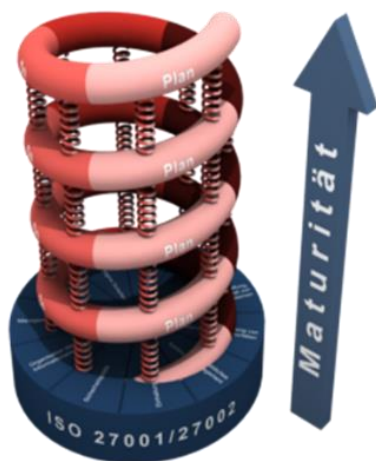


- **Documentation et enregistrements:** créez une documentation et des enregistrements prouvant le respect des politiques et des procédures de sécurité.
 - **Formation et sensibilisation:** formez les employés et augmentez la sensibilisation à la sécurité de l'information dans l'ensemble de l'organisation.
 - **Communication et rapports:** communiquez les progrès et les résultats de l'ISMS à la direction générale et à toutes les parties prenantes concernées.
- (2) La mise en place d'un ISMS conforme aux normes internationales telles que ISO 27001 peut être utile pour mettre en œuvre les meilleures pratiques et évaluer l'efficacité du ISMS. La mise en place d'un ISMS est un processus itératif au cours duquel l'organisation apprend et s'améliore en permanence afin de rester en phase avec l'évolution des menaces et des exigences.



Il est fortement recommandé par les experts de la Cyber Security Task Force de l'AES de mettre en place un ISMS afin d'augmenter la résilience des TIC.

5.4.10.3 ISMS selon ISO 27001



(1) Un système de gestion de la sécurité de l'information (ISMS) conforme à la norme ISO 27001 est un cadre conçu pour assurer, surveiller, gérer et améliorer en permanence la sécurité de l'information au sein d'une organisation. La norme ISO 27001 est une norme internationalement reconnue en matière de sécurité de l'information et définit les exigences relatives à l'élaboration, à la mise en œuvre et au fonctionnement d'un ISMS. Voici les composants clés d'un ISMS selon la norme ISO 27001:

- **Politique de sécurité de l'information:** l'organisation développe une politique formelle de sécurité de l'information qui exprime l'engagement de la direction envers la sécurité de l'information.
- **Définition du champ d'application:** l'organisation détermine le champ d'application de l'ISMS, y compris les actifs et processus pertinents à couvrir.

Figure 20: Spirale de maturité de l'ISMS

- **Évaluation et traitement des risques:** une évaluation complète des risques est effectuée afin d'identifier les menaces, les vulnérabilités et les risques pour la sécurité de l'information. Sur la base de cette évaluation, des contrôles et des mesures d'atténuation des risques appropriés sont sélectionnés et mis en œuvre.

- **Politiques et procédures de sécurité:** l'organisation élabore et documente des politiques et des procédures de sécurité qui garantissent le respect des exigences de sécurité.
 - **Soutien de la direction:** la direction générale s'engage en faveur de l'ISMS et fournit les ressources nécessaires.
 - **Contrôle de la documentation:** la documentation, y compris les politiques, procédures et registres de sécurité, est établie, gérée et contrôlée.
 - **Communication et sensibilisation:** l'organisation communique les politiques et procédures de sécurité aux employés et assure la formation et la sensibilisation à la sécurité de l'information.
 - **Surveillance et vérification:** la performance de l'ISMS est surveillée régulièrement et des audits internes sont réalisés pour vérifier l'efficacité des mesures de sécurité.
 - **Amélioration continue:** sur la base des résultats de la surveillance et de la vérification, des améliorations continues sont apportées afin d'optimiser la sécurité de l'information.
 - **Planification d'urgence et de récupération:** l'organisation élabore des plans de récupération des systèmes et des données en cas d'incident de sécurité ou de catastrophe.
 - **Audit et certification externes:** dans certains cas, l'organisation peut se soumettre à un audit et à une certification indépendants afin de démontrer sa conformité à la norme ISO 27001.
- (2) Un ISMS conforme à la norme ISO 27001 offre une approche systématique de la sécurité de l'information et permet aux entreprises et aux unités organisationnelles de minimiser les risques, d'améliorer la sécurité



et de gagner la confiance des parties prenantes. La mise en œuvre et le maintien d'un ISMS nécessitent la collaboration de différents secteurs de l'entreprise et de l'unité organisationnelle, ainsi qu'une surveillance et une mise à jour continues afin de suivre l'évolution des menaces et des exigences.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est recommandé de mettre en place un ISMS conforme à la norme ISO 27001, suivi d'une certification (pour les organisations avec un niveau de protection A ou B)

5.4.10.4 Les phases de l'AES pour la mise en place d'un ISMS

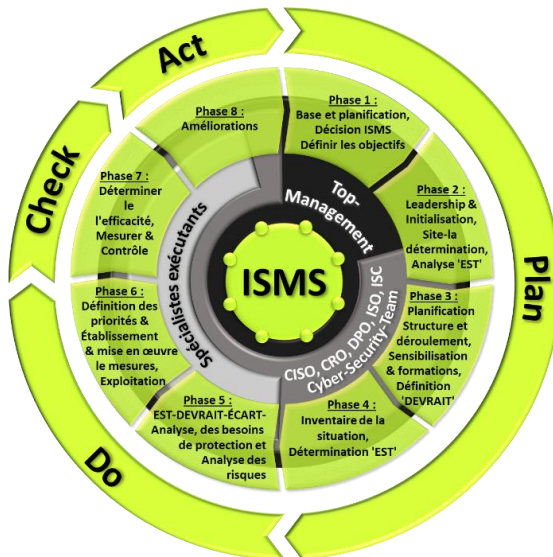


Figure 21: Phases de l'AES pour la mise en place de l'ISMS (source AES)

(1) La mise en place d'un système de gestion de la sécurité de l'information (ISMS) est un processus stratégique qui vise à garantir et à améliorer en permanence la sécurité de l'information au sein d'une organisation. Cette introduction se déroule en plusieurs phases successives:

(2) L'initiation constitue le point de départ. C'est à ce moment que la nécessité d'un ISMS est reconnue et acceptée. Cela peut être motivé par des exigences légales externes, des besoins des clients ou des évaluations internes des risques. La direction supérieure s'engage à soutenir l'ISMS.

(3) Vient ensuite l'analyse du contexte, qui permet d'identifier les facteurs internes et externes susceptibles d'influencer la sécurité de l'information. Cela inclut la détermination des parties prenantes, des lois et réglementations pertinentes ainsi que d'autres conditions cadres.

(4) La direction de l'entreprise définit clairement les rôles, les responsabilités et les pouvoirs en matière de sécurité de l'information. Le top management s'engage formellement à soutenir le ISMS afin de favoriser l'intégration de la

sécurité de l'information dans la culture d'entreprise.

- (5) La phase de planification consiste à élaborer un plan détaillé pour le ISMS. Cela comprend une évaluation complète des risques afin d'identifier les menaces et les vulnérabilités. Des objectifs et des mesures de sécurité sont élaborés afin de réduire le risque à un niveau acceptable pour l'entreprise et les unités organisationnelles.
- (6) La phase de mise en œuvre comprend l'implémentation concrète des mesures développées lors de la planification. Cela comprend l'introduction de directives de sécurité, la formation du personnel, la mise en place de contrôles de sécurité et l'installation de systèmes de surveillance.
- (7) La surveillance et la mesure sont essentielles pour garantir que les objectifs de sécurité définis sont atteints. Des audits internes et externes ainsi que des vérifications régulières garantissent que les processus définis sont efficaces et peuvent être améliorés en permanence.
- (8) L'évaluation des performances analyse les données collectées afin d'évaluer l'efficacité du ISMS. Cette phase identifie également les possibilités d'amélioration visant à optimiser les pratiques et les processus de sécurité.
- (9) L'amélioration continue est mise en œuvre sur la base des résultats de l'évaluation. Il peut s'agir d'adapter des processus, d'introduire de nouvelles technologies ou de former le personnel.
- (10) La revue de direction est effectuée régulièrement par la direction générale. Elle examine l'efficacité de l'ISMS par rapport aux objectifs commerciaux et aux orientations stratégiques de l'organisation. Des ajustements sont effectués pour s'assurer que l'ISMS reste conforme aux exigences.
- (11) La mise en place d'un ISMS est donc un processus cyclique qui vise à faire de la sécurité de l'information une partie intégrante de la culture d'entreprise et à l'améliorer en permanence.
- (12) La procédure de mise en place du ISMS est décrite en détail dans les chapitres suivants.



5.4.11 Sécurité de l'information: CSF NIST version 1.1



Illustration 22 Cadre de cybersécurité du NIST

(1) Le NIST Cybersecurity Framework (CSF) est un cadre de l'Institut national des normes et de la technologie (NIST) des États-Unis qui aide les entreprises et les unités organisationnelles à développer et à améliorer leur cybersécurité. Le cadre a été développé pour servir d'instrument volontaire pour les entreprises et les unités organisationnelles de toutes tailles et de tous secteurs. Il se compose de cinq fonctions centrales: «Identify», «Protect», «Detect», «Respond», et «Recover».

(2) La fonction «Identify» vise à comprendre les éléments fondamentaux des risques de cybersécurité. Cela comprend l'identification des actifs, des menaces et des vulnérabilités, ainsi que la définition des objectifs de protection et des priorités.

(3) Dans la fonction «Protect», des mesures sont prises pour limiter ou contrôler les risques identifiés. Cela comprend la protection des systèmes, des données et des processus par des contrôles de sécurité, des formations et une sensibilisation des employés à la

sécurité.

- (4) La fonction «Detect» se concentre sur l'identification précoce des anomalies et des incidents de sécurité. Pour ce faire, des mécanismes de surveillance, des systèmes de détection d'intrusion (IDS) et d'autres technologies sont utilisés afin de détecter toute activité inhabituelle.
- (5) La fonction «Respond» met l'accent sur la réaction rapide aux incidents de sécurité. Les entreprises et les unités organisationnelles développent des plans de réaction clairs afin de pouvoir réagir efficacement aux cyberattaques ou autres incidents de sécurité. Cela implique également la collaboration avec des partenaires externes et les autorités.
- (6) La fonction «Recover» s'adresse à la capacité d'une organisation à revenir le plus rapidement possible à un fonctionnement normal après un incident de sécurité. Cela implique la mise en œuvre de plans de récupération, l'évaluation de l'efficacité des mesures et l'adaptation des stratégies de récupération sur la base des enseignements tirés des incidents.
- (7) Le CSF NIST offre un cadre flexible qui permet aux entreprises et aux unités organisationnelles de développer et d'adapter leur propre stratégie de cybersécurité. Il est reconnu dans le monde entier comme une méthode éprouvée pour renforcer la résilience des TIC des entreprises et des unités organisationnelles et pour relever efficacement les défis croissants dans le domaine de la cybersécurité.



La norme minimale pour les TIC a été adoptée dans le contrat d'électricité. Ainsi, le cadre NIST doit être appliqué.

5.4.12 Sécurité de l'information: mise en réseau de l'ISMS avec le CSF NIST 1.1

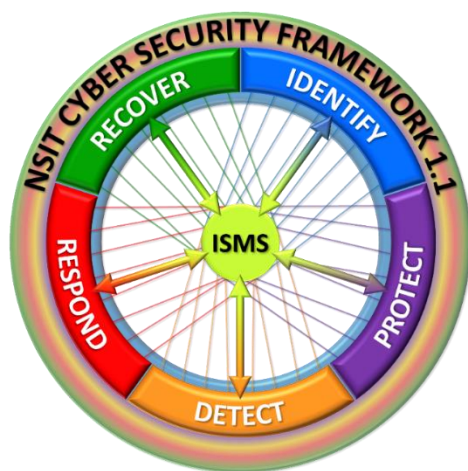


Figure 23: Mise en réseau ISMS avec CSF NIST

(1) La mise en réseau des systèmes de gestion de la sécurité de l'information (ISMS) avec le Cybersecurity Framework (CSF) NIST a du sens, car elle permet une stratégie de sécurité globale et équilibrée. Alors que l'ISMS couvre un large éventail d'aspects de la sécurité, le CSF NIST offre une focalisation spécifique sur les défis de la cybersécurité. L'intégration permet aux entreprises et aux unités organisationnelles de développer à la fois une pratique de sécurité générale robuste et de mettre en œuvre des mesures ciblées pour se prémunir contre les cybermenaces.

(2) L'ISMS fournit un cadre pour la gestion des risques et la mise en œuvre des bonnes pratiques, tandis que le CSF NIST fournit des orientations concrètes en matière de cybersécurité. Cette combinaison améliore la flexibilité et l'adaptabilité, car les entreprises et les unités organisationnelles peuvent intégrer les exigences spécifiques du CSF NIST dans leur ISMS.



- (3) Grâce à cette mise en réseau, les entreprises et les unités organisationnelles peuvent non seulement renforcer la sécurité de leurs informations, mais aussi réagir efficacement aux menaces dynamiques et en constante évolution de l'environnement numérique.
- (4) Voici quelques possibilités de mise en réseau d'un ISMS avec le CSF NIST:
- **Évaluation et gestion des risques:** l'ISMS offre une méthode complète d'identification, d'évaluation et de contrôle des risques. Ces processus peuvent être intégrés de manière transparente dans la composante d'évaluation des risques du NIST CSF afin de garantir une vision cohérente et holistique des risques.
 - **Protection et défense:** l'ISMS contient déjà des pratiques et des contrôles éprouvés pour la protection des systèmes et des données. Ces contrôles peuvent être comparés aux pratiques de protection et de défense du CSF NIST afin de s'assurer que les niveaux de protection sont complets et efficaces.
 - **Détection des événements et réaction:** le ISMS ne contient pas de processus de détection des incidents de sécurité et de réaction à ceux-ci. Ceux-ci peuvent être intégrés aux composantes de détection et de réponse aux incidents de sécurité du CSF NIST afin de garantir que les menaces sont détectées en temps utile et traitées de manière appropriée.
 - **Communication et coordination:** l'ISMS peut prendre en charge la communication interne et la coordination des activités de sécurité. Ces activités peuvent être intégrées dans les composantes de communication et de coordination du CSF NIST afin de garantir que les informations sur les incidents de sécurité sont partagées efficacement.
 - **Surveillance et amélioration:** les deux cadres soulignent l'importance de la surveillance et de l'amélioration continue. La surveillance des métriques de l'ISMS peut être intégrée dans les composantes de surveillance et d'amélioration du CSF NIST afin de garantir que les performances de sécurité sont évaluées et optimisées en permanence.
 - **Communication des risques:** la communication des cyber-risques et des mesures à prendre à la direction et aux parties prenantes est essentielle. Un ISMS peut servir de base à la communication des risques et s'intégrer parfaitement à la composante de communication et de coordination du CSF NIST.
- (5) L'intégration d'un ISMS au CSF NIST permet d'adopter une approche globale de la sécurité de l'information, en combinant les meilleures pratiques et méthodes des deux cadres. Elle garantit que l'organisation répond aux exigences globales de la sécurité de l'information et de la cybersécurité, tout en conservant la flexibilité et l'adaptabilité nécessaires pour répondre à l'évolution des menaces et des risques.



Figure 24 Collaboration (source allegria Blog)

5.4.13 Sécurité de l'information: collaboration

(1) La collaboration visant à accroître la résilience des TIC est essentielle pour garantir que les systèmes et les infrastructures TIC résistent aux perturbations et aux menaces. La résilience des TIC fait référence à la capacité des systèmes TIC à se remettre des perturbations, à se rétablir rapidement et à poursuivre leurs activités. Voici quelques aspects importants de la collaboration pour améliorer la résilience des TIC:

- **Collaboration avec les législateurs, les autorités et les régulateurs:** la collaboration avec les représentants légaux et les autorités est impérieuse sur le plan interdisciplinaire. Cela permet d'aborder et de réagir aux menaces actuelles. Les directives, compléments et adaptations visant à accroître la résilience des TIC peuvent ainsi être élaborés, adoptés et mis en œuvre ensemble de manière réaliste et en temps utile.
- **Collaboration au sein de la branche:** une collaboration nationale et internationale à l'échelle de la branche est essentielle pour accroître la résilience des TIC et doit impérativement être encouragée et maintenue. C'est le seul moyen pour créer et réviser les normes de la branche, et pour trouver un large soutien.
- **Collaboration avec les fabricants et les prestataires de services:** il est impératif de collaborer avec les fournisseurs, les fabricants et les prestataires de services. Cela permet d'augmenter la résilience des TIC dans les différents systèmes et de réagir en temps réel aux menaces actuelles dans les systèmes.



- **Équipes interdisciplinaires:** la résilience des TIC nécessite la collaboration d'experts de différents domaines. Cela inclut notamment les experts informatiques, les spécialistes de la sécurité, les équipes de gestion des urgences et les représentants d'autres services concernés, tels que les RH, le service juridique et la gestion des risques.
 - **Évaluation et gestion des risques:** une compréhension commune des risques et des menaces pesant sur les systèmes TIC est essentielle. Des équipes interdisciplinaires doivent effectuer des évaluations des risques afin d'identifier les vulnérabilités et les menaces spécifiques et de développer des mesures pour réduire les risques.
 - **Préparation et réponse aux situations d'urgence:** les équipes doivent élaborer des plans de préparation aux situations d'urgence afin d'être prêtes à faire face à des perturbations inattendues. Cela implique l'identification des systèmes TIC critiques, l'élaboration de plans d'urgence et la formation du personnel sur la manière de réagir en cas de panne.
 - **Planification de la continuité:** les plans de continuité ne peuvent être élaborés que de manière interdisciplinaire. Ces plans décrivent la manière dont les activités de l'entreprise seront maintenues, même si les systèmes TIC sont affectés. Cela peut inclure l'utilisation de systèmes de sauvegarde, de services cloud et d'autres mécanismes de récupération.
 - **Mesures de sécurité:** la résilience des TIC implique également la mise en œuvre de mesures de sécurité afin de protéger les systèmes contre les menaces. Les équipes de sécurité doivent travailler en étroite collaboration avec les équipes de résilience TIC afin de s'assurer que les mesures de protection sont intégrées dans les plans de résilience.
 - **Technologie et infrastructure:** les équipes TIC doivent surveiller l'infrastructure TIC et s'assurer qu'elle est résistante aux pannes. Cela peut inclure des solutions de haute disponibilité, la redondance et une maintenance régulière.
 - **Formation et sensibilisation:** les employés de différents départements et secteurs devraient être formés et sensibilisés à l'importance de la résilience des TIC et à la manière dont ils peuvent y contribuer.
 - **S'exercer et faire des essais:** des exercices et des essais réguliers des plans d'urgence et de récupération sont essentiels pour garantir l'efficacité des plans de résilience des TIC. Ces exercices doivent simuler des scénarios réalistes et encourager la collaboration entre les unités organisationnelles.
 - **Communication et échange d'informations:** une communication ouverte et efficace entre les équipes est essentielle, en particulier pendant un incident. Les équipes doivent savoir comment échanger des informations et prendre des décisions.
 - **Amélioration continue:** la collaboration visant à accroître la résilience des TIC devrait être un processus continu. Les équipes devraient régulièrement recueillir des informations en retour, analyser les dysfonctionnements et mettre à jour les plans afin d'améliorer continuellement la résilience.
- (2) La collaboration pour une résilience TIC accrue est un effort global qui nécessite l'interaction de différentes unités organisationnelles et d'experts. Il est important que l'organisation considère la résilience TIC comme une partie essentielle de son processus d'entreprise et qu'elle fournisse les ressources et le soutien nécessaires.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Une collaboration intensive et constructive constitue une base essentielle pour accroître la résilience des TIC. Elle doit être mise en place, encouragée, vécue activement et entretenue. Elle doit être vécue et soutenue par la direction.

5.5 Outils pour améliorer la résilience des TIC

- (1) L'utilisation d'outils joue un rôle crucial dans l'augmentation de la résilience TIC des entreprises et des unités organisationnelles. Ces outils comprennent des solutions logicielles, des instruments de surveillance, des plateformes de sécurité et des processus automatisés qui servent à identifier les vulnérabilités, à détecter les attaques et à permettre des réactions rapides aux incidents de sécurité. Ils aident à mettre en œuvre des politiques de sécurité, à effectuer des analyses de risques et à surveiller l'infrastructure TIC en temps réel. L'utilisation de tels outils permet une approche proactive de la sécurité des TIC en contribuant à la détection précoce des menaces potentielles et à la mise en place rapide de contre-mesures. L'intégration de technologies et d'outils avancés permet aux entreprises et aux unités organisationnelles de renforcer leur résistance aux cybermenaces et d'optimiser la protection de leurs technologies de l'information et de la communication.



5.5.1 Outils de l'AES pour accroître la résilience des TIC



Les outils suivants ont été développés et créés par l'AES et sont à la disposition des membres de l'AES pour augmenter la résilience des TIC:

- VSE&BFE-Assement-Tool_NIST-CSF-1.1_++
- VSE&BFE-Tool_for_NIST-CSF-1.1_Checkpoints_acc.to_NIST-SP800-53_CCM_CIS
- VSE-Assessment-Tool_ISO27001-Annex-A_incl._Checkpoints_acc.to_ISO27002
- VSE-Tool_ISO27001-ISMS_Assessment-Goals
- VSE-Tool_NIST-CSF-1.1_HoP-Mapping
- VSE-Tool_ISO27001-Annex-A_HoP-Mapping



Recommandation des experts de la Task Force Cyber Security de l'AES:

Les outils mis à disposition par l'AES doivent être appliqués. Ils aident l'utilisateur à augmenter systématiquement la résilience des TIC.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



Une description détaillée des outils de l'AES se trouve en annexe.



5.5.2 Autres outils disponibles pour aider à augmenter la résilience des TIC



Les outils suivants sont disponibles pour aider à augmenter la résilience des TIC:

- Common Vulnerability Scoring System CVSS
- Light and Right Security ICS (LARS ICS)
- Cybersecurity Evaluation Tool CSET®



Cette énumération n'est pas exhaustive. Il existe d'autres outils qui contribuent à augmenter la résilience des TIC.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

6. Procédure pour augmenter la résilience des TIC: mise en place du ISMS avec mise en réseau du CSF NIST 1.1

- (1) La mise en place d'un système de gestion de la sécurité de l'information (ISMS) avec une mise en réseau systématique avec le CSF NIST 1.1 par étapes a du sens car il offre une approche structurée et globale de la sécurité de l'information dans une organisation. Ceci pour les raisons suivantes:
 - **Planification systématique:** la mise en place progressive permet une planification approfondie de l'ISMS. Cela implique l'identification des objectifs, des ressources et des responsabilités.
 - **Engagement du top management:** grâce à une mise en œuvre progressive, le top management est impliqué dans le processus dès le début. L'engagement de la direction est essentiel à la réussite d'un ISMS, car il fournit des ressources et un soutien.
 - **Processus d'amélioration continue:** l'introduction progressive favorise l'idée d'amélioration continue. Les entreprises et les unités organisationnelles peuvent régulièrement examiner et adapter leurs pratiques de sécurité afin de rester en phase avec l'évolution des menaces et des exigences.
 - **Évaluation des risques:** l'introduction progressive permet une évaluation approfondie des risques. L'identification des risques est essentielle pour mettre en œuvre des mesures de sécurité appropriées.
 - **Allocation adéquate des ressources:** en adoptant une approche progressive, les entreprises et les unités organisationnelles peuvent s'assurer que des ressources suffisantes sont disponibles pour la mise en œuvre et le maintien de l'ISMS.
 - **Intégration dans les processus existants:** l'introduction progressive permet d'intégrer l'ISMS dans les processus commerciaux déjà existants. Cela facilite l'acceptation et la mise en œuvre par les collaborateurs.
 - **Formation et sensibilisation:** l'introduction progressive permet une formation ciblée des employés et une sensibilisation à la sécurité de l'information dans toute l'organisation.
 - **Certification et reconnaissance:** l'introduction progressive pose la première pierre d'une certification selon des normes internationales comme l'ISO 27001. Une telle certification peut renforcer la confiance des clients et des partenaires.
- (2) Dans l'ensemble, l'introduction progressive d'un ISMS avec la mise en réseau du NIST CFS 1.1 permet une mise en œuvre méthodique et bien coordonnée des pratiques de sécurité de l'information. Ceci est particulièrement important dans un monde de plus en plus interconnecté et numérisé, où la sécurité de l'information joue un rôle critique pour le succès de l'entreprise.



(3) La mise en place d'un ISMS avec la mise en réseau du CSF 1.1 du NIST est divisée en huit phases:

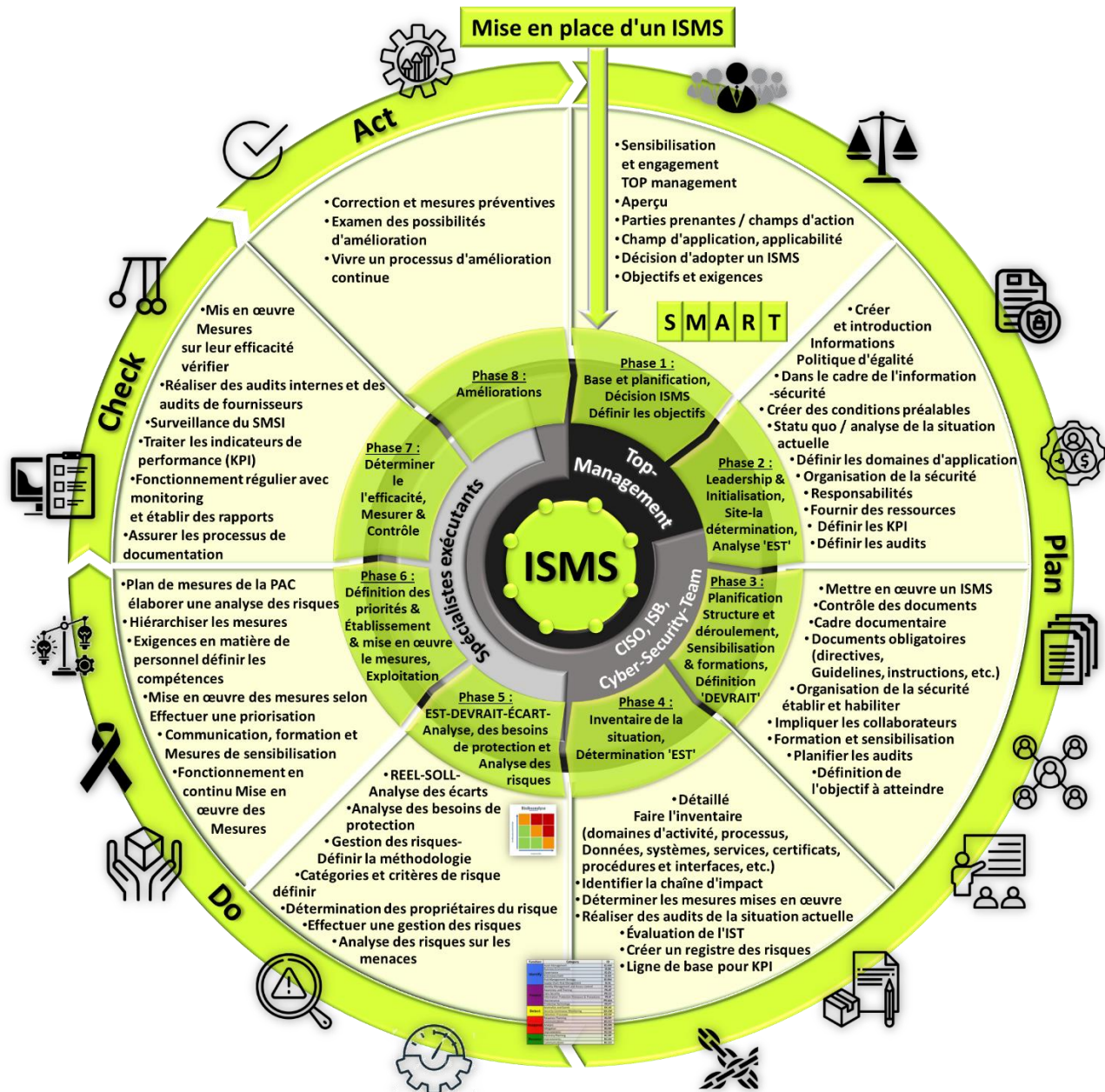


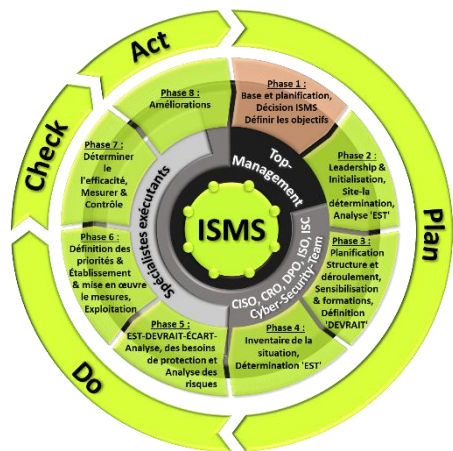
Figure 25: Circuit détaillé des huit phases de l'AES pour la mise en place et l'exploitation de l'ISMS (source AES)

(4) La mise en place d'un système de gestion de la sécurité de l'information (ISMS) en huit phases suit une approche structurée afin de garantir que les pratiques de sécurité de l'information sont développées et mises en œuvre efficacement au sein d'une organisation.



6.1 Phase 1: base et planification; décision d'adopter un ISMS; définition des objectifs

- (1) La base et la planification de la mise en place d'un ISMS constituent un fondement décisif pour la réussite de l'ensemble du projet.



Responsabilité:	Top management, niveau C
Compétence:	Top management, niveau C
Organismes impliqués:	Personnel spécifique de la sécurité de l'information, experts et consultants externes
Points à traiter	<ul style="list-style-type: none">■ Sensibilisation et engagement des cadres supérieurs en matière de sécurité de l'information■ Identification des groupes d'intérêt (stakeholders)■ Présenter et appliquer les exigences légales et réglementaires■ (en particulier les prescriptions selon l'OApEI)■ Définir l'applicabilité (outils d'évaluation)■ Dériver les processus commerciaux■ Mettre en évidence les champs d'action■ Définir / adapter l'objectif de la sécurité de l'information■ Décision de principe pour l'introduction d'un ISMS au niveau du conseil d'administration, de la direction du groupe ou de la direction générale (C-Level)■ Définir et initier les objectifs du ISMS

Tableau 7: Phase 1 ISMS: base et planification; décision d'adopter un ISMS; définition des objectifs

6.1.1 Sensibilisation et engagement des cadres supérieurs en matière de sécurité de l'information

- (1) La sensibilisation et l'engagement de la direction en matière de sécurité de l'information sont essentiels pour garantir la réussite de la mise en œuvre de l'ISMS dans l'ensemble de l'organisation. Ce processus comprend
- **Sensibilisation:** la sensibilisation commence par la création d'une conscience claire de l'importance de la sécurité de l'information. Cela peut se faire par le biais de formations, d'ateliers, de présentations ou d'autres moyens de communication. Il est important que le TOP management comprenne les menaces et les risques actuels pour la sécurité de l'information et soit conscient de l'impact que les incidents de sécurité peuvent avoir sur l'organisation.
 - **Engagement:** la direction doit s'engager activement à soutenir la mise en œuvre du ISMS. Cet engagement se manifeste par la mise à disposition de ressources, l'aide à la définition d'objectifs et de politiques de sécurité ainsi que l'intégration de la sécurité de l'information dans la culture globale de l'entreprise. La direction doit préciser que la sécurité de l'information n'est pas seulement une question technique, mais un élément fondamental de la gestion de l'entreprise.
- (2) La sensibilisation et l'engagement de la direction constituent la base de l'approche globale de la sécurité de l'information de l'entreprise et des unités organisationnelles. Si la direction comprend l'importance de la sécurité de l'information et s'engage à soutenir les mesures correspondantes, la probabilité d'une mise en place et du maintien du ISMS augmente considérablement. Ce soutien est également essentiel pour sensibiliser et motiver les collaborateurs à la sécurité de l'information à tous les niveaux de l'organisation.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-00: Politique de gestion et d'entrepreneuriat
- HoP-01-00: Directive sur la gestion des affaires



Les experts de la Task Force Cyber Security de l'AES recommandent de faire appel à un expert externe pour sensibiliser et engager les cadres supérieurs à la sécurité de l'information. Grâce à une exécution adaptée au management, l'affinité et l'obligation peuvent ainsi être mieux expliquées. Il est très important que la sécurité de l'information soit soutenue et encouragée de manière globale par le niveau de direction le plus élevé.



6.1.2 Identification des groupes d'intérêt (stakeholders)

- (1) L'identification des parties prenantes, également appelées stakeholders, est une étape essentielle dans le cadre de la mise en place d'un ISMS. Ces parties prenantes jouent un rôle crucial dans la définition, la mise en œuvre et le maintien du ISMS. Voici les étapes de l'identification des parties prenantes:
- **Analyse de la structure organisationnelle:** la structure organisationnelle doit être analysée afin d'identifier les acteurs clés et les départements qui ont une influence directe sur la sécurité de l'information. Cela inclut typiquement la direction, les départements IT/OT, les responsables de la sécurité, les départements de la conformité et d'autres domaines pertinents.
 - **Exigences légales et réglementaires:** l'identification des parties prenantes passe également par l'analyse des exigences légales et réglementaires. Celles-ci peuvent comprendre des dispositions relatives à la sécurité des données, des règles de protection des données ou des réglementations spécifiques à un secteur. Les autorités ou organes de contrôle correspondants sont considérés comme des parties prenantes importantes.
 - **Partenaires internes et externes:** les partenaires externes tels que les clients, les fournisseurs et les prestataires de services peuvent également être considérés comme des parties prenantes, en particulier s'ils ont accès à des informations sensibles. Les partenaires internes impliqués dans les processus commerciaux doivent également être pris en compte.
 - **Employés:** les employés à tous les niveaux de l'organisation sont des parties prenantes essentielles. Cela comprend non seulement le personnel informatique, mais aussi les employés d'autres unités organisationnelles, car ils peuvent tous contribuer à la sécurité des informations ou être concernés par celle-ci.
 - **Direction et propriétaires:** la direction et les propriétaires de l'organisation sont d'une importance capitale. Leur engagement et leur soutien sont essentiels à la réussite du ISMS. Il est donc essentiel d'identifier les décideurs clés et de les impliquer.
 - **Les parties prenantes externes:** les parties prenantes externes telles que les clients, les investisseurs, les actionnaires et le public peuvent avoir un intérêt dans la sécurité de l'information de l'organisation. Leurs attentes et exigences doivent être prises en compte.
 - **Évaluation des risques:** une évaluation des risques peut également aider à identifier les parties prenantes potentielles en analysant quelles parties pourraient être les plus touchées par les risques de sécurité.
- (2) L'identification des parties prenantes est un processus itératif qui nécessite une analyse minutieuse de l'organisation et de son environnement. Les besoins et les attentes de ces parties prenantes sont pris en compte dans les différentes phases du projet ISMS afin de s'assurer que leurs intérêts sont correctement adressés.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information



Recommandation des experts de la Task Force Cyber Security de l'AES:

Des formations de sensibilisation dispensées par un expert externe permettent d'obtenir la compréhension, l'acceptation et le soutien des parties prenantes. Les parties prenantes doivent être conscientes de la portée d'une politique de sécurité de l'information cohérente. Elles portent une grande responsabilité et il faut exiger et encourager leur participation et leur collaboration constructive. Toutes les parties prenantes doivent être conscientes de leur rôle en matière de sécurité de l'information!

6.1.3 Présenter et appliquer les exigences légales et réglementaires

- (1) Toutes les exigences légales et réglementaires en matière de sécurité de l'information qui s'appliquent à une entreprise et à ses unités organisationnelles doivent être identifiées, présentées et respectées. Dans ce guide, toutes les exigences légales et réglementaires sont énumérées en annexe. Celles-ci doivent être ancrées par les entreprises et les unités organisationnelles dans une directive correspondante. Grâce à la formation et à la sensibilisation, tous les services impliqués sont informés de ces directives.





Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'identification et l'application des exigences légales et réglementaires dans le cadre de la sécurité de l'information sont importantes pour garantir que l'entreprise se conforme aux exigences légales, assure la protection des données et minimise les risques juridiques potentiels.

6.1.4 Définir l'applicabilité (outils d'évaluation)

- (1) L'applicabilité détermine le champ d'application fondamental de la sécurité de l'information. Il s'agit pour les entreprises et les unités organisationnelles d'analyser et de déterminer comment les différents contrôles doivent être appliqués ou traités.

Applicabilité des contrôles du CSF NIST 1.1:

- (2) L'applicabilité du CSF NIST 1.1 se réfère à l'efficacité et à la polyvalence de l'application du framework dans différentes entreprises, unités organisationnelles et scénarios. Cette applicabilité repose sur la capacité du framework à aider les entreprises et les unités organisationnelles à identifier, protéger et détecter les incidents de sécurité, à y répondre de manière appropriée et à restaurer les infrastructures TIC après des interruptions ou des pannes dues à des cyberattaques.
- (3) La version 1.1 du CSF NIST fournit les meilleures pratiques et les lignes directrices pour le développement et l'amélioration des stratégies de cybersécurité. L'applicabilité du framework est démontrée par le fait que le cadre est suffisamment flexible pour être appliqué à différents secteurs, tailles d'entreprises et d'unités organisationnelles et paysages de menaces spécifiques.
- (4) Le framework permet aux entreprises et aux unités organisationnelles d'identifier leurs risques et actifs individuels, de mettre en œuvre des mesures de protection appropriées, de réagir rapidement aux menaces, de développer des plans de récupération efficaces après un incident et d'améliorer continuellement leurs pratiques de cybersécurité.
- (5) L'applicabilité du CSF NIST 1.1 s'étend à différents domaines puisqu'il sert de cadre à une stratégie globale de cybersécurité. Il permet aux entreprises et aux unités organisationnelles d'adapter le cadre à leurs besoins spécifiques tout en maintenant une approche cohérente et globale de la cybersécurité.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information



Pour définir l'applicabilité des contrôles dans le CSF NIST 1.1, on peut utiliser «VSE&BFE-Assessment-Tool_NIST-CSF-1.1_++».



En annexe se trouve une description détaillée pour l'«outil d'évaluation norme minimale TIC AES & OFEN-TIC++» et l'«outil d'évaluation AES_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.

«Statement of Applicability» (SoA) pour la norme ISO 27001:

- (6) «Statement of Applicability» (SoA) est un document important dans le contexte de l'ISO/ 27001.) La déclaration d'applicabilité sert à définir le champ d'application et les détails de la manière dont une organisation va mettre en œuvre les exigences de l'ISO 27001 pour protéger ses actifs informationnels. Voici une ventilation des principaux éléments de la «Statement of Applicability»:
 - **1. Champ d'application:** le SoA commence par une déclaration claire sur le champ d'application du ISMS. Elle définit les limites des valeurs d'information couvertes et la mesure dans laquelle les exigences de l'ISO 27001 sont appliquées.
 - **2. Objectifs de contrôle et contrôles applicables:** l'objectif principal du SoA est d'énumérer les objectifs de contrôle et les contrôles spécifiques de la norme ISO 27001 que l'organisation a mis en place.



Ces contrôles sont sélectionnés sur la base d'une évaluation des risques et du contexte individuel de l'organisation. Le SoA contient le numéro de chaque contrôle, son titre et une brève description de la manière dont il est appliqué.

- **3. Justification des exclusions:** s'il existe des objectifs de contrôle ou des contrôles que l'organisation a décidé de ne pas mettre en œuvre, le SoA devrait fournir une justification claire de ces exclusions. Cela est souvent lié à une évaluation des risques, dans laquelle l'organisation détermine qu'un contrôle particulier n'est pas nécessaire ou réalisable dans son contexte.
 - **4. Contrôles supplémentaires:** dans certains cas, les entreprises et les unités organisationnelles peuvent mettre en œuvre des contrôles supplémentaires qui ne sont pas explicitement mentionnés dans l'ISO 27001. Ceux-ci peuvent être ajoutés au SoA, ainsi que leurs descriptions et justifications.
 - **5. Compétence et responsabilités des contrôles:** le SoA peut également indiquer qui est responsable de la mise en œuvre et du maintien de chaque contrôle. Cela permet de s'assurer qu'il existe une responsabilité au sein de l'organisation pour chaque contrôle.
 - **6. Processus de révision et de mise à jour:** le document doit présenter le processus de révision et de mise à jour régulière de l'«énoncé d'applicabilité». Cela permet de s'assurer que le ISMS reste efficace lorsque le contexte et les risques de l'organisation évoluent.
- (7) Le «Statement of Applicability» est un document dynamique qui doit être régulièrement revu et mis à jour afin de refléter les changements dans l'environnement de sécurité de l'information de l'organisation et l'évolution des profils de risque. C'est un outil indispensable pour les entreprises et les unités organisationnelles qui souhaitent obtenir la certification ISO 27001, car il permet de comprendre clairement comment les contrôles de sécurité de l'information sont appliqués dans l'organisation.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information



Pour le SoA selon la norme ISO 27001 Annexe A, il convient d'utiliser l'outil «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».



En annexe se trouve une description détaillée pour «VSE&BFE-Assement-Tool_NIST-CSF-1.1_++» et «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

6.1.5 Mise en évidence et déclinaison des processus commerciaux

- (1) La représentation des processus d'entreprise en rapport avec la sécurité de l'information implique une analyse approfondie et une identification de toutes les activités et procédures au sein d'une organisation qui peuvent influencer la sécurité des informations. Ce processus est essentiel pour comprendre les risques potentiels et mettre en place des mesures de protection efficaces. Pour commencer, tous les processus commerciaux pertinents qui traitent, stockent ou transmettent des données sont identifiés. Cela inclut toutes les activités qui ont un lien direct avec des informations sensibles. L'analyse se concentre sur la manière dont les informations circulent au sein de ces processus, depuis leur origine jusqu'à leur transmission, en passant par leur traitement et leur stockage.
- (2) L'étape suivante consiste en une évaluation approfondie des risques. Cela comprend l'identification des vulnérabilités et des menaces qui mettent en péril l'intégrité, la confidentialité et la disponibilité des informations. L'évaluation des risques permet de déterminer la probabilité et l'impact des incidents de sécurité. Sur la base des résultats de l'évaluation des risques, des mesures de protection ciblées sont développées et mises en œuvre. Celles-ci peuvent être de nature technique, organisationnelle ou personnelle et visent à garantir la sécurité des processus commerciaux et des informations qui y sont traitées.
- (3) Il est important d'intégrer les politiques et les procédures de sécurité dans les processus d'entreprise. Cela permet de garantir que les aspects de sécurité sont pris en compte dès le départ et que les collaborateurs les observent dans leurs activités quotidiennes. La surveillance des processus commerciaux est un



processus continu. Cela garantit que les mesures de sécurité mises en œuvre sont efficaces et peuvent être adaptées si nécessaire pour répondre à l'évolution des menaces ou des besoins commerciaux.

- (4) Dans l'ensemble, la présentation complète des processus commerciaux dans le contexte de la sécurité de l'information contribue à développer une compréhension approfondie des exigences de sécurité d'une organisation et à garantir que des mesures de protection appropriées sont mises en œuvre pour assurer l'intégrité, la confidentialité et la disponibilité des informations.

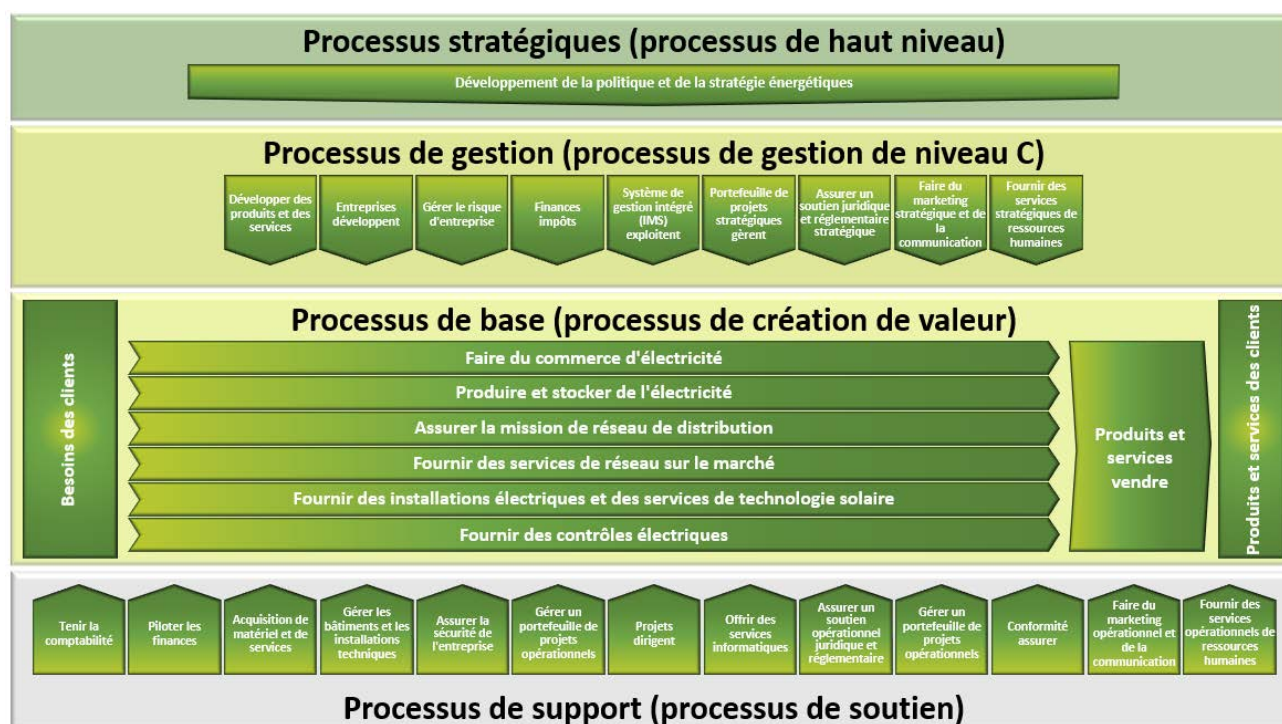


Figure 26: Processus dans les entreprises et les unités organisationnelles (source AES)

- (5) Les processus d'une organisation qui sont liés à la sécurité de l'information doivent être identifiés, identifiés et inventoriés en conséquence. Les entreprises et les unités organisationnelles doivent ancrer cela dans une directive correspondante. Grâce à la formation et à la sensibilisation, tous les services impliqués sont informés de ces directives.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS
- HoP-01-01-03-03 Guide de travail Domaine ISMS: Gestion des actifs et classification des informations



Recommandation des experts de la Task Force Cyber Security de l'AES:

La mise en évidence et la déduction des processus commerciaux pour la sécurité de l'information sont importantes pour comprendre les exigences et les risques spécifiques liés aux différentes activités de l'entreprise et pour développer des mesures de sécurité ciblées qui soutiennent et protègent les objectifs commerciaux. Les processus ne doivent pas se limiter à aux prescriptions faites dans l'OApEI. Il est recommandé d'introduire une ligne de base pour tous les processus de sécurité de l'information.

6.1.6 Identifier les champs d'action pour la sécurité de l'information

- (1) La définition des champs d'action pour la sécurité de l'information sur la base des processus commerciaux s'effectue par un processus minutieux d'analyse, d'identification et de catégorisation afin de garantir que tous les aspects pertinents de la sécurité de l'information sont pris en compte. Tout commence par une analyse approfondie des processus d'entreprise afin d'identifier toutes les activités liées au traitement, au stockage ou à la transmission d'informations. Cette analyse permet de comprendre les flux d'informations au sein de l'organisation et d'identifier les processus qui sont particulièrement critiques pour la sécurité de l'information.



- (2) Après l'identification de ces processus commerciaux critiques, une évaluation des risques est effectuée. Les points faibles potentiels, les menaces et les risques sont alors analysés afin de déterminer quels aspects de la sécurité de l'information sont les plus menacés. Cette évaluation aide à hiérarchiser les champs d'action et à définir les priorités pour les mesures de sécurité. La définition des champs d'action se réfère ensuite à des mesures concrètes qui doivent être prises pour réduire les risques identifiés. Il peut s'agir de l'introduction de mesures techniques de sécurité, de la mise en œuvre de politiques et de procédures de sécurité, de formations pour les employés ou d'adaptations organisationnelles.
- (3) Les champs d'action peuvent se concentrer sur différents domaines, tels que la protection contre les accès non autorisés, la garantie de l'intégrité des données, la disponibilité des systèmes critiques ou la mise en œuvre de plans de reprise après sinistre. La définition de ces champs d'action se fait en étroite collaboration avec les objectifs de l'organisation et les exigences spécifiques de ses processus commerciaux. Il s'agit d'un processus itératif qui nécessite un suivi et une adaptation continus.
- (4) Les domaines d'action peuvent évoluer au fil du temps, notamment à la lumière de l'évolution du paysage des menaces, des nouvelles technologies ou des exigences commerciales. Cette approche itérative permet de garantir que la sécurité de l'information est continuellement améliorée et qu'elle réagit aux circonstances actuelles.
- (5) Les champs d'action pour la sécurité de l'information doivent être définis par les entreprises et les unités organisationnelles et être documentés en conséquence.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS
- HoP-01-01-03-03 Guide de travail Domaine ISMS: Gestion des actifs et classification des informations



Recommandation des experts de la Task Force Cyber Security de l'AES:

Les champs d'action ne doivent pas être limités aux prescriptions de l'OApEI. Il est recommandé d'introduire une ligne de base pour tous les champs d'action de la sécurité de l'information.

6.1.7 Définir / adapter l'objectif de la sécurité de l'information

- (1) Les prescriptions de l'ordonnance sur l'électricité définissent l'orientation de la sécurité de l'information des entreprises et unités organisationnelles critiques pour l'approvisionnement:

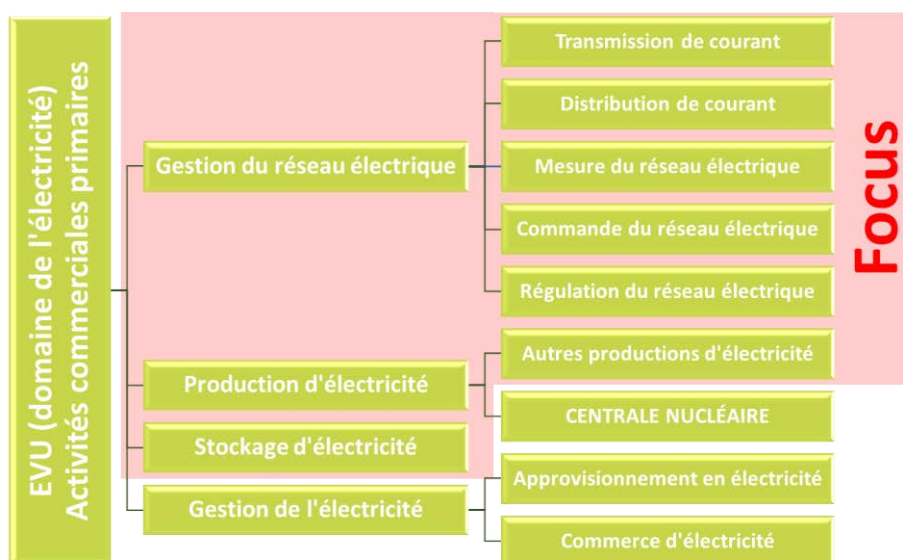


Figure 27: Détermination du point focal selon l'OApEI (source AES)



- (2) Chaque entreprise et chaque unité organisationnelle doit définir où se situent ses activités commerciales primaires. Les activités commerciales¹ suivantes sont considérées comme pertinentes dans ce guide et seront traitées plus en détail:
- **Gestion du réseau électrique:** la gestion du réseau électrique comprend la planification, l'exploitation, la surveillance et le contrôle des réseaux électriques pour un approvisionnement en électricité fiable. Elle comprend la planification et la conception du réseau, l'exploitation quotidienne du réseau ainsi que la sécurité du réseau et l'intégration de solutions d'énergie renouvelable. L'objectif est d'assurer une alimentation électrique stable, de minimiser les pannes et de répondre aux exigences d'efficacité énergétique et de durabilité grâce à une coordination complexe des infrastructures.
 - **Production d'électricité:** la production d'électricité génère de l'énergie électrique à partir de différentes sources, dont les combustibles fossiles, les énergies renouvelables comme le vent et le soleil, l'énergie hydraulique et l'énergie nucléaire. Ce processus peut être centralisé ou décentralisé, en fonction des technologies et de la structure du réseau. L'efficacité et l'impact environnemental dépendent de la source d'énergie et de la technologie. L'objectif est un approvisionnement en électricité fiable et durable, nécessite une planification minutieuse, des investissements dans les infrastructures et une intégration renouvelable.
 - **Stockage de l'électricité:** le stockage de l'énergie est essentiel pour l'économie énergétique moderne, il permet de stocker et d'appeler l'énergie électrique en cas de besoin. Cela comprend différentes méthodes telles que les batteries, les centrales de pompage-turbinage et le stockage thermique. Le stockage permet de compenser les fluctuations de la demande en énergie, de soutenir les énergies renouvelables et d'améliorer la stabilité du réseau. Les technologies efficaces de stockage de l'énergie contribuent à améliorer l'efficacité énergétique et la durabilité, et jouent un rôle clé dans la transformation du secteur énergétique.
- (3) La sécurité de l'information ne doit toutefois pas se concentrer uniquement sur le point focal défini. La sécurité de l'information doit couvrir l'ensemble de l'organisation de manière globale.
- (4) L'accent mis sur la sécurité de l'information doit être défini par les entreprises et les unités organisationnelles et documenté en conséquence.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS
- HoP-01-01-03-03 Guide de travail Domaine ISMS: Gestion des actifs et classification des informations



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'accent doit certes être mis sur les prescriptions de l'ordonnance sur l'électricité. Néanmoins, tous les domaines de la sécurité de l'information doivent être couverts. Il est recommandé d'introduire une ligne de base pour tous les domaines de la sécurité de l'information.

6.1.8 Décision de principe pour l'introduction d'un ISMS au niveau du groupe ou de la direction (niveau C)

- (1) La décision de principe d'introduire un système de gestion de la sécurité de l'information (ISMS) au niveau C, c'est-à-dire au niveau du groupe ou de la direction, est d'une importance stratégique. Cette décision reflète la reconnaissance de l'importance de la sécurité de l'information pour l'organisation. Elle montre la compréhension du fait que la protection des informations sensibles et la garantie de la résilience des TIC sont essentielles pour les activités commerciales et la réputation de l'entreprise et des unités organisationnelles.
- (2) La démarche de mise en œuvre d'un ISMS au plus haut niveau de la direction signale l'engagement en faveur d'une approche globale et systématique de la sécurité de l'information. Elle montre que la direction est prête à allouer les ressources nécessaires pour établir un ISMS efficace. Cette décision de principe reflète également la prise de conscience des menaces croissantes dans le paysage numérique et la nécessité de prendre des mesures de protection proactives.

¹ Selon la définition de l'ordonnance sur l'électricité



- (3) La direction pose ainsi la première pierre d'une culture de la sécurité au sein de l'organisation et fixe des priorités claires en matière de sécurité de l'information. Cette décision va au-delà des simples questions technologiques et concerne la stratégie globale de l'entreprise, car la sécurité de l'information est étroitement liée aux processus commerciaux, aux exigences de conformité et à la protection des actifs de l'entreprise. Globalement, la décision de principe d'introduire un ISMS au niveau C reflète la reconnaissance que la sécurité de l'information n'est pas seulement une question informatique, mais qu'elle a une influence décisive sur le succès global de l'entreprise.



Les documents suivants contiennent des orientations et des instructions:

- Norme BSI 200-1 Systèmes de gestion de la sécurité de l'information (ISMS)



La mise en place d'un ISMS nécessite des ressources considérables dans les entreprises et les unités organisationnelles. L'effort à fournir ne doit pas être sous-estimé. Ces circonstances doivent impérativement être prises en compte lors de la décision d'introduire un ISMS.



Recommandation des experts de la Task Force Cyber Security de l'AES:

La décision de principe de mettre en place un ISMS au niveau C est importante pour souligner l'importance de la sécurité de l'information pour l'ensemble de l'entreprise, mobiliser les ressources et assurer un leadership et un soutien clairs pour la mise en œuvre du ISMS.

6.1.9 Définir et initier les objectifs du ISMS



(1) La définition des objectifs du système de gestion de la sécurité de l'information devrait répondre aux critères SMART. Cela signifie qu'ils doivent être spécifiques (Specific), mesurables (Measurable), atteignables (Achievable), pertinents / réalistes (Relevant) et temporellement définis (Time-bound).

- (2) Des objectifs spécifiques définissent clairement les aspects de la sécurité de l'information qui sont concernés. Ils doivent être mesurables afin de pouvoir contrôler les progrès et évaluer le succès. En outre, les objectifs doivent être atteignables et réalistes afin de permettre leur mise en œuvre. La pertinence garantit que les objectifs contribuent directement à la sécurité de l'information et soutiennent les objectifs généraux de l'entreprise. Les objectifs temporels garantissent que les objectifs sont atteints dans un délai défini.
- (3) Ces objectifs SMART servent de lignes directrices pour la planification et la mise en œuvre des mesures de sécurité dans le cadre de l'ISMS. Ils permettent d'orienter précisément les efforts vers des objectifs de sécurité concrets afin de renforcer la sécurité de l'information de manière efficace et mesurable.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS



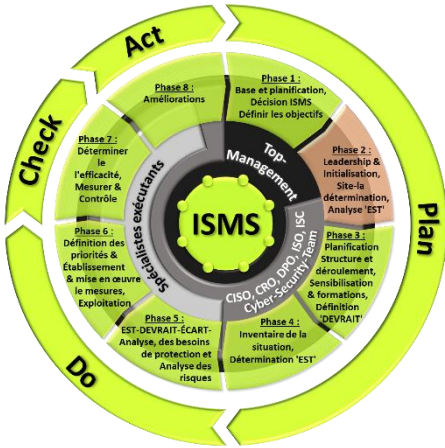
Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est important de définir les objectifs du ISMS selon le principe SMART afin de s'assurer qu'ils sont spécifiques, mesurables, réalisables, pertinents et datés, ce qui augmente leur efficacité dans l'amélioration de la sécurité de l'information et établit des lignes directrices claires pour leur réussite.



6.2 Phase 2: direction et initialisation; état des lieux

- (1) La deuxième phase de la mise en place d'un ISMS aborde les domaines de la direction et de l'initialisation ainsi que l'évaluation de la situation:



Responsabilité:	Top management, niveau C
Compétence:	Top management, niveau C
Organismes impliqués:	CISO, CRO, DPO, ISO, ISC, équipe de cybersécurité Experts et consultants externes
Points à traiter	<ul style="list-style-type: none">Créer et mettre en place la politique et la stratégie de sécurité de l'information: Comment traiter la sécurité de l'information?Définir le cadre de la sécurité de l'informationCréation des conditions préalablesDéterminer le statu quo / effectuer une analyse de la situation actuelle dans le domaine de la sécurité de l'informationDéfinir le champ d'application de la sécurité de l'information selon les directives de l'OApEIDéfinir un champ d'application supplémentaire pour la sécurité de l'informationDéfinir le champ d'application de l'ISMSMettre en place / adapter l'organisation de la sécuritéDéfinir / adapter les responsabilitésDéfinir des indicateurs de performance (KPI)Définir une procédure pour les audits

Tableau 8: Phase 2 ISMS: direction et initialisation; état des lieux

6.2.1 Créer et mettre en place la politique et la stratégie de sécurité de l'information: Comment traiter la sécurité de l'information ?

- (1) La création et la mise en place d'une politique et d'une stratégie de sécurité de l'information est une étape clé pour la sécurité des données de l'entreprise. Ce processus implique l'élaboration de lignes directrices et de stratégies claires visant à garantir la confidentialité, l'intégrité et la disponibilité des informations et à soutenir les objectifs généraux de l'entreprise. Cette politique de sécurité définit les principes et objectifs fondamentaux, tandis que la stratégie fournit des moyens concrets pour atteindre ces objectifs. L'intégration de ces documents dans les opérations de l'entreprise et la communication à toutes les parties prenantes sont essentielles pour sensibiliser à la sécurité de l'information et garantir une mise en œuvre cohérente.
- (2) Il est important de noter qu'une stratégie de sécurité doit être conçue sur mesure afin de répondre aux besoins et aux risques spécifiques d'une entreprise et de ses unités organisationnelles. En outre, la collaboration avec des experts en sécurité et le respect des bonnes pratiques sont essentiels pour élaborer et mettre en œuvre une stratégie de sécurité efficace.

Les documents suivants aident l'utilisateur à élaborer et à mettre en place la politique et la stratégie de sécurité de l'information:



- Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC) d'avril 2023
- Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC) 2018-2022
- Plan de mise en œuvre de la Stratégie nationale pour la protection de la Suisse contre les cyber- risques (SNPC) 2018-2022
- Évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyber- risques pour les années 2018 à 2022
- Sécurité intégrée pour l'Allemagne, Stratégie de sécurité nationale



Recommandation des experts de la Task Force Cyber Security de l'AES:

La création et la mise en place d'une politique et d'une stratégie de sécurité de l'information sont essentielles pour établir des lignes directrices claires qui constituent la base de la sécurisation de l'information et permettent d'orienter toutes les activités et mesures vers cet objectif.



6.2.2 Définir le cadre de la sécurité de l'information: Créer une directive sur la sécurité de l'information et une directive sur le cadre de la sécurité de l'information.

- (1) La définition du cadre de la sécurité de l'information est une étape nécessaire pour créer un contexte clair pour la protection de l'information. Ce processus comprend la définition d'aspects clés tels que les responsabilités, les objectifs et le champ d'application de la sécurité de l'information. Le cadre constitue la base des politiques, procédures et mesures visant à garantir la confidentialité, l'intégrité et la disponibilité des données. Une définition claire du cadre fournit une base solide pour la gestion globale de la sécurité de l'information et contribue à l'élaboration d'une stratégie de sécurité cohérente et efficace.
- (2) La création d'une directive sur la sécurité de l'information nécessite une analyse approfondie des besoins et des risques de votre organisation. Elle doit fournir des instructions et des principes clairs en matière de sécurité de l'information et être rédigée et soutenue par la direction.
- (3) La création d'une politique pour le cadre de la sécurité de l'information est une étape clé pour établir des lignes directrices claires pour la protection des données de l'entreprise. Cette politique définit le contexte dans lequel la sécurité de l'information opère, y compris les responsabilités, les objectifs et le champ d'application. Elle constitue l'ensemble de règles de base sur lequel se basent les autres mesures de sécurité. Une politique bien conçue garantit que toutes les parties concernées ont une compréhension commune des exigences de sécurité et favorise une mise en œuvre cohérente des mesures de sécurité de l'information dans l'ensemble de l'entreprise et des unités organisationnelles.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information ISM
- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information



Les documents suivants aident l'utilisateur à élaborer et à introduire une politique de sécurité de l'information et la politique du domaine de la sécurité de l'information:

- NIST SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security
- Norme BSI 100-2: Procédure de protection informatique de base



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est important d'établir un cadre pour la sécurité de l'information afin de définir les principes de base, les objectifs et les responsabilités en matière de protection de l'information et de s'assurer que toutes les mesures de sécurité sont appliquées de manière cohérente et efficace.

6.2.3 Création des conditions préalables

- (1) La création des conditions nécessaires à la mise en place et à l'exploitation d'un système de gestion de la sécurité de l'information (ISMS) est une étape importante pour garantir la sécurité des données de l'entreprise. Ce processus implique la mise à disposition des ressources nécessaires, la définition des responsabilités et l'établissement d'un cadre clair pour l'ISMS. L'établissement de ces bases garantit que l'ISMS peut être mis en œuvre efficacement et exploité à long terme. Une préparation minutieuse pose les bases de la réussite du système de gestion de la sécurité de l'information et garantit une protection complète des informations.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information



La mise en place d'un ISMS nécessite des ressources considérables dans les entreprises et les unités organisationnelles. L'effort à fournir ne doit pas être sous-estimé. Il convient de tenir compte de ces circonstances lors de la mise en place des conditions préalables.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est important de créer les conditions nécessaires à la mise en place et au fonctionnement d'un système de gestion de la sécurité de l'information (ISMS) afin de garantir une approche structurée et efficace de la sécurité de l'information, de promouvoir le respect des normes et de renforcer la confiance des parties prenantes.



6.2.4 Déterminer le statu quo / effectuer une analyse de la situation actuelle dans le domaine de la sécurité de l'information

- (1) La détermination du statu quo ou l'analyse de la situation actuelle dans le domaine de la sécurité de l'information est une étape fondamentale pour comprendre l'état actuel des pratiques de sécurité. Ce processus implique une analyse approfondie des mesures de sécurité existantes, des points faibles et des politiques. L'analyse de l'état actuel permet d'identifier les forces et les faiblesses dans le domaine de la sécurité afin de créer une base solide pour le développement de stratégies de sécurité. Une détermination précise de l'état actuel permet de planifier et de mettre en œuvre des mesures ciblées pour améliorer la sécurité de l'information.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine ISM: Cadre de la sécurité de l'information



Le «VSE&BFE-Assement-Tool_NIST-CSF-1.1_++» doit être utilisé pour le statu quo / l'analyse de la situation actuelle dans le domaine de la sécurité de l'information des contrôles dans le cadre du CSF NIST 1.1.



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.



Pour le statu quo / l'analyse de la situation actuelle dans le domaine de la sécurité de l'information des contrôles dans le cadre de l'ISO 27001 Annexe A, il convient d'utiliser l'outil «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



En annexe se trouve une description détaillée pour «VSE&BFE-Assement-Tool_NIST-CSF-1.1_++» et «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».

6.2.5 Définir le champ d'application du ISMS dans son ensemble

- (1) La définition du champ d'application dans le cadre de la sécurité de l'information est une étape essentielle de la mise en œuvre d'un système de gestion de la sécurité de l'information. Il s'agit de définir précisément quelles parties de l'organisation et quels systèmes d'information sont pris en compte dans l'ISMS. Ce processus comprend l'identification des actifs, des processus opérationnels et des partenaires externes qui entrent dans le champ d'application de l'ISMS.
- (2) Une définition claire du champ d'application crée la base pour le développement de politiques et de mesures de sécurité. Cette définition permet d'identifier et d'évaluer les risques de manière appropriée et de mettre en œuvre les mesures de protection adéquates. Cela contribue à développer une stratégie de sécurité de l'information efficace et ciblée et à garantir que tous les domaines pertinents de l'organisation sont protégés de manière adéquate.
- (3) Il est important de souligner que le champ d'application n'est pas statique et qu'il peut être nécessaire de l'adapter au fil du temps. Des changements dans la structure organisationnelle, les processus commerciaux ou le paysage des menaces peuvent nécessiter une adaptation du champ d'application. Il est donc important de vérifier régulièrement le champ d'application et de l'adapter si nécessaire.
- (4) La définition du champ d'application constitue la base du développement des objectifs de sécurité, de la mise en œuvre des mesures de sécurité et de la réalisation d'audits dans le cadre de l'ISMS. Un champ d'application clairement défini permet à l'organisation de cibler ses efforts en matière de sécurité de l'information sur les domaines pertinents et de s'assurer que l'ISMS est utilisé de manière efficace et efficiente.
- (5) Le champ d'application de la sécurité de l'information pour les entreprises et les unités organisationnelles est défini par les prescriptions de l'ordonnance sur l'électricité et doit donc être repris ou couvert par les entreprises et les unités organisationnelles.



- (6) Les entreprises et les unités organisationnelles doivent décider si elles ne limiteront pas le champ d'application de la sécurité de l'information aux seules prescriptions de l'ordonnance sur l'électricité.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-02-01: Directive Domaine de la sécurité de l'information: cadre de la sécurité de l'information
- HoP-01-01-02: Directive Domaine de la sécurité de l'information: champ d'application, mise en place et fonctionnement de l'ISMS



Les experts de la Task Force Cyber Security de l'AES recommandent d'étendre le champ d'application de la sécurité de l'information à l'ensemble de l'entreprise et de ne pas le limiter aux seules prescriptions de l'OApEI. Tous les domaines de l'entreprise doivent être couverts de manière globale et complète. Il faut décider si les prescriptions de l'OApEI doivent être reprises pour l'ensemble du domaine de la sécurité de l'information ou si des prescriptions propres doivent être définies pour les domaines non réglementés par l'OApEI.

6.2.6 Mettre en place et adapter l'organisation de la sécurité

- (1) La mise en place d'une organisation de la sécurité visant à accroître la résilience des TIC est essentielle pour garantir la résistance des entreprises et des unités organisationnelles aux perturbations, aux catastrophes et aux menaces de sécurité dans le domaine numérique. Une structure typique d'une organisation de la sécurité dans le contexte de l'augmentation de la résilience des TIC est présentée au point 5.4.7.
- (2) La structure et les responsabilités exactes peuvent varier selon les entreprises et les unités organisationnelles et doivent être adaptées aux besoins et aux risques spécifiques des entreprises et des unités organisationnelles. Une organisation de la sécurité bien coordonnée et axée sur la résilience des TIC est essentielle pour garantir que l'entreprise et les unités organisationnelles sont en mesure de réagir efficacement aux perturbations des TIC et aux menaces pour la sécurité et de maintenir leurs activités numériques.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-02-01: Directive Domaine de la sécurité de l'information: cadre de la sécurité de l'information
- HoP-01-01-02: Directive Domaine de la sécurité de l'information: champ d'application, mise en place et fonctionnement de l'ISMS



Recommandation des experts de la Task Force Cyber Security de l'AES:

Lors de la mise en place de l'organisation de la sécurité, tous les éléments de la sécurité de l'information doivent être couverts. Cela implique également de définir les interfaces avec les parties prenantes externes telles que les fabricants / fournisseurs, le SOC, le CERT, etc.

6.2.7 Définir / adapter les responsabilités

- (1) La définition des responsabilités dans le cadre de la sécurité de l'information et du système de gestion de la sécurité de l'information (ISMS) est une étape importante pour garantir que tous les acteurs concernés comprennent et remplissent des rôles et des responsabilités clairs dans le contexte de la sécurité. Ce processus commence souvent par l'identification des acteurs clés et de leurs tâches spécifiques.
- (2) La définition des responsabilités commence au plus haut niveau de la direction. La direction ou le top management assume la responsabilité globale de la sécurité des systèmes d'information. Cela inclut la définition des politiques de sécurité, des objectifs et de l'allocation des ressources.
- (3) Au niveau suivant, les responsables de la sécurité ou Information Security Officer (ISO) sont souvent chargés de la mise en œuvre et du suivi de la stratégie de sécurité de l'information. Ils veillent à ce que les consignes de sécurité soient appliquées au niveau opérationnel.
- (4) Les responsables IT/OT jouent également un rôle clé, car ils sont responsables de la mise en œuvre technique des mesures de sécurité, de la protection des systèmes et du contrôle de l'accès aux données. Les administrateurs réseau, les administrateurs système et d'autres équipes techniques peuvent avoir des responsabilités spécifiques dans le cadre de la sécurité technique.
- (5) Au niveau des employés, tous les utilisateurs ont une certaine responsabilité en matière de sécurité des informations, notamment en ce qui concerne l'utilisation sûre des données et le respect des politiques de sécurité. Les formations et les programmes de sensibilisation sont essentiels pour garantir que tous les employés comprennent leur rôle dans le concept de sécurité.



- (6) Les responsables de la conformité pourraient être chargés de veiller au respect des normes de sécurité et des réglementations externes. Les délégués à la protection des données (DPO) s'occupent de la conformité aux règles de protection des données.
- (7) La collaboration entre les différentes responsabilités est essentielle pour garantir une stratégie de sécurité globale et efficace. Des responsabilités clairement définies favorisent la transparence, facilitent la coordination des mesures de sécurité et permettent d'identifier plus facilement les points faibles ou les mesures à prendre.
- (8) En outre, les responsables des interfaces avec les parties prenantes externes telles que les fabricants / fournisseurs, les services fédéraux comme l'OFCS, le SOC, les CERT, les partenaires, etc. doivent être désignés.
- (9) Globalement, la définition des responsabilités est un processus dynamique qui s'adapte à l'évolution des exigences et des menaces. Il nécessite une communication et une collaboration continues afin de garantir que toutes les parties prenantes comprennent leur rôle dans la sécurité de l'information et y contribuent activement.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-02-01: Directive Domaine de la sécurité de l'information: cadre de la sécurité de l'information
- HoP-01-01-02: Directive Domaine de la sécurité de l'information: champ d'application, mise en place et fonctionnement de l'ISMS



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est important de définir les responsabilités dans le cadre de la sécurité de l'information et du ISMS afin d'établir des responsabilités claires, de mettre en œuvre efficacement les mesures de sécurité, de minimiser les risques et de garantir l'intégrité de la sécurité de l'information.

6.2.8 Définir des indicateurs de performance (KPI)

- (1) La définition d'indicateurs de performance (KPI) dans le cadre de la sécurité de l'information et du ISMS est essentielle pour la mesure et l'amélioration continue des mesures de sécurité. Les KPI sont des mesures quantitatives qui rendent compte de la performance dans des domaines clés de la sécurité de l'information.
- (2) Le choix des KPI est basé sur les objectifs stratégiques de l'ISMS et les exigences de sécurité spécifiques de l'organisation. Des exemples d'indicateurs clés de performance pourraient être le nombre d'incidents de sécurité par mois, le temps moyen de correction des vulnérabilités, le taux de réussite des formations à la sécurité ou la vérification régulière des journaux d'accès.
- (3) La définition des KPI nécessite un lien clair avec les objectifs de sécurité, par exemple la réduction des incidents de sécurité. Les KPI doivent être spécifiques, mesurables, atteignables, réalistes et temporellement définis (SMART). Il est important de revoir et d'adapter régulièrement les KPI afin de tenir compte du contexte actuel de la sécurité et de l'évolution des besoins de l'entreprise.
- (4) La définition des KPI va souvent de pair avec l'identification d'une base de référence pour la mesure des performances. Une communication claire des KPI aux parties prenantes favorise une compréhension commune et contribue à la réalisation des objectifs de sécurité de l'organisation. Globalement, des KPI bien définis dans l'ISMS fournissent une base objective pour l'évaluation des performances de sécurité et permettent une amélioration ciblée en accord avec les objectifs stratégiques de l'entreprise.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-02-01: Directive Domaine de la sécurité de l'information: cadre de la sécurité de l'information
- HoP-01-01-02: Directive Domaine de la sécurité de l'information: Champ d'application, mise en place et fonctionnement de l'ISMS



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est important de définir des indicateurs de performance (KPI) pour la sécurité de l'information et l'ISMS afin de mesurer l'efficacité des mesures de sécurité, d'identifier les points faibles et de permettre une amélioration continue.

6.2.9 Définir une procédure pour les audits

- (1) La procédure d'audit dans le cadre de la sécurité de l'information et du système de gestion de la sécurité de l'information (ISMS) est un processus structuré qui permet de vérifier le respect des politiques,



procédures et normes de sécurité. Les audits sont essentiels à l'efficacité du ISMS et à l'amélioration continue de la sécurité de l'information.

- (2) Le processus d'audit commence par la définition du champ d'application de l'audit et des objectifs de l'audit, en accord avec les objectifs de sécurité du ISMS et les objectifs de l'entreprise. La réalisation de l'audit comprend la vérification systématique des documentations de sécurité, des processus et des implémentations techniques, y compris l'implication des rôles et fonctions responsables.
- (3) L'analyse des résultats de l'audit identifie les écarts par rapport aux normes et évalue les aspects positifs. Le rapport d'audit qui en résulte contient des recommandations d'amélioration, les points faibles identifiés et les aspects positifs. Ce rapport est transmis aux parties prenantes concernées et à la direction.
- (4) La mise en œuvre de mesures correctives est une étape décisive pour remédier aux points faibles identifiés et renforcer la sécurité de l'information. Ce processus transparent comprend le retour des résultats de l'audit aux secteurs concernés. Globalement, la procédure structurée des audits dans l'ISMS permet une évaluation objective de la sécurité de l'information et contribue à l'amélioration continue, afin de garantir que les mesures de sécurité correspondent aux normes définies et sont axées sur les menaces actuelles.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-02-01: Directive Domaine de la sécurité de l'information: cadre de la sécurité de l'information
- HoP-01-01-02: Directive Domaine de la sécurité de l'information: champ d'application, mise en place et fonctionnement de l'ISMS

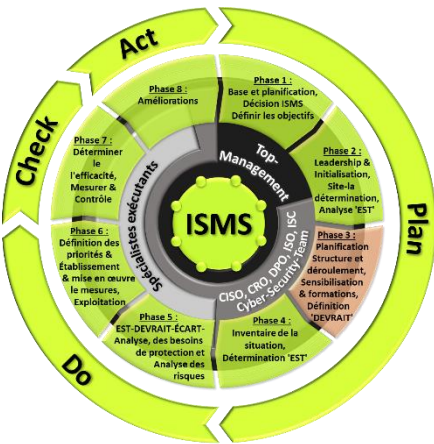


Recommandation des experts de la Task Force Cyber Security de l'AES:

L'élaboration d'un plan d'audit aide les responsables à planifier les audits de manière adéquate sur l'année et à allouer les ressources nécessaires. De même, il donne une vue d'ensemble des domaines de sécurité qui doivent être audités.

6.3 Phase 3: planification de la mise en place et du déroulement; sensibilisation et formation; définition de l'«état souhaité»

- (1) La troisième phase de la mise en place d'un ISMS est axée sur la planification, la mise en place et le déroulement du ISMS, ainsi que sur la sensibilisation et la formation et la définition des objectifs (état souhaité):



Responsabilité:	Top management, niveau C
Compétence:	CISO, CRO, DPO, ISO, ISC, équipe de cybersécurité
Organismes impliqués:	Personnel spécifique de la sécurité de l'information, experts et consultants externes
Points à traiter:	<ul style="list-style-type: none">■ Mettre en œuvre, établir, adapter et étendre un ISMS■ Introduire / adapter la maîtrise des documents■ Créer, compléter et adapter les documents axés sur la base de référence du ISMS (directives, lignes directrices, instructions de travail, etc.■ Établir / habilitier / adapter l'organisation de la sécurité■ Impliquer les employés dans le domaine de la sécurité de l'information■ Introduire / élargir / adapter la sensibilisation et la formation■ Définir l'«état souhaité» pour la sécurité de l'information■ Etablir un catalogue de mesures■ Planifier les audits

Tableau 9: Phase 3 ISMS: planification de la mise en place et du déroulement; sensibilisation et formation; définition de l'«état souhaité».



6.3.1 Mettre en place, adapter et étendre un ISMS

- (1) La mise en œuvre, l'établissement, l'adaptation et l'extension d'un système de gestion de la sécurité de l'information (ISMS) est un processus continu qui vise à assurer et à améliorer en permanence la sécurité de l'information d'une organisation.
 - **Mise en œuvre de l'ISMS:** commence par la définition d'un cadre clair, y compris le contexte, les objectifs commerciaux et le champ d'application. Des responsabilités claires et une évaluation des risques conduisent à la définition d'objectifs de sécurité concrets qui servent de base aux politiques, procédures et processus.
 - **Mise en place de l'ISMS:** Nécessite un engagement fort de la part de la direction générale, une participation active et la mise à disposition de ressources. Un mécanisme d'amélioration continue est mis en place, accompagné de formations et de mesures de sensibilisation pour les collaborateurs. Des audits internes vérifient l'efficacité du ISMS.
 - **Adaptation de l'ISMS:** un processus dynamique par lequel l'organisation réagit aux changements de l'environnement, de la technologie et des menaces. La direction générale joue un rôle central pour garantir que l'ISMS répond aux exigences actuelles. Des formations et des audits continus permettent de vérifier et d'adapter régulièrement le système.
 - **Extension de l'ISMS:** implique l'intégration avec d'autres systèmes de gestion afin d'assurer une approche globale. L'organisation s'assure que l'ISMS répond aux exigences de conformité. Les nouvelles technologies et l'évolution des menaces sont prises en compte afin d'étendre et d'améliorer en permanence l'ISMS.
- (2) Globalement, ce processus exige une attitude proactive, une surveillance et une adaptation continues. Un engagement continu permet à l'organisation de s'assurer que son ISMS reste robuste et efficace et qu'il répond aux exigences en constante évolution en matière de sécurité de l'information.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-02-01: Directive Domaine de la sécurité de l'information: cadre de la sécurité de l'information
- HoP-01-01-02: Directive Domaine de la sécurité de l'information: champ d'application, mise en place et fonctionnement de l'ISMS



Les documents suivants contiennent des orientations et des instructions:

- Norme BSI 200-1 Systèmes de gestion de la sécurité de l'information (ISMS)



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'introduction, l'adaptation et l'extension d'un ISMS est un processus qui doit être adapté et amélioré en permanence. Il est important que les directives et documents nécessaires soient toujours à jour et disponibles à tout moment pour tous les employés concernés.

6.3.2 Introduire / adapter la maîtrise des documents

- (1) L'introduction de la gouvernance documentaire dans l'ISMS garantit des documents de sécurité systématiquement créés, approuvés, contrôlés et mis à jour. Cette étape implique l'identification des documents pertinents et la définition de procédures et de responsabilités claires pour leur création. Les contrôles de version garantissent l'utilisation de documents à jour, tandis que les procédures d'approbation permettent de s'assurer qu'ils sont revus avant leur entrée en vigueur.
- (2) Une surveillance et une mise à jour régulières, notamment en cas de modification des exigences de sécurité ou de la législation, garantissent l'actualité des documents. L'efficacité du système de contrôle des documents favorise la transparence, l'accessibilité et facilite le respect des normes du ISMS.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01-04: Instructions de travail domaine de la sécurité de l'information: maîtrise des documents



Recommandation des experts de la Task Force Cyber Security de l'AES:

La mise en place d'une gouvernance documentaire et ses adaptations continues sont importantes pour garantir la cohérence et l'actualité des politiques et de la documentation de sécurité, ce qui augmente l'efficacité du système de gestion de la sécurité de l'information et favorise le respect des normes. La maîtrise des documents est créée et gérée dans le domaine des systèmes de



gestion intégrés (SGI). La gouvernance des documents est créée et gérée dans le domaine des systèmes de gestion intégrés (IMS). Ainsi, une concertation avec les autres secteurs de l'entreprise est impérative.

6.3.3 Élaborer, compléter et adapter les documents de référence axés sur la base de référence du ISMS (directives, lignes directrices, instructions de travail, etc.

- (1) La création de documents axés sur la base de référence du système de gestion de la sécurité de l'information dans le cadre de la sécurité de l'information est un processus crucial pour établir des politiques, des lignes directrices et des instructions de travail claires et contraignantes. Ces documents servent de base aux pratiques de sécurité au sein de l'organisation et contribuent à établir un environnement de sécurité cohérent.
- (2) Le processus commence par une analyse complète des besoins et des objectifs de l'organisation en matière de sécurité. Les menaces, les risques et les exigences commerciales spécifiques sont pris en compte. Sur la base de cette analyse, les documents nécessaires sont identifiés, tels que les politiques de sécurité, les guides et les instructions de travail.
- (3) L'élaboration de directives de sécurité nécessite une formulation claire des principes et des règles de comportement en matière de sécurité de l'information. Ces directives doivent refléter les objectifs stratégiques du ISMS et être compréhensibles par tous afin d'être appliquées par l'ensemble du personnel.
- (4) Les guides fournissent des instructions et des recommandations détaillées sur des aspects spécifiques de la sécurité. Il peut s'agir par exemple de la configuration sécurisée des systèmes, de la gestion des droits d'accès ou de l'utilisation sécurisée des ressources informatiques. Les guidelines complètent les directives en fournissant des instructions d'action concrètes.
- (5) Les guides de travail fournissent des étapes et des procédures détaillées pour des tâches spécifiques liées à la sécurité de l'information. Il peut s'agir d'effectuer des contrôles de sécurité, de signaler des incidents de sécurité ou de mettre en œuvre des mesures de sécurité.
- (6) L'élaboration de ces documents nécessite une étroite collaboration entre les responsables de la sécurité de l'information, les experts techniques et les parties prenantes concernées. Il est important de s'assurer que les documents sont précis, cohérents et compréhensibles pour le public cible.
- (7) La version et la mise à jour de ces documents sont nécessaires pour s'assurer qu'ils correspondent aux menaces et aux développements technologiques actuels. Des révisions et des mises à jour régulières devraient être intégrées dans le processus de création des documents.
- (8) La création de documents axés sur la base de référence du ISMS joue un rôle central dans la définition des normes et des meilleures pratiques en matière de sécurité de l'information. Des documents bien structurés et compréhensibles contribuent largement à la mise en œuvre efficace des politiques et procédures de sécurité.



A l'aide de l'outil «VSE-NIST-CSF-1.1_HoP-Mapping-Tool», les différents points du CSF NIST 1.1 peuvent être attribués aux documents correspondants. Cela permet de s'assurer que tous les points sont traités.



Dans l'outil «VSE-ISO27002-Annex-A_HoP-Mapping-Tool», les différents éléments de l'ISO 27001 Annex A peuvent être attribués aux documents de la Maison des politiques en amont de la création des documents. Cela permet de s'assurer que tous les points sont traités.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



Les annexes contiennent des exemples types qui peuvent être appliqués:

- HoP-01-00-00 Directive Systèmes de gestion intégrés (SGI)
- HoP-01-00-00-01 Instructions de travail domaine SGI: Maison des processus
- HoP-01-00-00-02 Instructions de travail domaine SGI: Maison des politiques
- HoP-01-00-00-03 Instructions de travail domaine SGI: maîtrise des documents
- HoP-01-00-01-04 Instructions de travail domaine SGI: audits
- HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information SGI
- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information



- HoP-01-01-01-01 Instructions de travail Domaine SGI: Sécurité de l'information Organisation
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS
- HoP-01-01-03-01 Instructions de travail domaine ISMS: protection de base de la sécurité de l'information (sécurité des données)
- HoP-01-01-03-02 Instructions de travail domaine ISMS: gestion des risques IT/OT
- HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations
- HoP-01-01-03-04 Instructions de travail domaine ISMS: formation et sensibilisation
- HoP-01-01-03-05 Instructions de travail domaine ISMS: sécurité physique des actifs TIC
- HoP-01-01-03-06 Instructions de travail domaine ISMS: contrôle d'accès
- HoP-01-01-03-07 Instructions de travail domaine ISMS: authentification multi-facteurs
- HoP-01-01-03-08 Instructions de travail domaine ISMS: gestion des droits d'accès privilégiés
- HoP-01-01-03-09 Instructions de travail domaine ISMS: systèmes (serveur et client)
- HoP-01-01-03-10 Instructions de travail domaine ISMS: composants contrôle-commande
- HoP-01-01-03-11 Instructions de travail domaine ISMS: systèmes d'exploitation et applications
- HoP-01-01-03-12 Instructions de travail domaine ISMS: cryptage
- HoP-01-01-03-13 Instructions de travail domaine ISMS: réseaux
- HoP-01-01-03-14 Instructions de travail domaine ISMS: sauvegarde et liste de contrôle pour la sauvegarde
- HoP-01-01-03-15 Instructions de travail domaine ISMS: nettoyage des médias
- HoP-01-01-03-16 Instructions de travail domaine ISMS: gestion LOG
- HoP-01-01-03-17 Instructions de travail domaine ISMS: gestion des logiciels malveillants et des vulnérabilités
- HoP-01-01-03-18 Instructions de travail domaine ISMS: gestion des incidents liés à la sécurité de l'information (Incident Management)
- HoP-01-01-03-19 Instructions de travail domaine ISMS: gestion de la continuité des opérations (BCM)
- HoP-01-01-03-20 Instructions de travail domaine ISMS: gestion des situations d'urgence
- HoP-01-01-03-21 Instructions de travail domaine ISMS: mesures de sécurité pour les prestataires de services
- HoP-01-01-03-22 Instructions de travail domaine ISMS: gestion des fournisseurs
- HoP-01-01-03-23 Instructions de travail domaine ISMS: sécurité de l'information dans le domaine des ressources humaines
- HoP-01-01-03-24 Instructions de travail domaine ISMS: sécurité de l'information dans les projets
- HoP-01-01-03-25 Instructions de travail domaine ISMS: utilisation de services en cloud
- HoP-01-01-03-26 Instructions de travail domaine ISMS: utilisation de l'apprentissage automatique et de l'intelligence artificielle
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information
- HoP-01-01-04-01 Instructions de travail domaine GSI: utilisation d'appareils mobiles
- HoP-01-01-04-02 Instructions de travail domaine GSI: utilisation des actifs OT



L'élaboration des documents de référence pour la ligne de base nécessite beaucoup de ressources. Des ressources suffisantes doivent être mises à disposition. Il est important que tous les points soient traités dans leur intégralité et que les documents soient compréhensibles pour le public cible.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Une approche systématique est proposée pour l'élaboration des documents de la ligne de base dans l'ISMS. Il s'agit tout d'abord de rassembler tous les points nécessaires pour chaque consigne et chaque document et de les insérer dans les documents de base. Ensuite, les consignes et les documents peuvent être structurés et mis sous leur forme définitive. Il est important que les documents soient continuellement adaptés afin de pouvoir réagir aux menaces les plus actuelles et de prioriser les mesures.

6.3.4 Établir / habiliter / adapter l'organisation de la sécurité

- (1) L'établissement et l'habilitation de l'organisation de la sécurité dans le cadre de la sécurité de l'information et du système de gestion de la sécurité de l'information (ISMS) est un processus global qui vise à créer une structure robuste et à fournir les ressources nécessaires pour assurer efficacement la sécurité de l'information.



- (2) Tout commence par la définition de l'organisation de la sécurité, y compris la désignation des postes clés et des responsabilités. Cela pourrait inclure le rôle du responsable en chef de la sécurité de l'information (CISO) ou d'un responsable de la sécurité, d'un responsable de la protection des données, d'un expert en sécurité informatique et d'autres fonctions. Les responsabilités devraient être clairement définies et se rapporter aux objectifs stratégiques du ISMS.
- (3) L'établissement de l'organisation de la sécurité nécessite également l'intégration des aspects de la sécurité dans la structure organisationnelle. Cela signifie que la fonction de sécurité n'est pas isolée, mais intégrée dans les différents départements et niveaux de l'organisation. Cela favorise une culture de sécurité globale.
- (4) L'habilitation de l'organisation de la sécurité implique la mise à disposition de formations et de ressources afin de garantir que les professionnels de la sécurité et le personnel de l'organisation possèdent les compétences et les connaissances nécessaires. La formation pourrait couvrir des sujets tels que la programmation sécurisée, la protection des données, la gestion des risques et d'autres aspects pertinents de la sécurité.
- (5) L'organisation de la sécurité devrait disposer des pouvoirs nécessaires pour prendre des décisions en matière de sécurité et faire appliquer des mesures. Cela pourrait inclure la mise en place de politiques de sécurité, le contrôle du respect des normes de sécurité et la réalisation d'audits de sécurité.
- (6) Il est important de s'assurer que l'organisation de la sécurité coopère efficacement avec d'autres fonctions pertinentes de l'organisation. Il s'agit notamment des unités organisationnelles IT/OT, du service juridique, de la gestion des risques et d'autres domaines pertinents. La communication et la collaboration entre ces fonctions sont essentielles pour développer et mettre en œuvre une stratégie de sécurité globale.
- (7) L'organisation de la sécurité doit également être en mesure de réagir à l'évolution des menaces et des technologies. Cela nécessite une révision et une adaptation régulières de la stratégie de sécurité ainsi que l'intégration des meilleures pratiques et des innovations dans les pratiques de sécurité.
- (8) Globalement, l'établissement et l'habilitation de l'organisation de la sécurité est un processus continu qui vise à créer une forte culture de la sécurité. Une organisation de la sécurité bien établie et habilitée est essentielle à la réussite du ISMS et à la gestion efficace des risques liés à la sécurité de l'information.



La mise en place, l'habilitation et l'adaptation de l'organisation de la sécurité sont les premières étapes d'une initialisation réussie de l'impact du ISMS.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Une organisation de la sécurité adaptée aux besoins de l'entreprise et des unités organisationnelles doit être mise en place, établie et habilitée. Les fonctions concernées doivent être conscientes de leurs responsabilités et disposer des capacités et compétences adéquates.

6.3.5 Impliquer tous les employés dans l'établissement d'une culture de la sécurité à l'échelle de l'entreprise

- (1) L'intégration des employés dans l'ISMS vise à établir une culture de sécurité globale et à maximiser l'efficacité du ISMS. Une communication claire à tous les niveaux souligne l'importance de la sécurité de l'information pour chaque employé.
- (2) Les formations et les programmes de sensibilisation sensibilisent aux dangers et aux meilleures pratiques, adaptés à l'organisation. L'intégration dans les processus de travail, la participation au processus de développement des politiques et des procédures de sécurité et une communication claire favorisent la participation active et la responsabilisation des employés. Créer et former des mécanismes de retour d'information et des voies de signalement des incidents de sécurité, et établir une culture de communication ouverte. L'implication des employés dans la conception des processus et des mesures de sécurité favorise une culture de sécurité participative.
- (3) L'implication continue contribue à créer un large soutien en faveur de la sécurité de l'information, à renforcer l'efficacité du ISMS et à sensibiliser l'ensemble de l'organisation à la sécurité.



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'implication de tous les employés dans le domaine de la sécurité de l'information doit se faire en temps réel et de manière récurrente. Les employés sont la base de la culture de sécurité de chaque entreprise, qui est renforcée par leur implication.



6.3.6 Introduire / élargir / adapter la sensibilisation et la formation

- (1) La planification, l'introduction, l'extension et l'adaptation d'un programme de sensibilisation et de formation à la sécurité de l'information et au système de gestion de la sécurité de l'information (ISMS) sont des étapes critiques pour garantir que les employés possèdent les connaissances nécessaires pour assurer la sécurité de l'information de l'organisation.
 - **Planification du programme de sensibilisation et de formation:** la planification commence par une analyse complète des besoins en matière de formation. Cela implique d'identifier les employés qui travaillent dans des fonctions liées à la sécurité et de déterminer les domaines clés dans lesquels la sensibilisation doit être renforcée. Le plan comprend également la sélection de méthodes de formation appropriées, y compris des cours, du matériel de formation, des ateliers et éventuellement des simulations. Il est également essentiel de définir des objectifs clairs, tels que l'amélioration de la compréhension des politiques de sécurité et la sensibilisation aux menaces potentielles.
 - **Introduction du programme de sensibilisation et de formation:** l'introduction se fait par une communication claire aux employés. Le top management joue un rôle clé en soulignant l'importance de la sécurité de l'information et en insistant sur la nécessité de participer à la formation. La mise en œuvre implique la mise à disposition de ressources, de matériel de formation et la planification des dates de formation. Il est important que les formations soient adaptées aux besoins du groupe cible et qu'elles contiennent des éléments interactifs afin de favoriser l'engagement. La mesure du succès se fait par l'évaluation de la sensibilisation à la sécurité avant et après les formations.
 - **Extension du programme de sensibilisation et de formation:** L'extension du programme implique l'intégration de nouveaux contenus de formation en réponse à l'évolution des menaces et des technologies. Il peut s'agir d'introduire des formations sur des politiques de sécurité spécifiques, des règles de protection des données ou de nouvelles technologies. L'organisation s'efforce de sensibiliser en permanence les employés en réagissant aux évolutions actuelles dans le domaine de la sécurité de l'information. De nouvelles méthodes ou plates-formes de formation peuvent également être intégrées afin d'accroître l'efficacité du programme.
 - **Améliorer et adapter le programme de sensibilisation et de formation:** l'amélioration et l'adaptation se font en réponse aux retours d'information, aux vérifications et à l'évolution des exigences. Des évaluations régulières du programme de formation sont effectuées afin de déterminer si les objectifs ont été atteints et si des ajustements sont nécessaires. L'avis des employés est activement recueilli afin d'évaluer la pertinence et l'efficacité des formations. Le programme est maintenu flexible afin de prendre en compte les changements dans la structure de l'entreprise, les nouvelles technologies ou l'évolution des menaces.
- (2) Dans l'ensemble, un programme de sensibilisation et de formation réussi nécessite une planification réfléchie, une communication claire, une adaptation et une extension continues afin de rester en phase avec les exigences en constante évolution en matière de sécurité de l'information.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-03-04 Instructions de travail domaine ISMS: formation et sensibilisation



Les documents suivants contiennent des orientations et des instructions:

- Programme de formation selon la publication spéciale NIST 800-50



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est recommandé d'élaborer et de mettre en œuvre un programme de formation conformément à la publication spéciale 800-50 du NIST.

6.3.7 Définir l'«état souhaité» de la sécurité de l'information (définition de l'«objectif»)

- (1) La définition de l'état «cible» pour la sécurité de l'information dans le cadre du système de gestion de la sécurité de l'information (ISMS) est une étape cruciale pour établir des objectifs et des normes clairs pour la sécurité de l'information dans une organisation. L'état «souhaité» représente la vision souhaitée de la sécurité de l'information, qui correspond aux exigences commerciales, aux exigences légales et aux tolérances aux risques de l'organisation.



- (2) Cette phase consiste à identifier des objectifs et des exigences de sécurité complets, basés sur les objectifs stratégiques de l'organisation. Il pourrait s'agir de garantir la confidentialité, l'intégrité et la disponibilité des informations, de respecter les exigences légales, de réduire les risques et de promouvoir une culture de la sécurité.
- (3) La définition de l'«état souhaité» nécessite une analyse approfondie des processus commerciaux, des flux d'informations et des technologies sous-jacentes. Les menaces et les vulnérabilités potentielles sont prises en compte afin de s'assurer que les objectifs de sécurité sont précis et complets.
- (4) L'intégration des meilleures pratiques et des normes sectorielles, comme ISO 27001, peut aider à définir un «état souhaité» robuste. Ces normes fournissent des cadres pour la sécurité de l'information qui sont acceptés par de nombreuses entreprises et unités organisationnelles dans le monde entier.
- (5) L'«état souhaité» devrait également inclure des directives claires en matière de politiques, de procédures et de contrôles de sécurité. Cela comprend des aspects techniques tels que la sécurité du réseau, les contrôles d'accès, le cryptage, mais aussi des aspects organisationnels tels que la formation, la sensibilisation et les plans de réponse aux incidents.
- (6) Il est important que l'«état souhaité» ne soit pas statique, mais qu'il s'adapte à l'évolution des besoins commerciaux, des technologies et des menaces. Il convient donc de procéder à des révisions et à des mises à jour régulières de la situation «cible» afin de s'assurer qu'elle reste actuelle, réaliste et efficace.
- (7) La définition de l'«état souhaité» constitue la base de l'ensemble de la mise en œuvre et de l'exploitation du ISMS. Elle sert de guide pour toutes les activités de sécurité et permet de cibler les ressources afin d'atteindre les objectifs de sécurité visés. L'état «souhaité» fait office de point d'orientation pour l'ensemble de la stratégie de sécurité de l'information et aide l'organisation à mettre en place un environnement de sécurité résistant et efficace.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information



Les directives de l'OFEN dans l'ordonnance sur l'électricité définissent déjà les objectifs à atteindre selon le CSF NIST 1.1. Les obligatoires doivent être reprises comme objectif minimal par les entreprises et les unités organisationnelles concernées dans les domaines correspondants de la sécurité de l'information.



Pour la définition de l'état souhaité dans le domaine de la sécurité de l'information des contrôles dans le cadre du CSF NIST 1.1, il est possible d'utiliser l'outil «VSE&BFE-Assement-Tool_NIST-CSF-1.1_++». Les directives de l'OFEN dans l'ordonnance sur l'électricité sont déjà visibles dans l'outil.



L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.



Pour la définition de l'état souhaité dans la sécurité de l'information des contrôles dans le cadre de la norme ISO 27001 Annexe A, il convient d'utiliser l'outil «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



En annexe se trouve une description détaillée pour «VSE&BFE-Assement-Tool_NIST-CSF-1.1_++» et «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».



Recommandation des experts de la Task Force Cyber Security de l'AES:

Les outils mis à disposition par l'AES doivent être utilisés pour la réalisation des définitions de l'état souhaité. La «définition de l'état souhaité» doit être choisie de manière à ce que les objectifs puissent être atteints!!!



6.3.8 Etablir un catalogue de mesures, définir les mesures à appliquer

- (1) Le choix ou la définition des mesures à appliquer dans un catalogue de mesures est un processus complexe et de grande envergure, décisif pour la suite des opérations. Tout d'abord, les entreprises et les unités organisationnelles doivent déterminer dans quel domaine quelles mesures doivent être sélectionnées et à partir de quels cadres ou normes. Les entreprises et les unités organisationnelles doivent se fixer sur une famille de mesures, éventuellement sur un mélange entre les sources existantes comme par exemple la publication NIST 800-53, les CIS Critical Security Controls, la CSA Cloud Controls Matrix et la norme ISO 27002. De nombreuses mesures figurant dans les sources énumérées sont identiques, c'est pourquoi il faut décider avec précision sur quelle source se focaliser. Dans le cadre de l'état minimal des TIC, on se concentre sur la publication NIST 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix, car elles sont complètes et couvrent toutes les exigences pour l'augmentation de la résilience des TIC. La définition de l'applicabilité et de la SoA a déjà permis de déterminer les domaines nécessaires dans une première étape. Ainsi, le catalogue de mesures ne doit être établi que pour les domaines définis.
- (2) Les mesures de la norme ISO 27002 ne couvrent que globalement les exigences nécessaires et ne sont pas exhaustives. C'est pourquoi l'application des mesures de la norme ISO 27002 n'est recommandée qu'à titre de complément.
- (3) L'Office fédéral allemand de la sécurité dans la technologie de l'information (BSI) poursuit une autre approche avec le recueil de protection de base. Des éléments de processus et de système sont représentés pour les domaines de mesures nécessaires. Ceux-ci peuvent ensuite être utilisés pour définir le catalogue de mesures. Le BSI a ainsi créé une approche complète et holistique pour l'élaboration du catalogue de mesures. Toutefois, les mesures correspondent également aux sources mentionnées ci-dessus.
- (4) Pour des domaines spécifiques, il faut également faire appel à des normes qui, si nécessaire, élargissent le catalogue de mesures. Ces normes sont par exemple CEI/EN 62443, CEI/EN 62351, CEI/EN 60850, CEI/EN 61850, IEEE, etc.
- (5) L'élaboration du catalogue de mesures représente un grand défi pour l'entreprise et les unités organisationnelles. Il s'agit de décider quels contrôles ou mesures de quel standard doivent être appliqués.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est recommandé d'appliquer les mesures selon la publication NIST 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix. Le catalogue de mesures doit être établi à partir de ces trois sources. L'outil mis à disposition par l'AES doit être utilisé comme base. Les mesures peuvent être complétées par les points de la norme ISO 27002. Les outils CSF peuvent être utilisés à titre de soutien sur <https://csf.tools/>.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information



L'élaboration du plan de mesures avec les contrôles de la publication NIST 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix ne constitue que la base. Pour des domaines spécifiques, le catalogue de mesures doit être complété par des contrôles issus de normes telles que IEC/EN 62443, IEC/EN 62351, IEC/EN 60850, IEC/EN 61850, IEEE, etc.



L'élaboration du catalogue de mesures est un processus de grande envergure qui nécessite beaucoup de ressources. Mais ce processus doit impérativement être mis en œuvre par les entreprises et les unités organisationnelles, car il est décisif pour la globalité et l'efficacité.



L'outil «VSE&BFE-Tool_for_NIST-CSF-1.1_Checkpoints_acc.to_NIST-SP800-53_CCM_CIS» permet d'établir le plan de mesures.



Les outils NIST CSF disponibles sur <https://csf.tools/> aident les entreprises et les unités organisationnelles à trouver et à définir les mesures nécessaires. Dans les outils, l'ensemble du cadre de cybersécurité NIST est mis en réseau avec les mesures de la publication NIST 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix.



Les documents suivants contiennent des orientations et des instructions:

- Compendium BSI IT-Grundschutz



6.3.9 Planifier les audits

- (1) La planification des audits dans le cadre d'un système de gestion de la sécurité de l'information (ISMS) est une étape cruciale pour s'assurer que les processus et les contrôles de sécurité sont efficaces. La planification vise à vérifier systématiquement la conformité avec les normes de sécurité établies et à identifier les domaines d'amélioration potentiels.
- (2) La première étape consiste à déterminer le champ d'application de l'audit, qui définit les domaines et les processus qui doivent être contrôlés pendant l'audit. Cela comprend souvent une analyse des processus commerciaux critiques et des informations qui y sont liées. Parallèlement, on définit les objectifs de l'audit, qui visent généralement à vérifier le respect des politiques et des procédures de sécurité, à identifier les points faibles et à s'assurer que les objectifs de sécurité sont atteints.
- (3) Le choix des auditeurs est un autre aspect essentiel de la planification. Les auditeurs doivent posséder les compétences nécessaires en matière de sécurité de l'information, tout en étant indépendants et objectifs.
- (4) La planification tient également compte du calendrier de l'audit et garantit que suffisamment de temps est disponible pour un examen approfondi de tous les aspects pertinents. Un plan d'audit est établi, qui esquisse le déroulement détaillé de l'audit. Cela comprend le calendrier, les domaines à auditer, les personnes impliquées et les ressources à utiliser.
- (5) La communication avec les parties concernées, y compris celles qui sont auditées, est essentielle pour favoriser la transparence et la coopération. Au cours de l'audit, différentes méthodes de collecte et de vérification des données sont utilisées, notamment des entretiens, des examens de documents et éventuellement des tests techniques.
- (6) Les résultats sont documentés afin de donner un aperçu clair du respect des normes de sécurité et des possibilités d'amélioration identifiées. Une fois l'audit terminé, un rapport est établi, dans lequel sont consignés les résultats, les constatations et les recommandations. Ces rapports sont fondamentaux pour l'amélioration continue du ISMS. L'organisation prend alors des mesures pour remédier aux éventuelles lacunes et continuer à optimiser l'état de la sécurité.
- (7) Globalement, la planification des audits dans le cadre d'un ISMS est un processus stratégique qui permet de s'assurer que l'examen de la sécurité de l'information est effectué de manière systématique, objective et efficace.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-00-01-04 Instructions de travail domaine SGI: audits



Recommandation des experts de la Task Force Cyber Security de l'AES: La planification des audits est établie et gérée dans le domaine des systèmes de gestion intégrés (SGI). Il est donc impératif de se concerter avec les autres secteurs de l'entreprise et les unités organisationnelles.



6.4 Phase 4: état des lieux; détermination de l'«état réel».

- (1) La quatrième phase est placée sous le signe de l'état des lieux et de la détermination de la situation «actuelle»:



Tableau 10: Phase 4 ISMS: état des lieux; détermination de l'«état réel».

6.4.1 Faire un inventaire détaillé

- (1) La collecte d'un inventaire détaillé des actifs dans le cadre de la sécurité de l'information et du système de gestion de la sécurité de l'information (ISMS) est une étape essentielle pour obtenir une vue d'ensemble des ressources d'information utilisées par une organisation. Ce processus vise à identifier, classer et documenter tous les actifs afin de garantir efficacement leur sécurité.
- (2) La mise en œuvre commence par l'identification de tous les actifs et ressources d'information au sein de l'organisation. Cela inclut non seulement les équipements physiques tels que les serveurs et les ordinateurs, mais aussi les bases de données, les logiciels, les équipements de réseau, les flux d'informations et d'autres éléments pertinents. Une analyse minutieuse est essentielle pour s'assurer qu'aucun actif important n'est négligé.
- (3) L'étape suivante consiste à classer les actifs identifiés. Cela implique d'évaluer leur sensibilité, leur importance et leur impact sur les processus d'entreprise. La classification permet de définir des priorités et d'allouer des ressources en fonction de l'importance des actifs.
- (4) La documentation des actifs est un élément essentiel de ce processus. Il s'agit de recueillir des informations détaillées sur chaque actif, y compris son emplacement, son propriétaire, les droits d'utilisation, les spécifications techniques et les dépendances par rapport aux autres actifs. Une documentation minutieuse facilite la gestion et la protection ultérieures des actifs.
- (5) Parallèlement, les risques liés à chaque actif sont évalués. Cela comprend l'identification des menaces potentielles, des vulnérabilités et des effets possibles sur la sécurité de l'actif. L'évaluation des risques est essentielle pour développer des mesures de sécurité ciblées et s'assurer que les ressources disponibles sont utilisées efficacement.
- (6) La réalisation de l'inventaire détaillé des actifs nécessite souvent la collaboration de différentes unités organisationnelles et parties prenantes au sein de l'entreprise et des unités organisationnelles. Les départements IT/OT, les responsables de la protection des données et les unités commerciales doivent apporter leurs perspectives respectives afin de garantir que tous les actifs pertinents sont répertoriés.
- (7) L'ensemble du processus n'est pas unique, mais doit être répété régulièrement. Les nouveaux actifs, les changements dans l'infrastructure TIC ou les processus d'entreprise nécessitent une mise à jour continue de l'inventaire afin de s'assurer que la sécurité de l'information est à jour.
- (8) Globalement, la réalisation d'un inventaire détaillé des actifs permet de disposer d'une base solide pour le développement et la mise en œuvre d'une stratégie efficace de sécurité de l'information. En connaissant précisément toutes les ressources utilisées, l'organisation peut s'assurer que ses actifs informationnels sont protégés de manière adéquate.
- (9) Un inventaire détaillé de la sécurité de l'information comprend les éléments suivants:



- domaines d'activité et leurs processus commerciaux
- informations et données (toutes les données pertinentes pour le traitement des processus commerciaux)
- ressources matérielles telles que serveurs, ordinateurs, composants réseau, etc.
- systèmes d'exploitation, bases de données, micrologiciels, logiciels pilotes, programmes d'application, outils logiciels, etc.
- adresses MAC et IP
- services, protocoles et ports
- certificats
- flux de données et chaîne d'impact
- utilisateur (User)



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations



Il ne faut pas sous-estimer le travail nécessaire à l'établissement d'un inventaire complet. L'inventaire complet et actuel est toutefois d'une importance fondamentale pour la sécurité de l'information dans son ensemble. Les vulnérabilités ne peuvent être identifiées que sur la base d'un inventaire complet et actuel.



Recommandation des experts de la Task Force Cyber Security de l'AES: Pour établir l'inventaire complet, il convient d'adopter une approche systématique. Des outils logiciels et des applications aident les entreprises et les unités organisationnelles à automatiser l'inventaire. Il est important que l'inventaire soit à jour à tout moment.

6.4.2 Identification de la chaîne d'impact

- (1) L'identification de la chaîne d'impact dans l'ISMS est une approche proactive qui permet de comprendre les liens entre les événements, les vulnérabilités et les impacts potentiels sur la sécurité de l'information. En commençant par l'enregistrement de différents événements, elle analyse systématiquement leur lien et leur impact sur la confidentialité, l'intégrité et la disponibilité des informations ainsi que sur la réputation de l'organisation. La chaîne d'impact qui en résulte montre des effets en cascade et permet d'identifier les points faibles et les chemins critiques.
- (2) L'implication des différentes parties prenantes et les mises à jour régulières garantissent une vision globale. Cette approche proactive constitue une base solide pour l'élaboration de stratégies de réduction des risques dans l'ISMS.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations



Recommandation des experts de la Task Force Cyber Security de l'AES: L'identification de la chaîne d'impact est importante pour que les liens entre les différents éléments puissent être mis en évidence. Ainsi, les vecteurs d'attaque possibles peuvent être mieux identifiés et compris. Cela corrobore le fait que les attaques ne sont souvent pas exécutées directement sur les systèmes ou les éléments, mais qu'elles passent par les chaînes d'approvisionnement ou les éléments en réseau.

6.4.3 Déterminer les mesures mises en œuvre pour la sécurité de l'information

- (1) L'identification des mesures mises en œuvre dans l'ISMS est essentielle pour garantir l'efficacité des mesures de sécurité. Le processus commence par l'examen des politiques et des plans de sécurité, y compris les mesures techniques, organisationnelles et personnelles.
- (2) Les aspects techniques sont évalués sur la base des logiciels, des configurations de réseau et des mesures de sécurité physiques. Les mesures organisationnelles, telles que la formation et la sensibilisation, sont examinées quant à leur mise en œuvre dans les processus opérationnels. L'attribution des responsabilités et le suivi des incidents de sécurité sont également des aspects essentiels.



- (3) La collaboration entre les différentes unités organisationnelles et les contrôles réguliers sont essentiels pour maintenir la sécurité de l'information à un niveau approprié et pour réagir de manière adéquate aux menaces actuelles.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations



L'outil «VSE&BFE-Tool_for_NIST-CSF-1.1_Checkpoints_acc.to_NIST-SP800-53_CCM_CIS» permet d'enregistrer les mesures mises en œuvre et leur maturité.



Il ne faut pas sous-estimer l'effort nécessaire pour déterminer les mesures mises en œuvre. La détermination doit être faite de manière complète et globale sur l'ensemble du domaine de la sécurité de l'information.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Une approche structurée aide à déterminer les mesures mises en œuvre. L'utilisation d'outils appropriés est impérative.

6.4.4 Audit de l'état réel: déterminer l'état réel de la sécurité de l'information

- (1) La réalisation d'audits de l'état réel dans le cadre de la sécurité de l'information et du système de gestion de la sécurité de l'information (ISMS) est une approche proactive qui permet de vérifier la mise en œuvre effective des mesures de sécurité et de s'assurer qu'elles sont conformes aux normes et directives établies. Ces audits sont essentiels pour identifier les points faibles, découvrir les possibilités d'amélioration et s'assurer que la sécurité de l'information est à un niveau approprié.
- (2) Le processus commence souvent par la définition des domaines et des objectifs de l'audit. Cela implique la définition des systèmes, des processus et des mécanismes de contrôle à vérifier, ainsi que la détermination claire des objectifs de l'audit. Il est important que ces objectifs soient en accord avec les politiques et les objectifs de sécurité de l'organisation.
- (3) La réalisation proprement dite de l'audit de l'état réel comprend l'examen de la documentation, des processus et des mises en œuvre techniques. Cela peut inclure l'analyse des politiques de sécurité, des documents de formation, des autorisations d'accès, des configurations de systèmes et d'autres documents pertinents. Parallèlement, une vérification sur place est effectuée afin de s'assurer que les processus documentés sont effectivement mis en œuvre dans la pratique et vécus par les unités organisationnelles.
- (4) La communication et la collaboration avec les responsables et les employés constituent un élément essentiel de l'audit de l'état réel. Les auditeurs interagissent avec les parties prenantes concernées afin de recueillir des informations, d'obtenir une compréhension des processus et de s'assurer que les mesures de sécurité fonctionnent efficacement dans la pratique quotidienne.
- (5) L'analyse des résultats se fait en étroite collaboration avec les objectifs de l'audit. Les écarts éventuels par rapport aux normes établies sont identifiés et évalués. Ceux-ci peuvent être de nature technique, organisationnelle ou procédurale. Parallèlement, les aspects positifs et les mises en œuvre réussies sont mis en évidence.
- (6) L'analyse est suivie de la rédaction d'un rapport contenant les résultats de l'audit. Ce rapport contient des recommandations d'amélioration, les points faibles identifiés et les aspects positifs. Il est transmis aux parties prenantes concernées et à la direction de l'organisation.
- (7) La mise en œuvre de mesures correctives est une étape décisive après un audit de l'état réel. Les points faibles identifiés sont alors corrigés et des mesures sont prises pour renforcer encore la sécurité de l'information. Ce processus doit être transparent et inclure le retour des résultats de l'audit aux secteurs concernés.
- (8) Dans l'ensemble, la réalisation d'audits de l'état réel offre une occasion précieuse d'améliorer continuellement la sécurité de l'information. Les résultats de ces audits ne servent pas seulement à corriger les



faiblesses existantes, mais aussi à affiner la stratégie de sécurité de l'organisation et à l'adapter aux menaces actuelles.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-00-01-04 Instructions de travail domaine SGI: audits
- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations



Il ne faut pas sous-estimer l'effort de détermination nécessaire à la réalisation d'un audit. Un audit nécessite une préparation méticuleuse et un contrôle détaillé. L'évaluation qui s'ensuit détermine la situation actuelle et sert de base aux mesures correctives.



Recommandation des experts de la Task Force Cyber Security de l'AES:

La réalisation d'audits est impérative. C'est le seul moyen de déterminer la situation actuelle et d'introduire les mesures correctives nécessaires.

6.4.5 Réaliser un assessment de l'état «Actuel»

- (1) Dans l'ISMS, l'état actuel est évalué pour la sécurité de l'information dans une organisation. Tout d'abord, les domaines et les objectifs de l'audit sont définis en fonction des politiques et des objectifs de sécurité.
- (2) L'évaluation analyse la documentation, les processus et les implémentations techniques, à la fois par l'examen des documents et sur place. La communication avec les responsables et les employés est essentielle à cet égard. L'analyse des résultats identifie les écarts par rapport aux normes et met en évidence les aspects positifs.
- (3) Un rapport final contenant des recommandations d'amélioration est transmis aux parties prenantes et à la direction. La mise en œuvre de mesures correctives clôt le processus, l'évaluation de l'état actuel offrant ainsi une opportunité d'amélioration continue de la sécurité de l'information.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS



L'outil «VSE&BFE-Assement-Tool_NIST-CSF-1.1_++» doit être utilisé pour l'évaluation de l'état réel dans le domaine de la sécurité de l'information des contrôles dans le cadre du CSF NIST 1.1. Les directives de l'OFEN dans l'OApEI sont déjà visibles dans l'outil.



L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.



L'outil «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002» doit être utilisé pour l'évaluation de l'état réel dans la sécurité de l'information des contrôles dans le cadre de l'ISO 27001 Annexe A.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



En annexe se trouve une description détaillée pour «VSE&BFE-Assement-Tool_NIST-CSF-1.1_++» et «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».



Recommandation des experts de la Task Force Cyber Security de l'AES:

Les outils mis à disposition par l'AES doivent être utilisés pour la réalisation de l'évaluation de la situation actuelle.



6.4.6 Créer un registre des risques

- (1) La création d'un registre des risques dans l'ISMS est essentielle pour recenser et surveiller systématiquement les risques. Le processus commence par l'identification de toutes les menaces potentielles pour la sécurité de l'information, tant internes qu'externes.
- (2) L'évaluation des risques analyse leur impact et leur probabilité d'occurrence. Les risques prioritaires sont inscrits dans le registre des risques, qui contient des informations détaillées, les responsabilités et le statut du traitement des risques.
- (3) Des mises à jour régulières et une communication transparente avec les parties prenantes garantissent l'efficacité du registre et permettent de réagir de manière proactive aux menaces.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-03-02 Instructions de travail domaine ISMS: gestion des risques IT/OT



Recommandation des experts de la Task Force Cyber Security de l'AES:

Pour identifier les risques potentiels, il est possible de recourir aux fonctions de risque au sein de l'entreprise et des unités organisationnelles. De même, les BIA se prêtent parfaitement à l'identification des risques effectifs.

6.4.7 Déterminer un scénario de référence (baseline) pour les KPI

- (1) La détermination d'un scénario de référence pour les indicateurs clés de performance (KPI) dans l'ISMS est un processus stratégique visant à établir des points de départ pour la mesure de la performance de la sécurité de l'information. Elle commence par l'analyse des objectifs de l'ISMS, qui servent de base à la sélection des KPI pertinents. Les KPI identifiés doivent être directement liés aux objectifs de sécurité et couvrir des domaines critiques.
- (2) Le scénario de référence est formé par la collecte de données de départ représentant les niveaux de performance actuels pour les indicateurs clés de performance sélectionnés. Pendant la détermination, il est important de tenir compte des fluctuations et des influences saisonnières. Le scénario de référence doit être revu et actualisé régulièrement afin d'évaluer précisément les progrès réalisés dans le contexte de l'évolution des besoins de l'entreprise.
- (3) Un scénario de référence pertinent est essentiel pour surveiller les progrès et réagir de manière ciblée aux points faibles ou aux possibilités d'amélioration de la sécurité de l'information.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports



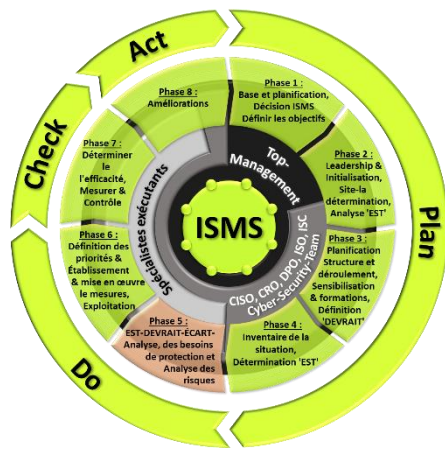
Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est important de définir un scénario de référence pour les indicateurs de performance clés (KPI), car il sert de point de départ pour mesurer les progrès et les performances. Sans, il est difficile d'évaluer le succès ou l'échec d'initiatives ou de mesures. Le scénario de référence permet de suivre les changements au fil du temps et de comprendre si les objectifs sont atteints. Il constitue également la base de la définition d'objectifs réalistes et de l'élaboration de stratégies d'amélioration des performances.



6.5 Phase 5: analyse de l'écart entre l'état réel et l'état souhaité; analyse des besoins de protection et des risques

- (1) La cinquième phase est consacrée à l'analyse de l'écart entre l'état réel et l'état souhaité, à l'analyse des besoins de protection et à l'analyse des risques:



Responsabilité:	Top management, C-Level, CISO, CRO, DPO, ISO
Compétence:	ISC, équipe de cybersécurité, spécialistes exécutants
Organismes impliqués:	Personnel spécifique de la sécurité de l'information (experts et consultants externes)
Points à traiter	<ul style="list-style-type: none">Analyse des écarts entre l'état actuel et l'état prévuDéfinir le besoin de protection pour un champ d'application supplémentaire dans l'ISMSDéfinir une méthodologie de gestion des risquesDéfinir les catégories et les critères de risqueDétermination des propriétaires du risque (Risk-Owner)Effectuer une gestion des risquesAnalyse des risques sur les menaces

Tableau 11: Phase 5 ISMS: analyse de l'écart entre l'état réel et l'état souhaité; analyse des besoins de protection et analyse des risques

6.5.1 Analyse de l'écart entre l'état réel et l'état souhaité

- (1) L'analyse de l'écart entre l'état réel et l'état souhaité dans le système de gestion de la sécurité de l'information (ISMS) est essentielle pour comparer les pratiques de sécurité existantes avec les objectifs à atteindre. L'analyse identifie les écarts entre l'état réel et l'état souhaité.
- (2) Pour commencer, les pratiques de sécurité actuelles sont évaluées de manière exhaustive, y compris les politiques, les processus et les technologies. Les aspects techniques, organisationnels et procéduraux doivent être pris en compte.
- (3) L'organisation définit ensuite des objectifs à atteindre en se basant sur les normes de sécurité, les exigences légales ou les directives spécifiques au secteur. L'état souhaité représente les pratiques de sécurité idéales.
- (4) L'analyse des écarts proprement dite compare l'état réel et l'état souhaité en identifiant les écarts. Cela comprend les aspects quantitatifs et qualitatifs, y compris l'évaluation des risques. Les écarts identifiés sont documentés et classés par ordre de priorité.
- (5) Les résultats constituent la base d'un plan de mesures visant à combler les lacunes. Ce dernier définit des objectifs clairs, des responsabilités, des délais et des exigences en matière de ressources.
- (6) L'analyse de l'écart entre l'état réel et l'état souhaité doit être répétée régulièrement, en particulier lorsque les exigences, le paysage des menaces ou les normes de sécurité évoluent. Elle permet ainsi une adaptation et une amélioration continues de l'ISMS.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS



Pour l'analyse GAP dans le domaine de la sécurité de l'information des contrôles dans le cadre du CSF NIST 1.1, l'outil «VSE&BFE-Assement-Tool_NIST-CSF-1.1_++» doit être utilisé.





L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.



Pour l'analyse GAP dans la sécurité de l'information des contrôles dans le cadre de l'ISO 27001 Annexe A, il convient d'utiliser l'«outil d'évaluation AES_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002».



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



Recommandation des experts de la Task Force Cyber Security de l'AES:
Les outils mis à disposition par l'AES doivent être utilisés pour la réalisation de l'analyse de la consommation réelle et théorique.

6.5.2 Définir le besoin de protection pour un champ d'application supplémentaire dans l'ISMS

- (1) Les prescriptions de l'ordonnance sur l'électricité définissent le besoin de protection selon le niveau de protection. Il est néanmoins recommandé de procéder à une analyse des besoins de protection dans le reste du domaine de la sécurité de l'information.
- (2) La définition des besoins de protection dans le cadre de l'ISMS vise à déterminer les exigences et les risques spécifiques pour certains actifs ou systèmes d'information. Pour ce faire, on procède à un inventaire détaillé et à une catégorisation des valeurs ou des systèmes dans le champ d'application supplémentaire, en se basant sur leur importance et leur effet potentiellement dommageable.
- (3) Une évaluation des risques analyse les menaces, les vulnérabilités et les conséquences potentielles en tenant compte des facteurs externes et internes. Sur cette base, les besoins de protection sont définis, y compris le niveau de protection requis et les mesures de sécurité appropriées.
- (4) La définition des besoins de protection s'effectue en coordination avec les objectifs stratégiques et l'ISMS global. Elle s'appuie sur les principes de gestion des risques afin d'aligner les décisions de sécurité sur les objectifs commerciaux.
- (5) La documentation du besoin de protection est essentielle et constitue la base des mesures de sécurité concrètes dans le champ d'application supplémentaire. Le processus itératif devrait être régulièrement contrôlé et mis à jour, notamment en cas d'évolution des exigences organisationnelles, des paysages de menaces ou des normes de sécurité. Cela permet une adaptation dynamique des mesures de protection pour une sécurité de l'information adéquate.



Recommandation des experts de la Task Force Cyber Security de l'AES:
Les directives de l'OApEI définissent le besoin minimal de protection pour les domaines selon le niveau de protection. Il est toutefois recommandé qu'une analyse des besoins de protection soit tout de même effectuée dans les autres domaines de la sécurité de l'information au sein de l'entreprise et des unités organisationnelles.

6.5.3 Définir une méthodologie de gestion des risques

- (1) La méthodologie de gestion des risques dans l'ISMS est essentielle pour identifier les risques de manière proactive et mettre en œuvre des mesures de sécurité appropriées. Le processus commence par la définition du champ d'application afin de rester concentré. L'identification des risques implique l'analyse des menaces, des vulnérabilités et des impacts potentiels, avec la participation des parties prenantes pertinentes.
- (2) Après l'identification, les risques sont évalués en termes de probabilité d'occurrence et d'impact potentiel. La définition de stratégies de traitement des risques se base sur les résultats, en tenant compte des objectifs de l'entreprise et de l'unité organisationnelle, des ressources et des tolérances aux risques.
- (3) La mise en œuvre de mesures de sécurité fait partie intégrante du traitement des risques et s'effectue conformément à la méthodologie. La surveillance et le contrôle continus des risques comprennent l'évaluation régulière des mesures mises en œuvre et l'adaptation en cas de changement.
- (4) L'adaptation flexible de la méthodologie à l'évolution des conditions et des exigences ainsi que l'amélioration continue du processus de gestion des risques sont essentielles. Une méthodologie bien pensée



contribue globalement à maintenir la sécurité de l'information à un niveau approprié en offrant une approche systématique de l'identification, de l'évaluation et du traitement des risques.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-03-02 Instructions de travail domaine ISMS: gestion des risques IT/OT



Recommandation des experts de la Task Force Cyber Security de l'AES:

La gestion des risques est importante car elle aide les entreprises à identifier, évaluer et gérer les dangers potentiels avant qu'ils ne deviennent des problèmes graves. En appliquant une méthodologie structurée, les organisations peuvent aborder les risques de manière proactive afin de minimiser les pertes, de saisir les opportunités et de garantir la stabilité à long terme. Une méthodologie efficace de gestion des risques offre également transparence et confiance aux investisseurs, aux clients et aux autres parties prenantes, ce qui favorise en fin de compte la croissance et la durabilité de l'entreprise.

6.5.4 Définir les catégories et les critères de risque

- (1) La définition de catégories et de critères de risque dans le cadre de l'ISMS est un processus stratégique d'identification, de classification et d'évaluation des risques. Ils constituent la base de l'analyse ultérieure des risques.
- (2) Pour commencer, les catégories de risques sont identifiées en classant les risques potentiels en groupes sur la base de caractéristiques communes, comme les risques techniques, organisationnels, personnels ou externes. Ensuite, des critères d'évaluation des risques sont définis afin de permettre une évaluation uniforme et comparable, que ce soit sur le plan quantitatif ou qualitatif.
- (3) Il est essentiel de lier étroitement les catégories et les critères de risque aux objectifs et aux processus commerciaux de l'organisation. Cela garantit que l'identification et l'évaluation sont adaptées aux exigences spécifiques, avec la participation des parties prenantes pertinentes.
- (4) Les définitions ne sont pas statiques, mais doivent être régulièrement revues et adaptées afin de s'adapter à l'évolution des exigences, des paysages de menaces et des stratégies commerciales. Cette flexibilité permet une évaluation des risques toujours actuelle et pertinente.
- (5) Les résultats servent de base à l'analyse des risques dans l'ISMS, facilitent l'identification et l'évaluation systématiques des risques et permettent ainsi le développement de mesures de sécurité efficaces. Globalement, la définition de catégories et de critères de risque établit une approche cohérente et acceptée dans toute l'organisation pour la gestion des risques.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-03-02 Instructions de travail domaine ISMS: gestion des risques IT/OT



Recommandation des experts de la Task Force Cyber Security de l'AES:

Les catégories de risques aident à identifier différents types de risques (p. ex. financiers, opérationnels). Les critères évaluent les risques en fonction de leur impact et de leur probabilité d'occurrence afin de définir des priorités et d'utiliser les ressources de manière efficace.

6.5.5 Détermination des propriétaires des risques (Risk-Owner)

- (1) L'identification des propriétaires des risques (risk owner) dans l'ISMS est essentielle pour garantir des responsabilités claires en matière d'identification, d'évaluation et de traitement des risques. Le propriétaire du risque est la personne ou l'unité organisationnelle qui est finalement responsable d'un risque spécifique et qui prend des décisions à son sujet.
- (2) La détermination des propriétaires des risques commence par l'identification et l'évaluation des risques, au cours desquelles chaque risque identifié est attribué à un propriétaire de risque. Celui-ci doit avoir l'expertise et l'autorité nécessaires pour prendre des décisions en rapport avec le risque.
- (3) Les responsabilités du propriétaire des risques comprennent la surveillance continue, la mise à jour de l'évaluation des risques, la définition de mesures d'atténuation des risques et la communication d'informations sur les risques aux parties prenantes concernées. La désignation du propriétaire du risque se fait en étroite collaboration avec les parties prenantes afin de garantir des responsabilités claires.



- (4) Ce processus est dynamique et devrait être régulièrement revu et adapté, notamment en cas de changements organisationnels, de nouveaux processus commerciaux ou d'évolution des profils de risque. La définition claire des propriétaires des risques contribue globalement à gérer les risques de manière efficace et efficace, en établissant des responsabilités et des processus de décision clairs.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations
- HoP-01-01-03-02 Instructions de travail domaine ISMS: gestion des risques IT/OT



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est important d'identifier les propriétaires des risques afin de définir clairement les responsabilités en matière de gestion des risques au sein de l'entreprise et de s'assurer que les risques sont gérés activement.

6.5.6 Effectuer une gestion des risques

- (1) La gestion des risques dans l'ISMS est un processus continu à plusieurs niveaux. Il commence par l'identification des menaces et des vulnérabilités potentielles en collaboration avec les parties prenantes. Les risques sont ensuite évalués et classés par ordre de priorité en fonction de critères prédéfinis afin de se concentrer sur les défis essentiels.
- (2) Vient ensuite le traitement des risques, au cours duquel des stratégies sont définies, telles que la mise en œuvre de mesures de sécurité ou l'acceptation de certains risques. Le suivi des mesures mises en œuvre garantit le maintien de la protection souhaitée, avec des ajustements en cas de changement dans l'organisation ou le paysage des menaces.
- (3) L'ensemble du processus est répété régulièrement, de nouvelles informations et expériences en matière d'incidents de sécurité pouvant conduire à des mises à jour de l'évaluation des risques et à des adaptations des stratégies de traitement des risques. L'objectif est de mettre en place une stratégie de sécurité proactive qui, grâce à des améliorations continues, permet de réagir avec souplesse à l'évolution des conditions et de maintenir la sécurité de l'information à un niveau optimal.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations
- HoP-01-01-03-02 Instructions de travail domaine ISMS: gestion des risques IT/OT



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'application de la gestion des risques dans l'ISMS est importante pour identifier les menaces potentielles, les évaluer et y répondre de manière appropriée afin de garantir la sécurité de l'information et de minimiser les risques.

6.5.7 Analyse des risques sur les menaces TOP

- (1) L'analyse des risques sur les menaces TOP dans l'ISMS se concentre sur les menaces les plus graves pour la sécurité de l'information. L'identification se fait par une analyse complète du paysage des menaces, en tenant compte des risques internes et externes.
- (2) L'évaluation des TOP menaces se fait sur la base de critères définis au préalable, qui tiennent compte des aspects techniques ainsi que des significations commerciales, réglementaires et stratégiques. Il s'ensuit l'élaboration de mesures de réduction des risques ciblées visant à aborder efficacement les risques les plus importants et à renforcer la sécurité de l'information.
- (3) La mise en œuvre des mesures se fait en étroite collaboration avec les parties prenantes et les propriétaires de risques concernés. Le processus dynamique exige des répétitions régulières afin de pouvoir réagir de manière flexible aux changements dans le paysage des menaces, aux nouvelles technologies ou aux adaptations commerciales.
- (4) Globalement, l'analyse des risques sur les menaces TOP permet à l'organisation de concentrer des ressources limitées sur les défis les plus critiques. Cela contribue au développement d'une stratégie de



sécurité de l'information efficace et efficiente afin de garantir que les risques les plus importants sont adressés de manière appropriée.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations
- HoP-01-01-03-02 Instructions de travail domaine ISMS: gestion des risques IT/OT

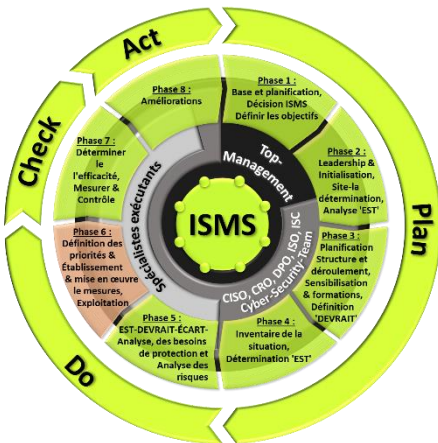


Recommandation des experts de la Task Force Cyber Security de l'AES:

L'analyse des risques sur les TOP menaces dans l'ISMS est importante pour se concentrer sur les risques les plus graves, utiliser efficacement les ressources et développer des mesures de sécurité ciblées pour minimiser ces risques. L'analyse des risques doit donc être effectuée dans un premier temps sur les menaces TOP actuelles. Par la suite, il est possible de simplifier la priorisation des mesures et de concentrer la protection sur les circonstances actuelles.

6.6 Phase 6: priorisation, établissement et mise en œuvre des mesures; exploitation

- (1) La sixième phase est entièrement placée sous le signe de la priorisation, de l'établissement et de la mise en œuvre des mesures. Elle traite également de l'exploitation pour la mise en œuvre continue des mesures:



Responsabilité:	Top management, C-Level, CISO, CRO, DPO, ISO
Compétence:	ISC, équipe de cybersécurité, spécialistes exécutants
Organismes impliqués:	Personnel spécifique de la sécurité de l'information (experts et consultants externes)
Points à traiter	<ul style="list-style-type: none">■ Elaborer un plan de mesures à partir de l'analyse GAP ou de l'analyse des risques■ Hiérarchiser les mesures■ Définir les exigences et les compétences du personnel■ Mettre en œuvre les mesures conformément à la priorisation■ Mettre en œuvre des mesures de communication, de formation et de sensibilisation■ Exploitation pour une mise en œuvre continue des mesures

Tableau 12: Phase 6 ISMS: priorisation, établissement et mise en œuvre des mesures; exploitation

6.6.1 Elaborer un plan de mesures à partir de l'analyse GAP ou de l'analyse des risques

- (1) L'élaboration d'un plan de mesures à partir de l'analyse GAP et de l'analyse des risques dans l'ISMS est décisive pour identifier les déficits et les risques et développer les mesures de protection correspondantes. L'analyse GAP compare les mesures de sécurité existantes aux objectifs de sécurité, identifie les lacunes et constitue la base du plan de mesures. L'analyse des risques se concentre sur l'évaluation des menaces et des vulnérabilités afin de définir les priorités des mesures de protection.
- (2) Le plan de mesures, développé en collaboration avec les parties prenantes concernées, comprend des objectifs, des responsabilités, des calendriers et des ressources clairs pour chaque mesure. La priorisation est basée sur l'évaluation des risques et l'urgence. La communication avec les employés et la formation en font partie intégrante, tout comme la mise en œuvre progressive et le suivi continu.
- (3) L'évaluation des mesures se fait par des contrôles réguliers, des audits et des métriques de sécurité. Cela s'intègre dans le cycle d'amélioration continue de l'ISMS. Globalement, le développement du plan de mesures renforce la sécurité de l'information, adapte l'ISMS aux exigences actuelles et favorise une amélioration continue du niveau de sécurité.





Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



Les outils «VSE&BFE-Tool_for_NIST-CSF-1.1_Checkpoints_acc.to_NIST-SP800-53_CCM_CIS» et «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002» doivent être utilisés pour le plan des mesures.



L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



Les différents points du plan de mesures doivent être introduits dans les documents Maison des politiques correspondants (directives et instructions de travail) et traités en conséquence.



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'élaboration d'un plan de mesures à partir de l'analyse GAP ou de l'analyse des risques est importante pour combler les lacunes identifiées et réduire les risques afin que l'entreprise soit mieux préparée à relever les défis potentiels.

6.6.2 Hiérarchiser les mesures

- (1) La priorisation des mesures issues de l'analyse GAP et de l'analyse des risques dans l'ISMS est un processus stratégique qui permet de cibler les mesures de protection sur les principaux défis. L'analyse GAP identifie les différences entre les mesures actuelles et les normes. L'analyse des risques évalue les menaces potentielles. La hiérarchisation est basée sur une approche globale, prend en compte la gravité, l'impact, la probabilité et les facteurs externes tels que les exigences légales. Les aspects liés aux ressources et à la faisabilité jouent un rôle.
- (2) Un dialogue itératif avec les parties prenantes, dont les responsables de la sécurité et les cadres, est essentiel. Le plan de priorisation qui en résulte donne des instructions claires pour la mise en œuvre, prend en compte différents types de mesures et s'oriente sur le calendrier. Une révision et une adaptation régulières sont indispensables pour adapter en permanence les mesures de protection à l'évolution des conditions et garantir une utilisation efficace des ressources.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



Le «VSE&BFE-Tool_for_NIST-CSF-1.1_Checkpoints_acc.to_NIST-SP800-53_CCM_CIS» et le «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002» doivent être utilisés pour le plan des mesures et la priorisation.



L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.





Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



La hiérarchisation des mesures doit, si nécessaire, être intégrée dans les documents correspondants de la Maison des politiques (directives et instructions de travail) et traitée en conséquence.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Il est important de prioriser les mesures issues de l'analyse GAP et de l'analyse des risques afin d'utiliser efficacement les ressources et de se concentrer sur les domaines les plus critiques afin d'obtenir les plus grandes améliorations et de minimiser les risques.

6.6.3 Définir les exigences et les compétences du personnel

- (1) La définition des exigences et des compétences en matière de personnel dans l'ISMS est essentielle pour la mise en œuvre effective des mesures prioritaires. Cela nécessite une évaluation approfondie des compétences requises, y compris l'expertise technique dans des domaines tels que la sécurité du réseau ou la conformité. La sélection des membres de l'équipe doit permettre de créer une équipe équilibrée, dotée de compétences et d'expériences variées, adaptées à la nature des mesures. La sensibilisation aux évolutions actuelles, la capacité d'adaptation et l'esprit proactif sont des compétences essentielles.
- (2) L'implication des parties prenantes pertinentes et des formations régulières sont essentielles pour garantir que les équipes répondent aux objectifs stratégiques et restent à jour. Les compétences en matière de communication et de travail en équipe sont tout aussi importantes que les connaissances techniques spécialisées, afin de garantir que les mesures ne sont pas seulement efficaces sur le plan technique, mais aussi réalisables sur le plan organisationnel. Globalement, la définition des exigences et des compétences en matière de personnel est un processus dynamique qui s'adapte à l'évolution des exigences et des menaces. Une équipe bien constituée et dotée des bonnes compétences est essentielle pour mettre en œuvre efficacement les mesures de sécurité et renforcer la sécurité de l'information.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-01-01 Instructions de travail Domaine SGI: Sécurité de l'information Organisation
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



Les exigences et compétences en matière de personnel doivent être introduites dans les documents de la Maison des politiques concernés (directives et instructions de travail) et traitées en conséquence.



Recommandation des experts de la Task Force Cyber Security de l'AES:

La définition des exigences et des compétences en matière de personnel dans l'ISMS est essentielle pour garantir que l'équipe dispose des capacités nécessaires pour mettre en œuvre efficacement les mesures prioritaires et exploiter avec succès le système de gestion de la sécurité de l'information. Il est souvent nécessaire de faire appel à des ressources externes.

6.6.4 Mettre en œuvre les mesures conformément à la priorisation

- (1) La mise en œuvre de mesures prioritaires dans l'ISMS est essentielle pour combler les failles de sécurité et minimiser les risques de manière appropriée. Les équipes se voient attribuer des responsabilités claires et travaillent en étroite collaboration avec les parties prenantes. Des mesures techniques, organisationnelles et procédurales sont mises en œuvre, notamment les nouvelles technologies, les formations et les processus nécessaires.
- (2) Une communication et un suivi continus sont des facteurs clés pour identifier les obstacles et évaluer les progrès. Une adaptation flexible aux changements et une collaboration étroite entre les équipes et les parties prenantes sont indispensables.



- (3) Le processus itératif nécessite une planification claire, une communication transparente et une surveillance continue afin de renforcer la sécurité de l'organisation et d'atteindre les objectifs ISMS fixés.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01-01 Directive domaine SGI: cadre de la sécurité de l'information
- HoP-01-01-01-01 Instructions de travail Domaine SGI: Sécurité de l'information Organisation
- HoP-01-01-02 Directive domaine SGI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



L'outil «VSE&BFE-Tool_for_NIST-CSF-1.1_Checkpoints_acc.to_NIST-SP800-53_CCM_CIS» et «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002» doivent être utilisés comme aide pour la mise en œuvre des mesures.



L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



La hiérarchisation des mesures doit, si nécessaire, être intégrée dans les documents correspondants de la Maison des politiques (directives et instructions de travail) et traitée en conséquence.



Recommandation des experts de la Task Force Cyber Security de l'AES:

La mise en œuvre des mesures conformément à la priorisation dans l'ISMS est importante, doit être mise en œuvre en temps opportun et de manière continue afin d'utiliser efficacement les ressources et de se concentrer sur les domaines les plus critiques afin d'améliorer efficacement la sécurité de l'information et de minimiser les risques.

6.6.5 Mettre en œuvre des mesures de communication, de formation et de sensibilisation

- (1) La mise en œuvre de mesures de communication, de formation et de sensibilisation dans l'ISMS est essentielle pour renforcer la conscience de la sécurité des employés. Les mesures de communication transmettent l'importance de la sécurité de l'information par des canaux internes mais aussi aux parties prenantes externes telles que les prestataires / fabricants, les partenaires et les clients par une communication externe ciblée.
- (2) Les mesures de formation offrent des connaissances spécifiques, y compris les aspects techniques et organisationnels. Les mesures de sensibilisation sensibilisent aux thèmes liés à la sécurité par le biais de matériel d'information et de simulations.
- (3) Une communication claire, des ressources pour la formation et un climat de sécurité positif sont essentiels. L'évaluation des mesures garantit des adaptations à l'évolution des menaces et des exigences. Cette approche globale crée une conscience culturelle de la sécurité de l'information grâce à des efforts continus.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01-03-04 Instructions de travail domaine ISMS: formation et sensibilisation
- HoP-01-01-03-21 Instructions de travail domaine ISMS: mesures de sécurité pour les prestataires de services
- HoP-01-01-03-22 Instructions de travail domaine ISMS: gestion des fournisseurs
- HoP-01-01-03-23 Instructions de travail domaine ISMS: sécurité de l'information dans le domaine des ressources humaines
- HoP-01-01-03-24 Instructions de travail domaine ISMS: sécurité de l'information dans les projets



Les documents suivants contiennent des orientations et des instructions:

- Programme de formation selon la publication spéciale NIST 800-50





Il faut s'assurer que les mesures de communication, de formation et de sensibilisation nécessaires sont également appliquées chez les prestataires de services, les fournisseurs et dans les projets.



Recommandation des experts de la Task Force Cyber Security de l'AES:

La mise en œuvre de mesures de communication, de formation et de sensibilisation dans l'ISMS est importante et doit être appliquée en permanence afin de promouvoir la compréhension de la sécurité de l'information, de sensibiliser les employés et d'améliorer leurs capacités à réduire les risques, ce qui, au final, augmente la sécurité de l'entreprise et des unités organisationnelles. Il est recommandé d'élaborer et de mettre en œuvre un programme de formation conformément à la publication spéciale 800-50 du NIST.

6.6.6 Mise en œuvre continue des mesures

- (1) La mise en œuvre continue des mesures de sécurité de l'information dans l'ISMS est un processus permanent qui comprend le suivi, les audits et les mises à jour régulières. Les informations et les événements relatifs à la sécurité permettent de détecter à temps les incidents potentiels. Les audits garantissent l'efficacité, identifient les points faibles et les connaissances acquises sont intégrées dans le processus d'amélioration.
- (2) L'adaptation régulière des directives de sécurité se fait en collaboration avec les parties prenantes. La formation et la sensibilisation continues sont essentielles, tout comme la révision et l'adaptation permanentes de l'évaluation des risques. L'intégration de plans de réponse aux incidents avec des procédures claires en cas d'incident est essentielle, et des exercices réguliers testent leur efficacité. L'étroite collaboration entre les unités organisationnelles au sein de l'ISMS favorise l'adaptation aux changements de conditions.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-01-01 Instructions de travail Domaine SGI: Sécurité de l'information Organisation
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



Les outils «VSE&BFE-Tool_for_NIST-CSF-1.1_Checkpoints_acc.to_NIST-SP800-53_CCM_CIS» et «VSE-Assessment-Tool_ISO27001-Annex-A_incl._Controls_acc.to_ISO27002» doivent être utilisés comme aide à la mise en œuvre continue des mesures.



L'utilisation de tous les documents et normes du NIST est gratuite et peut donc être utilisée sans restriction.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



La hiérarchisation des mesures doit, si nécessaire, être intégrée dans les documents correspondants de la Maison des politiques (directives et instructions de travail) et traitée en conséquence.



Recommandation des experts de la Task Force Cyber Security de l'AES:

La mise en œuvre continue des mesures de l'ISMS est importante et doit être activement encouragée afin de garantir en permanence la sécurité de l'information, de s'adapter à l'évolution des menaces et de maintenir l'efficacité du système.



6.7 Phase 7: détermination de l'efficacité; mesure et contrôle

- (1) La septième phase est consacrée à la vérification de l'efficacité de l'ISMS. La mesure et le contrôle de l'ISMS sont également abordés.

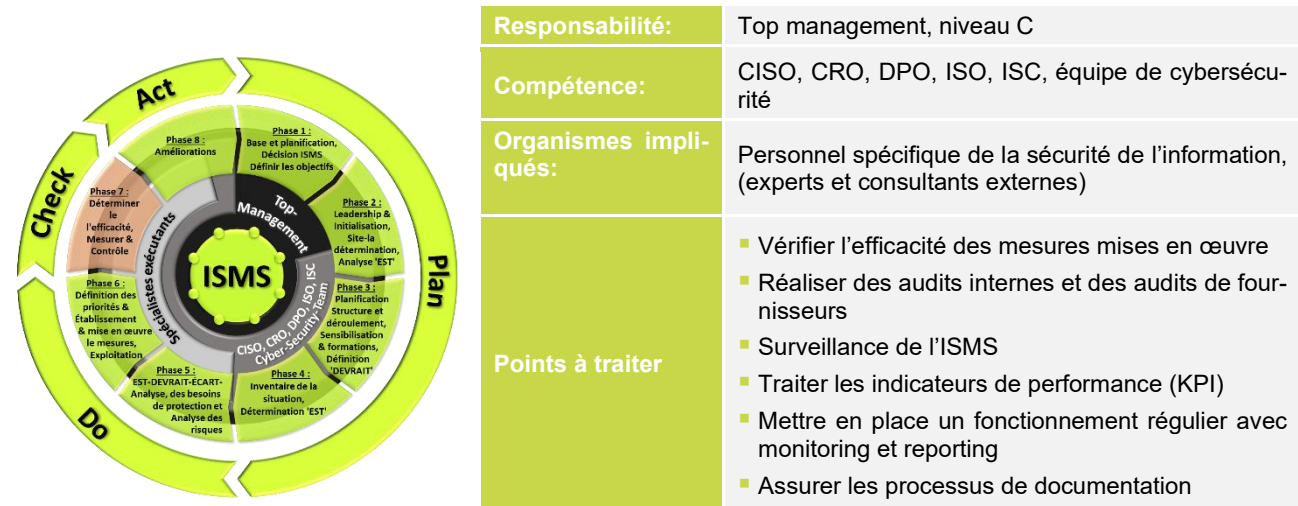


Tableau 13: Phase 7 ISMS: détermination de l'efficacité; mesure et contrôle

6.7.1 Vérifier l'efficacité des mesures mises en œuvre

- (1) La vérification des mesures ISMS est essentielle pour garantir la protection souhaitée et les objectifs de sécurité. Ce processus nécessite des critères clairs liés aux objectifs ISMS. Des audits et des surveillances systématiques évaluent les aspects techniques, organisationnels et procéduraux.
- (2) Les résultats identifient les points faibles qui sont pris en compte dans le processus d'amélioration continue. La communication se fait à différents niveaux, y compris au niveau de la direction. L'examen est un cycle continu qui rend l'ISMS agile face aux nouvelles menaces et technologies et permet des adaptations à long terme.
- (3) Globalement, l'audit est un élément essentiel du cycle de vie de l'ISMS, qui considère la sécurité de l'information comme un processus dynamique.



Recommandation des experts de la Task Force Cyber Security de l'AES:
Il est important de vérifier l'efficacité des mesures mises en œuvre dans l'ISMS afin de s'assurer qu'elles produisent effectivement les résultats escomptés et améliorent la sécurité de l'information, et de procéder à des ajustements si nécessaire. La vérification des mesures mises en œuvre peut se faire de différentes manières:

- Tests d'intrusion
- Vérification du savoir-faire
- Audits internes et externes
- etc.

6.7.2 Réaliser des audits internes et des audits de fournisseurs

- (1) La réalisation d'audits internes et de fournisseurs dans le cadre de l'ISMS garantit la mise en œuvre effective des politiques et processus de sécurité dans l'ensemble de la chaîne d'approvisionnement. Les audits internes vérifient le respect des directives de sécurité et l'efficacité de l'ISMS. Les audits des fournisseurs se concentrent sur le niveau de sécurité des partenaires et fournisseurs externes.
- (2) Une planification claire, le choix d'auditeurs objectifs et des vérifications systématiques sont essentiels. Les résultats donnent lieu à des recommandations d'amélioration qui sont partagées avec les parties concernées.
- (3) La mise en œuvre de formations, d'adaptations des politiques de sécurité et d'améliorations techniques se fait en réaction aux résultats des audits. Dans l'ensemble, ces audits font partie intégrante de l'ISMS, afin de garantir des mesures de sécurité efficaces et de veiller au respect des normes.



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-00-01-04 Instructions de travail domaine SGI: audits
- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information



- HoP-01-01-01 Instructions de travail Domaine SGI: Sécurité de l'information Organisation
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-03 Directive domaine ISM: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



Recommandation des experts de la Cyber Security Task Force de l'AES:

Les audits internes et des fournisseurs dans le cadre de l'ISMS sont importants et doivent être activement encouragés afin de vérifier le respect des normes de sécurité, de détecter les vulnérabilités potentielles et de s'assurer que toutes les parties impliquées mettent en œuvre et maintiennent les mesures de sécurité nécessaires. Le droit d'auditer les fournisseurs doit être inclus dans les contrats avec les fournisseurs. Définissez les points de contrôle que vous souhaitez vérifier ainsi que la vérification des risques des sous-traitants.

6.7.3 Surveillance de l'ISMS

- (1) La surveillance de l'ISMS dans le domaine de la sécurité de l'information est essentielle pour garantir l'efficacité des mesures de sécurité, procéder à des adaptations en fonction des menaces et respecter les normes de sécurité. Cela comprend l'examen continu des contrôles de sécurité, des mesures techniques telles que les analyses de protocole et les tests d'intrusion. Les aspects organisationnels tels que la formation et la conformité des employés sont également surveillés. Le respect des exigences légales est documenté et régulièrement mis à jour.
- (2) La surveillance comprend également l'évaluation des incidents de sécurité afin d'identifier les causes et de mettre en œuvre des mesures préventives. Les rapports réguliers informent les parties prenantes de l'efficacité de l'ISMS et servent de base aux décisions stratégiques. L'identification des possibilités d'amélioration se base sur l'analyse des résultats de la surveillance et sur le feedback reçu.
- (3) En résumé, la surveillance garantit que les mesures de sécurité de l'information sont agiles et s'améliorent continuellement pour répondre à l'évolution des menaces et des besoins de l'entreprise.



Références à des documents complémentaires:

- Norme BSI 200-1 Systèmes de gestion de la sécurité de l'information (ISMS)
- ISO/IEC 27004 ISMS Surveillance, mesure, analyse et évaluation



Les points sont illustrés dans les documents types suivants dans les annexes:

- HoP-01-00-01-04 Instructions de travail domaine SGI: audits
- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-01-01 Instructions de travail Domaine SGI: Sécurité de l'information Organisation
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03 Directive domaine GSI: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



Recommandation des experts de la Task Force Cyber Security de l'AES:

La surveillance de l'ISMS est essentielle pour s'assurer que les politiques et procédures de sécurité sont efficaces, que les menaces potentielles sont détectées à un stade précoce et que l'intégrité de la sécurité de l'information est garantie. L'outil mis à disposition par l'AES doit être utilisé pour la surveillance de l'ISMS.



L'outil «VSE-Tool_ISO27001-ISMS_Assessment-Goals» peut être utilisé pour surveiller l'ISMS.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



6.7.4 Traiter les indicateurs de performance (KPI)

- (1) Le traitement des KPI's dans l'ISMS est central pour mesurer l'efficacité des mesures de sécurité, surveiller les objectifs de sécurité et promouvoir l'amélioration continue. Les KPI's appropriés sont établis par des définitions d'objectifs claires dans l'ISMS, orientées vers les objectifs stratégiques de l'organisation. La mise en œuvre implique la définition d'indicateurs de mesure quantifiables qui font l'objet d'un suivi régulier.
- (2) Le suivi se fait en continu, des outils automatisés fournissant des informations en temps réel. L'interprétation des KPI nécessite une analyse approfondie afin d'identifier les tendances ou les écarts et de réagir de manière proactive aux risques. La communication des résultats à la direction et aux autres parties prenantes favorise la compréhension de la situation en matière de sécurité.
- (3) L'utilisation des KPI comme base d'amélioration continue clôt le processus en intégrant les résultats dans l'exploitation régulière. Dans l'ensemble, le traitement des KPI est un processus itératif qui permet d'améliorer l'ISMS de manière ciblée grâce à une définition claire des objectifs, une mise en œuvre systématique, un suivi continu, une analyse complète et l'intégration des enseignements dans l'exploitation normale.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03 Directive domaine GSI: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



Recommandation des experts de la Task Force Cyber Security de l'AES:

Le traitement des indicateurs de performance (KPI) dans l'ISMS est important et doit être activement encouragé afin de mesurer l'efficacité du système de gestion de la sécurité de l'information, d'identifier les points faibles et de permettre des améliorations.

6.7.5 Mettre en place un fonctionnement régulier avec monitoring et reporting

- (1) L'établissement d'un fonctionnement régulier avec surveillance et rapport dans l'ISMS garantit l'efficacité des mesures de sécurité mises en œuvre. Des rôles et des responsabilités clairs sont systématiquement mis en œuvre, tandis que le monitoring surveille les activités du réseau et d'autres événements liés à la sécurité.
- (2) Le reporting transforme les résultats de la surveillance en rapports réguliers contenant les incidents de sécurité, le statut de conformité et l'efficacité des contrôles. Des mécanismes de reporting automatisés facilitent ce processus et permettent d'établir des rapports en temps réel.
- (3) Le management joue un rôle central dans l'évaluation des rapports, la définition des priorités et l'initiation des adaptations de l'ISMS. Globalement, l'établissement du fonctionnement régulier est un processus continu qui garantit que les mesures de sécurité de l'information restent actuelles, efficaces et adaptables.



Les documents suivants contiennent des orientations et des instructions:

- Norme BSI 200-1 Systèmes de gestion de la sécurité de l'information (ISMS)

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports
- HoP-01-01-03 Directive domaine GSI: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes





Recommandation des experts de la Task Force Cyber Security de l'AES:

Il faut établir et promouvoir activement un fonctionnement régulier avec suivi et reporting dans l'ISMS afin de surveiller en permanence la sécurité de l'information, d'identifier les menaces potentielles à un stade précoce et d'y réagir de manière appropriée afin de garantir l'intégrité, la confidentialité et la disponibilité des informations. Il faut s'assurer à tout moment que la direction est également informée de l'état le plus récent de la sécurité de l'information.

6.7.6 Assurer les processus de documentation

- (1) Assurer les processus de documentation dans l'ISMS est essentiel pour garantir des informations claires, précises et à jour. Le processus commence par l'identification de la documentation nécessaire, dont les politiques de sécurité, les procédures et les protocoles. Les documents nécessaires, qui tiennent compte des normes du secteur et des exigences légales, sont élaborés en étroite collaboration avec les experts en sécurité et les responsables.
- (2) L'actualité est garantie par des vérifications et des mises à jour régulières, notamment en cas de changements dans la structure de l'entreprise et des unités organisationnelles. Une équipe de gestion des documents ou des responsables de la sécurité sont chargés de la maintenance, tandis que des formations garantissent que les employés comprennent et respectent les documents. Des audits réguliers garantissent le respect des normes et identifient les possibilités d'amélioration.
- (3) La démarche est un processus continu et itératif qui garantit l'efficacité et l'adaptabilité de la documentation relative à la sécurité de l'information grâce à une identification claire, une rédaction précise, une mise à jour régulière, une accessibilité adéquate et des formations.

Les points sont illustrés dans les documents types suivants dans les annexes:



- HoP-01-00-00-02 Instructions de travail domaine SGI: Maison des politiques
- HoP-01-00-00-03 Instructions de travail domaine SGI: maîtrise des documents
- HoP-01-00-01-04 Instructions de travail domaine SGI: audits
- HoP-01-01-01 Directive domaine GSI: cadre de la sécurité de l'information
- HoP-01-01-01-01 Instructions de travail Domaine SGI: Sécurité de l'information Organisation
- HoP-01-01-02 Directive domaine GSI: Champ d'application, mise en place et fonctionnement de l'ISMS
- HoP-01-01-03 Directive domaine GSI: scénario de référence dans l'ISMS et instructions de travail y afférentes
- HoP-01-01-04 Directive Sécurité de l'information Utilisateurs de valeurs d'information et instructions de travail correspondantes



Recommandation des experts de la Task Force Cyber Security de l'AES:

La garantie du processus de documentation dans l'ISMS est importante, doit être vécue et doit être activement encouragée afin d'enregistrer les politiques, les procédures et les décisions, ce qui permet le suivi, le respect et l'amélioration continue de la sécurité de l'information. L'outil mis à disposition par l'AES doit être utilisé pour garantir le processus de documentation dans l'ISMS.



L'outil «VSE-Tool_ISO27001-ISMS_Assessment-Goals» peut être utilisé pour assurer le processus de documentation de l'ISMS.

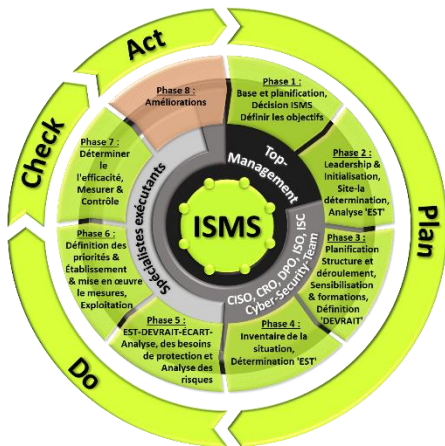


Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



6.8 Phase 8: Améliorations

(1) La huitième phase est placée sous le signe des améliorations:



Responsabilité:	Top management, niveau C
Compétence:	CISO, CRO, DPO, ISO, ISC, équipe de cybersécurité
Organismes impliqués:	Personnel spécifique de la sécurité de l'information, spécialistes de l'exécution (experts et consultants externes)
Points à traiter	<ul style="list-style-type: none">■ Correction et mesures préventives■ Examen des possibilités d'amélioration■ Vivre un processus d'amélioration continue

Tableau 14: Phase 8 ISMS: Améliorations

6.8.1 Correction et mesures préventives

- (1) La procédure d'actions correctives et préventives de l'ISMS est un processus systématique visant à résoudre les incidents de sécurité et à prévenir les événements futurs. En cas d'incident, des mesures immédiates sont essentielles pour limiter les dégâts et rétablir l'intégrité du système.
- (2) Après la phase de correction, une enquête approfondie est menée afin d'identifier les causes et de développer des mesures préventives. Celles-ci peuvent inclure des politiques de sécurité, de nouveaux contrôles, des formations ou des améliorations technologiques. Leur efficacité est évaluée par des contrôles et des audits réguliers. L'intégration dans l'ISMS documente les mesures réussies et assure des changements durables dans la culture de sécurité de l'organisation.
- (3) Cette approche répétitive permet d'améliorer constamment la sécurité de l'information et de réagir efficacement à l'évolution des menaces.



Recommandation des experts de la Task Force Cyber Security de l'AES:
Les mesures correctives et préventives du ISMS sont importantes et doivent être activement encouragées afin de résoudre les problèmes survenus et d'empêcher de futurs incidents de sécurité, améliorant ainsi la sécurité de l'information et minimisant les risques. L'outil mis à disposition par l'AES doit être utilisé pour améliorer l'ISMS.



L'outil «VSE-Tool_ISO27001-ISMS_Assessment-Goals» peut être utilisé pour améliorer l'ISMS.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

6.8.2 Examen des possibilités d'amélioration

- (1) L'examen des possibilités d'amélioration de l'ISMS est un processus essentiel pour identifier les points faibles, les mesures de sécurité inefficaces et pour augmenter l'efficacité globale. Le processus commence par une analyse approfondie des mesures de sécurité existantes par le biais d'audits internes et de contrôles de sécurité.
- (2) Les points faibles et les risques, tant techniques qu'organisationnels, sont identifiés. Les données collectées servent de base à l'identification des domaines d'amélioration dans lesquels l'ISMS ne répond pas aux normes ou dans lesquels des gains d'efficacité sont possibles. S'ensuit l'élaboration de mesures correctives, qui font l'objet d'un suivi continu pendant la mise en œuvre.
- (3) Une évaluation complète des résultats est effectuée après la mise en œuvre, en tenant compte du retour d'information de différentes unités organisationnelles. Les mesures réussies sont documentées en tant que bonnes pratiques et intégrées dans les politiques de sécurité. Dans l'ensemble, l'examen des



possibilités d'amélioration est un processus itératif qui permet à l'organisation de s'adapter efficacement à l'évolution des menaces et des exigences.



Références à des documents complémentaires:

- Norme BSI 200-1 Systèmes de gestion de la sécurité de l'information (ISMS)
- ISO/IEC 27004 ISMS Surveillance, mesure, analyse et évaluation



Recommandation des experts de la Task Force Cyber Security de l'AES:

L'outil mis à disposition par l'AES doit être utilisé pour vérifier les améliorations apportées au ISMS.



L'outil «VSE-Tool_ISO27001-ISMS_Assessment-Goals» peut être utilisé pour examiner les possibilités d'amélioration de l'ISMS.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

6.8.3 Maintenir un processus d'amélioration continue

- (1) Le processus d'amélioration continue de l'ISMS garantit l'optimisation continue des pratiques et des processus de sécurité d'une organisation. Ce processus passe par des cycles récurrents qui visent à identifier les points faibles, à établir les bonnes pratiques et à promouvoir une culture de sécurité solide. Le processus d'amélioration continue commence par la collecte de données sur les mesures de sécurité existantes par le biais d'audits internes, de surveillances, d'incidents de sécurité et de feedback des employés.
- (2) Les informations recueillies servent de base à l'identification des domaines d'amélioration. Des objectifs et des mesures clairement définis, comme la mise à jour des directives de sécurité ou la formation des employés, sont établis. Les objectifs sont mesurables afin de pouvoir suivre les progrès. Pendant la phase de mise en œuvre, les mesures sont appliquées, accompagnées d'un suivi qui peut inclure des vérifications techniques et des simulations d'incidents de sécurité.
- (3) Les résultats sont analysés afin de s'assurer que les mesures mises en œuvre apportent les améliorations prévues. La vérification et l'évaluation sont essentielles, et le feed-back des employés et des cadres est pris en compte. Le cycle de processus d'amélioration continue s'achève par la standardisation. Les mesures réussies sont documentées en tant que bonnes pratiques et intégrées dans les directives de sécurité. Cela garantit que les changements positifs sont intégrés durablement dans la culture d'entreprise. Le cycle de vie itératif du processus d'amélioration continue garantit que la sécurité de l'information est optimisée en permanence et adaptée à l'évolution des menaces.



Recommandation des experts de la Task Force Cyber Security de l'AES:

Le processus d'amélioration continue de l'ISMS doit être vécu et encouragé afin d'accroître l'efficacité du système de gestion de la sécurité de l'information et de suivre l'évolution des menaces grâce à un retour d'information et à des ajustements réguliers.



7. Interaction entre les documents de l'AES et les outils de l'AES

Le graphique suivant montre comment les documents de l'AES et les outils de l'AES sont liés pour augmenter la résilience des TIC. Il montre où les inputs des entreprises et des unités organisationnelles sont nécessaires et lesquels.

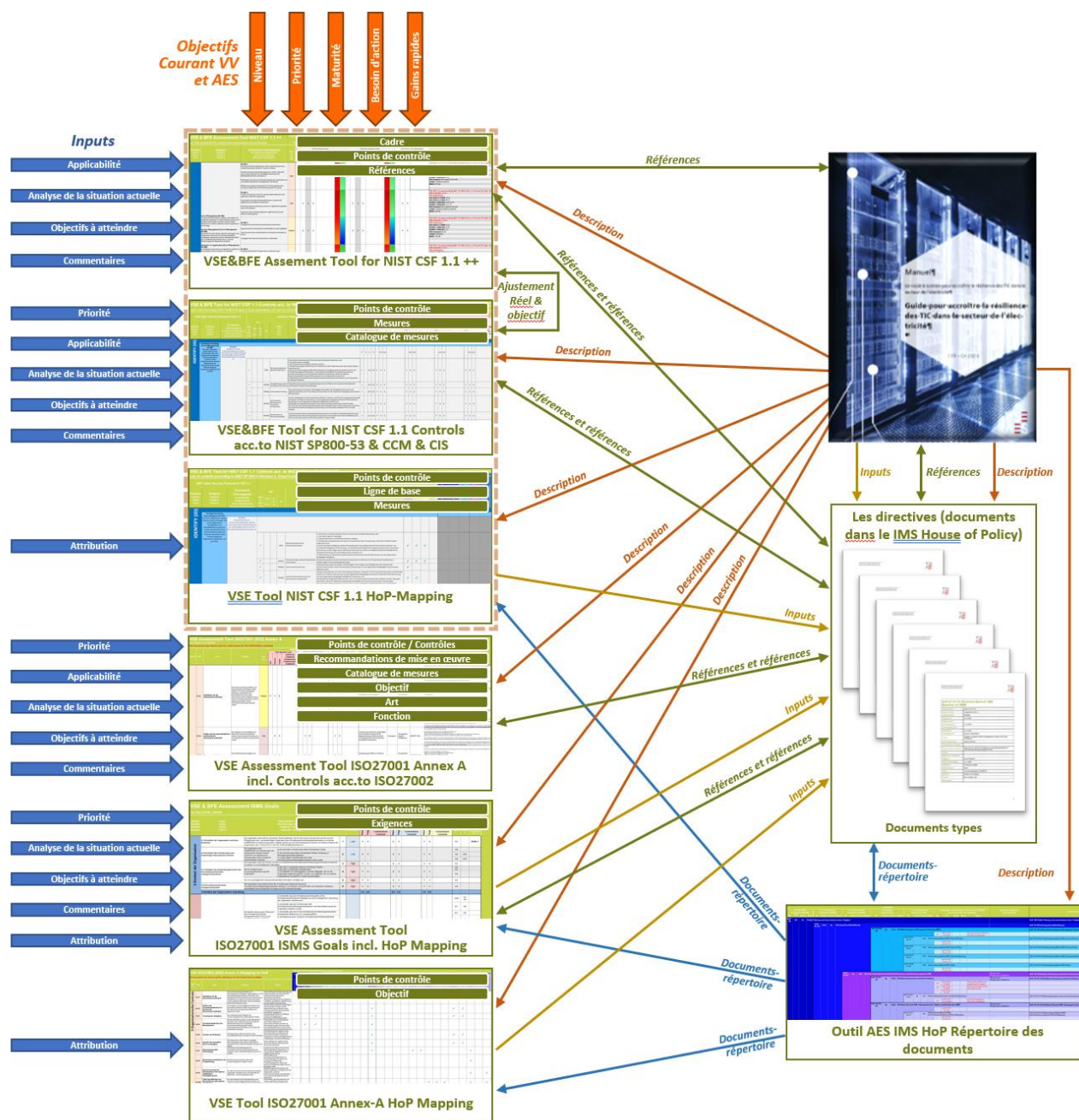


Figure 28: Interaction des documents de l'AES avec les outils de l'AES pour augmenter la résilience des TIC (source AES)

8. Conclusion et résumé

- (1) Les conclusions du guide sur l'amélioration de la résilience des TIC dans le domaine de la sécurité de l'information soulignent l'importance d'une approche globale pour renforcer la résilience des technologies de l'information et de la communication face aux menaces et aux perturbations.
- (2) Le guide souligne la nécessité d'une évaluation complète des risques afin d'identifier les vulnérabilités et les risques spécifiques dans l'infrastructure TIC. Cela permet de développer des mesures ciblées pour renforcer la résilience. L'accent est mis non seulement sur les aspects technologiques, mais aussi sur les aspects organisationnels et les processus.
- (3) Un aspect central est la prise en compte de la résilience des TIC dans toutes les phases du cycle de vie des TIC, de la planification et de la mise en œuvre au suivi et à l'amélioration continue. Cela nécessite une étroite collaboration entre les experts en TIC, les responsables de la sécurité et les décideurs à tous les niveaux de l'organisation.
- (4) Le guide souligne également l'importance de la formation et de la sensibilisation afin de s'assurer que tous les employés de l'organisation comprennent le rôle de la résilience des TIC et peuvent y contribuer activement. Cela inclut également des mesures de sensibilisation aux risques de sécurité et de formation à la gestion des incidents de sécurité potentiels.
- (5) Une conclusion décisive est la nécessité de surveiller et d'adapter en permanence les mesures de résilience des TIC. Le paysage des menaces étant en constante évolution, il est important que les entreprises et les unités organisationnelles puissent réagir de manière flexible aux nouveaux défis. Cela nécessite des révisions régulières, des mises à jour des politiques et l'intégration de nouvelles technologies pour répondre à l'évolution des besoins.
- (6) En outre, il est souligné que la collaboration au niveau sectoriel et international joue un rôle important. Les informations et les meilleures pratiques doivent être partagées entre les entreprises et les unités organisationnelles afin de construire ensemble une infrastructure TIC plus résistante. Cela nécessite une communication ouverte et la volonté d'apprendre les uns des autres.
- (7) Dans l'ensemble, le guide sur le renforcement de la résilience des TIC dans le domaine de la sécurité de l'information met en évidence le fait que la résilience ne doit pas être considérée uniquement comme une réponse aux menaces, mais comme une partie intégrante de la planification stratégique et de la mise en œuvre des systèmes TIC. Une approche proactive, une adaptation continue et une collaboration à différents niveaux sont essentielles pour renforcer la résilience face aux cybermenaces et autres risques.



Anhang A: Annexe A: Glossaire

Terme	Description
Anti-virus	Logiciel aussi appelé scanner de virus. Programme qui protège l'ordinateur contre les virus, les vers et les chevaux de Troie.
Attachment	(Pièce jointe). Fichier joint à un e-mail. De nombreux programmes malveillants (malware, crimeware) se propagent ainsi et sont activés par l'ouverture du message ou l'ouverture de la pièce jointe. Les pièces jointes ne devraient donc être ouvertes que si l'on utilise un logiciel antivirus et si l'on connaît l'expéditeur du message.
Sauvegarde (backup)	Opération consistant à empêcher la perte éventuelle de données en les stockant sur des supports de stockage externes.
Nom d'utilisateur	(Username) Généralement utilisé en combinaison avec un mot de passe pour se connecter à un service (par exemple, internet) ou à un programme. Système d'exploitation Logiciel système, appelé «OS» (Operating System) dans sa forme abrégée en anglais. Il s'agit d'un ensemble de programmes spéciaux qui rendent l'ordinateur et les programmes d'application (p. ex. Microsoft Word ou Excel) utilisables.
Navigateur	Programme que l'on utilise pour consulter des informations sur internet. (par ex. Internet Explorer, Opera ou Firefox)
Gestion de la continuité des activités (BCM)	Le Business Continuity Management (BCM) est une approche à l'échelle de l'entreprise qui permet de garantir que les processus commerciaux critiques peuvent être maintenus en cas d'événements internes ou externes massifs et importants. Le BCM vise à minimiser les conséquences opérationnelles, financières, juridiques et de réputation de tels événements (source: directive BCM).
Business Impact Analysis (BIA)	L'analyse d'impact sur les activités (BIA) est une analyse qui évalue l'impact des interruptions sur les processus d'entreprise afin d'identifier les fonctions et les ressources critiques et de planifier les mesures d'urgence appropriées.
Client	Ordinateur connecté à un réseau et communiquant avec d'autres ordinateurs.
Cracker	Un pirate informatique qui utilise ses connaissances et son expérience pour nuire à autrui.
Crimeware	Terme général pour les programmes utilisés par les crackers et les être utilisés par d'autres utilisateurs d'ordinateurs criminels pour nuire à d'autres utilisateurs d'ordinateurs. La plupart du temps, les crimewares visent à voler de l'argent ou des informations précieuses (p. ex. numéro de carte de crédit). Une forme moins agressive est appelée spyware.
Cybersécurité	Le terme «cybersécurité» désigne toutes les mesures organisationnelles et techniques visant à protéger la disponibilité, l'intégrité et la confidentialité des informations, tant dans le domaine informatique que dans celui de l'informatique opérationnelle.
Datadiode	Une datadiode est un périphérique réseau qui n'autorise le trafic réseau que dans une seule direction. Les données ne peuvent être échangées que d'une zone réseau sécurisée vers une zone réseau non sécurisée, mais pas de la zone non sécurisée vers la zone sécurisée.
Défense-in-depth	On entend par «Defense-in-Depth» des concepts de sécurité à plusieurs niveaux qui vont au-delà de la sécurité informatique purement technique. Les concepts «Defense-In-Depth» prennent également en compte, par exemple, la sécurité physique, la gestion de la continuité des activités, les processus, les personnes et les prestataires de services externes.
Zone démilitarisée (DMZ)	Par zone démilitarisée, on entend un sous-réseau séparé logiquement et / ou physiquement avec des possibilités d'accès aux systèmes qui y sont connectés, contrôlées du point de vue de la sécurité.
Contrat de service (SLA)	L'abréviation «SLA» signifie «Service Level Agreement». Il s'agit d'une prestation convenue par contrat, que le prestataire de services informatiques s'est engagé à remplir. En règle générale, les SLA définissent les temps d'arrêt et de réaction maximum autorisés.



Terme	Description
Facility management	Voir Gestion technique du bâtiment
Bus de terrain	Un bus de terrain est un élément de réseau qui relie plusieurs appareils dans un environnement OT. Par définition, les appareils de bus de terrain sont compatibles avec le temps réel. Typiquement, dans une installation, des appareils de terrain tels que des capteurs et des actionneurs sont reliés à un appareil d'automatisation pour communiquer.
Bus de terrain	Un bus de terrain est un élément de réseau qui relie plusieurs appareils dans un environnement OT. Par définition, les appareils de bus de terrain sont compatibles avec le temps réel. Typiquement, dans une installation, des appareils de terrain tels que des capteurs et des actionneurs sont reliés à un appareil d'automatisation pour communiquer.
Appareil de terrain	Un appareil de terrain est un dispositif technique dans le domaine de la technique d'automatisation qui est en relation directe avec un processus de production. «Terrain» désigne, dans la technique d'automatisation, la zone située en dehors des armoires électriques ou des salles de contrôle.
Technique de contrôle de terrain	Commande «sur place» et surveillance «sur place» des différents panneaux de commande
Tête de commande à distance	Le concentrateur de données est utilisé comme appareil de télégestion pour l'automatisation de la station locale et pour la saisie des données des compteurs.
Technique de téléconduite	La téléopération (ou opération à distance) indique le contrôle d'un système ou d'une machine à distance. Son sens est similaire à celui de « télécommande », mais on le rencontre généralement dans les domaines de la recherche scientifique des technologies (Source Wikipedia)
Dispositifs de terrain	Voir appareil de terrain
Bus de terrain	Voir bus de terrain
Pare-feu	Un pare-feu (mieux connu sous le nom de passerelle de sécurité) est un système de composants logiciels et matériels permettant de coupler des réseaux IP de manière sécurisée. (Source BSI)
Frontend	Voir tête de télécommande
Passerelle (gateway)	En informatique, le mot passerelle désigne un composant (matériel et/ou logiciel) qui établit une connexion entre deux systèmes. (Source Wikipedia)
Gestion technique du bâtiment	La gestion technique des bâtiments désigne l'administration et la gestion des bâtiments ainsi que de leurs installations et équipements techniques.
Pirate informatique (hacker)	Spécialiste qui dispose d'une énorme connaissance des ordinateurs et des réseaux et qui identifie et exploite les erreurs existantes. Contrairement aux crackers, les hackers n'ont pas d'intentions illégales.
Durcissement	En informatique, le durcissement consiste à augmenter la sécurité d'un système en n'utilisant que des logiciels dédiés, nécessaires au fonctionnement du système et dont le bon déroulement peut être garanti du point de vue de la sécurité. Le système doit ainsi être mieux protégé contre les attaques externes. (Source Wikipedia)
Domotique	Voir Gestion technique du bâtiment
Maison des politiques	La Maison des politiques (House of Policy), dans le contexte d'un système de gestion de la sécurité de l'information (ISMS), décrit la structure et les processus des directives relatives à la sécurité de l'information.
Maison des processus	La Maison des processus (House of Processes) est un modèle de représentation de la gestion des processus qui intègre différents aspects tels que les intrants, les processus, les extrants et les besoins des clients dans un diagramme maison. Il permet de mieux comprendre et d'optimiser les processus.
Human Maschine Interface (HMI)	L'interface utilisateur est également appelée «interface homme-machine» (IHM) ou, en anglais, «Human Machine Interface» (HMI) ou «Man Machine Interface» (MMI) et permet à l'opérateur, dans certaines circonstances, d'observer les états de l'installation et d'intervenir dans le processus, au-delà de la commande de la machine.



Terme	Description
Systèmes de contrôle industriels (ICS)	Les systèmes de contrôle industriels ou «Industrial Control Systems» en anglais, sont utilisés dans l'industrie ainsi que dans le domaine des infrastructures critiques pour des fonctionnalités de contrôle, de mesure et de régulation.
Messagerie instantanée	Programme permettant d'échanger de courts messages texte en temps réel.
Dispositif électronique intelligent (IED)	Un dispositif électronique intelligent ou «Intelligent Electronic Device» en anglais est un terme utilisé dans l'industrie électrique pour décrire les commandes à microprocesseur des systèmes d'alimentation électrique, tels que les disjoncteurs, les transformateurs et les bancs de condensateurs.
Information Communications Technology (ICT)	Voir Techniques d'information et de communication
Système de gestion de la sécurité de l'information (ISMS)	Le système de gestion de la sécurité de l'information ou «Information Security Management» en anglais, est un ensemble de procédures et de règles au sein d'une entreprise, qui servent à définir, gérer, contrôler, maintenir et améliorer en permanence la sécurité de l'information.
Stratégie de sécurité de l'information (SSI)	La stratégie de sécurité de l'information est une planification de haut niveau qui définit l'orientation et les objectifs à long terme pour la protection des informations au sein d'une organisation. Elle définit le cadre des mesures et des initiatives de sécurité.
Politique de sécurité de l'information (PSI)	La politique de sécurité de l'information est une directive globale qui définit les principes et les procédures visant à protéger la confidentialité, l'intégrité et la disponibilité des informations au sein d'une organisation.
Technologies de l'information et de la communication (TIC)	Les technologies de l'information et de la communication sont les méthodes et les technologies qui réalisent la transmission, la réception et le traitement des informations (y compris les technologies numériques).
Intégrité	L'intégrité désigne le fait de garantir l'exactitude (l'intégrité) des données et le bon fonctionnement des systèmes. Lorsque le terme intégrité est appliqué aux données, il exprime le fait que les données sont complètes et inchangées. Dans le domaine des technologies de l'information, il est généralement utilisé de manière plus large et s'applique aux informations. Le terme «information» est alors utilisé pour désigner des données auxquelles peuvent être attribués, selon le contexte, certains attributs tels que l'auteur ou la date de création. La perte d'intégrité des informations peut donc signifier que celles-ci ont été modifiées sans autorisation, que les données relatives à l'auteur ont été falsifiées ou que les données temporelles de création ont été manipulées. (Source: BSI)
Système de détection d'intrusion (IDS)	Un système de détection d'intrusion ou «Intrusion Detection System» en anglais, est un système de détection automatisée des attaques sur les réseaux informatiques.
Système de prévention des intrusions (IPS)	Un système de prévention des intrusions ou «Intrusion Prevention System» en anglais, est en mesure de détecter les attaques sur les réseaux ou les systèmes informatiques et de prendre des mesures de défense automatiques.
Adresse IP	Adresse numérique qui identifie de manière univoque les appareils dans un réseau (par ex. internet).
IT-Security	Voir Sécurité informatique
Sécurité informatique	Par «sécurité informatique», on entend toutes les mesures organisationnelles et techniques visant à protéger la disponibilité, l'intégrité et la confidentialité des informations. La technologie informatique (IT) désigne les technologies de traitement des données qui ne sont pas directement liées à la fourniture d'électricité (par ex. gestion des données clients, centres de données).
Junk-Mail	(Pourriel) Le courrier électronique non sollicité, généralement de la publicité, est également appelé spam.
KPI	Le terme Key Performance Indicator (KPI) ou indicateur de performance clé désigne les indicateurs qui permettent de mesurer et/ou de déterminer les progrès ou le degré de réalisation par rapport à des objectifs importants ou des facteurs de réussite critiques au sein d'une organisation.



Terme	Description
Méthodes Lean	Les méthodes Lean visent à minimiser le gaspillage et à promouvoir l'amélioration continue. Les principes clés comprennent la création de valeur, le principe «pull», le flux continu, la standardisation, la méthode 5S, le Kanban et les systèmes de contrôle visuel. L'objectif est de créer des processus efficaces et de haute qualité.
Legacy System	En informatique, le terme «Legacy System» désigne une application établie, qui s'est développée au fil du temps dans le domaine des logiciels d'entreprise.
Contrôle-commande	Le contrôle-commande regroupe les flux de données des niveaux inférieurs, du champ ou des cellules individuelles, comme par exemple les signaux de la technique de mesure, de commande et de régulation, afin de commander et de surveiller ainsi l'ensemble du processus de fabrication.
Réseau local (LAN)	Le réseau local ou «local area network» en anglais, est un réseau informatique qui relie des ordinateurs et des appareils intelligents dans une zone géographique limitée (généralement moins de 10 km).
Logiciels malveillants	Également appelés maliciels. Terme générique désignant les programmes malveillants et nuisibles, tels que les virus, les vers ou les chevaux de Troie.
Man-Machine Interface (MMI)	Voir Interface homme-machine
Media Access Control Address (MAC Address)	Media Access Control Address est l'adresse matérielle unique d'un adaptateur réseau. Elle est gravée de manière immuable par le fabricant dans la mémoire ROM d'un adaptateur. Les entrées sont attribuées une seule fois dans le monde entier.
Interface homme-machine (IHM)	Voir Human Maschine Interface
Multiprotocol Label Switching - Transport Profile (MPLS-TP)	Le MPLS-TP a été spécialement optimisé pour les réseaux centraux (ou métropolitains), d'agrégation et d'accès. L'objectif est de fournir des fonctionnalités comparables à celles des technologies basées sur le TDM (Time Division Multiplexing) et de prendre en charge les connexions point à point et any to any avec un niveau de prévisibilité, de fiabilité et de fonctionnalités OAM (Operations, Administration and Management) similaire à celui des réseaux TDM qui ont fait leurs preuves depuis longtemps.
Multiprotocol Label Switching (MPLS)	Le MPLS permet la transmission orientée connexion de paquets de données dans un réseau sans connexion le long d'un chemin préalablement établi («signalisé»). Ce procédé de commutation est principalement utilisé par les exploitants de grands réseaux de transport qui proposent des services vocaux et de données sur la base de l'IP. (Source Wikipedia)
Network access control (NAC)	Network access control ou contrôle d'accès au réseau est une technique utilisée pour se protéger contre les accès non autorisés au réseau.
Network Address Translation (NAT)	Network Address Translation désigne une procédure de remplacement automatique et transparent des informations d'adresse dans les paquets de données. Les procédures NAT sont généralement utilisées sur les routeurs et les passerelles de sécurité, principalement pour utiliser le plus efficacement possible l'espace d'adressage IPv4 limité et pour masquer les adresses IP locales par rapport aux réseaux publics. (Source BSI)
Technique de gestion du réseau	Comprend les techniques de mesure, de commande et de régulation des réseaux, comme par exemple les réseaux électriques. La technique de contrôle des réseaux est une spécialité de la technique de contrôle des processus; elle fait partie des sciences appliquées de l'ingénieur.
Fonctionnement normal	Etat de l'installation dans les limites d'exploitation spécifiques et selon les prescriptions en vigueur (source IFSN)
OEM	Original Equipment Manufacturer, que l'on peut traduire par «fabricant d'équipement d'origine». On entend par là un fabricant de composants ou de produits qui les produit dans ses propres usines, mais qui ne les met pas lui-même en vente au détail. Les logiciels OEM peuvent se distinguer de la version dite complète (retail) par un volume de livraison moins important ou des fonctionnalités limitées.
Office IT	Le terme fait référence aux technologies informatiques utilisées dans les environnements de bureau pour soutenir le travail de bureau. Cela comprend



Terme	Description
	typiquement les applications logicielles, les réseaux, le matériel informatique et l'infrastructure informatique pour les tâches de bureau.
Sécurité OT	Par «sécurité OT», on entend toutes les mesures organisationnelles et techniques visant à protéger la disponibilité, l'intégrité et la confidentialité des informations pour la surveillance et la commande des installations de distribution (et de production) d'électricité ainsi que la protection des personnes et des installations. La technologie opérationnelle (Operational Technology, OT) désigne ici les technologies directement nécessaires à la mise à disposition ou à la fourniture d'électricité (p. ex. SCADA, PIA, accès à distance aux installations dans les sous-stations, télécommande centralisée, compteurs intelligents).
Patch	Mise à jour des programmes dans lesquels des erreurs ont été détectées. Voir aussi «Mise à jour».
Test de pénétration	Par «test de pénétration», on entend un test de sécurité complet de systèmes ou de réseaux individuels. Il s'agit de vérifier la mise en œuvre technique des mesures de cybersécurité. Les tests de pénétration font partie intégrante d'un audit de sécurité.
Cycle PDCA	Le cycle PDCA est un processus d'amélioration continue, composé de la planification, de la mise en œuvre, de la vérification et de l'adaptation, qui sert à rendre les processus plus efficaces et à améliorer continuellement la qualité.
PGP	(Pretty Good Privacy, en français: «assez bonne vie privée») Programme de cryptage des données.
Pharming	Attaque de phishing avancée qui manipule l'ordinateur de la victime de manière à ce que l'attaque ne soit détectable que par des spécialistes professionnels de la sécurité ou des réseaux. Compte tenu de cette méthode d'attaque, l'utilisation d'un antivirus, d'un pare-feu et l'application quotidienne de correctifs sur l'ordinateur sont fortement recommandées.
Phishing	Le phishing ou hameçonnage est une méthode d'attaque visant à inciter une victime à transmettre à un pirate des données de connexion à des services financiers (p. ex. eBanking); soit par e-mail, soit par la visite d'un site internet déguisé en original.
Port	Indication numérique qui rend un service adressable sur un ordinateur. Elle permet de distinguer clairement les différents paquets de données sur le réseau.
Technique primaire	Outre les transformateurs nécessaires à la transformation, la sous-station comprend également des installations de commutation pour les lignes partant en haute et en basse tension. Les installations techniques (transformateurs, jeux de barres, etc.) ainsi que les lignes sont généralement redondantes, de sorte qu'en cas de défaillance d'un équipement, l'alimentation continue d'être garantie.
Contrôle logique programmable (PLC)	Voir Automate programmable
Fournisseur	Fournisseur d'accès à des réseaux (par ex. internet). Les fournisseurs d'accès connus sont Bluewin, Sunrise ou Cablecom.
Système de couplage de processus	Le système de couplage de processus représente l'élément de liaison entre le niveau de processus et le niveau de contrôle.
Technique de contrôle des processus	La technique de contrôle des processus désigne les moyens et les procédés qui servent à la commande, à la régulation et à la sécurité des installations techniques de processus. Le système de contrôle des processus et l'automate programmable en sont les moyens centraux.
Modèle RASCI	Le modèle RASCI est un modèle de responsabilité qui définit les rôles et les responsabilités dans un projet ou un processus. Il attribue les lettres R, A, S, C et I aux termes «Responsible» (responsable), «Accountable» (responsable), «Support» (soutien), «Consulted» (consulté) et «Informed» (informé).
Accès à distance	Accès distant à un réseau ou à un ordinateur, généralement via internet. De tels accès ne devraient être possibles qu'à l'aide de technologies de sécurité telles que les pare-feu et les VPN.
Unité de terminal à distance (RTU)	Le Remote Terminal Unit (RTU) est un instrument de régulation ou de commande à distance.



Terme	Description
Résilience	La résilience désigne la capacité d'un système à se rétablir après des perturbations, à s'adapter et à en ressortir plus fort.
Risque	Le risque est la prévision, souvent basée sur des calculs, d'un dommage possible dans le cas négatif (danger) ou d'un bénéfice possible dans le cas positif (chance). Ce qui est considéré comme un dommage ou un bénéfice dépend des valeurs. Le risque est également souvent défini comme la combinaison de la probabilité qu'un dommage se produise et de l'ampleur de ce dommage. (Source BSI)
Routeur	Appareil qui relie les réseaux entre eux. Également connu sous le nom de routeur ADSL.
Sandbox	Une sandbox est une zone isolée au sein d'une application ou d'un système d'exploitation. Elle empêche l'exécution d'actions indésirables en dehors de l'environnement contrôlé. Les dangers et les effets des programmes malveillants sont ainsi repoussés. (Source BSI)
SCADA (Supervisory Control and Data Acquisition)	Par Supervisory Control and Data Acquisition, on entend la surveillance et la commande de processus techniques au moyen d'un système informatique. Synonyme: système ICS (Industrial Control System)
Maliciel	Voir Malware
Objet protégé	Les objets à protéger sont les infrastructures, les services, les systèmes, les applications, les réseaux, les collections de données, etc. qui doivent être utilisés pour remplir la mission de l'entreprise et qui doivent donc être protégés.
Systèmes de protection	Système de sécurité composé de capteurs, de logique et d'éléments de commande permettant de ramener un processus à un état sûr lorsque des conditions prédéfinies ont été violées.
Objectif de protection	Les objectifs de protection décrivent des objets protégés qui sont protégés par les mesures correspondantes.
Technique secondaire	La notion de technique secondaire englobe les équipements d'une sous-station qui ne participent pas directement à la transformation de la tension. On entend par là, par exemple, la commande locale, la régulation de la tension, la protection du réseau, le comptage de l'énergie, la télécommande, etc.
Serveur	Ordinateur qui met des services à la disposition d'autres ordinateurs (clients) dans un réseau. (par ex. serveur de messagerie)
Audit de sécurité	Par «audit de sécurité», on entend un examen complet des mesures de cybersécurité organisationnelles et techniques. Il s'agit d'analyser les points faibles de la cybersécurité dans le domaine de la conception/architecture, de la mise en œuvre, de l'exploitation, des erreurs humaines et de la sécurité du site, ainsi que la sécurité des différents composants du système.
Culture de la sécurité	La culture de la sécurité comprend les valeurs, les visions du monde, les comportements verbaux et non verbaux ainsi que les caractéristiques de l'environnement physique créé par l'homme, partagés par les membres de l'organisation de l'exploitant d'une installation nucléaire. La culture de la sécurité comprend les valeurs, les visions du monde, les comportements et les caractéristiques de l'environnement qui déterminent ou montrent comment les membres de l'organisation gèrent la sécurité nucléaire (source IFSN).
Signature (numérique)	Signature numérique à caractère obligatoire.
Six Sigma	Six Sigma est une méthode de gestion de la qualité visant à améliorer les processus, à réduire les erreurs et à augmenter l'efficacité, basée sur des analyses statistiques. L'objectif est de minimiser les écarts dans les processus et de parvenir à une standardisation élevée de la qualité.
Security Information and Event Management (SIEM)	Les systèmes SIEM sont utilisés pour identifier et évaluer les événements liés à la sécurité et alerter l'administrateur en conséquence.
Smart metering	Systèmes de mesure intelligents capables de transmettre leurs données de mesure et d'assumer des tâches de contrôle via une communication bidirectionnelle.
Smart Card	Carte en plastique dotée d'une puce pouvant stocker des données qui peuvent être libérées par la saisie d'un code (PIN).



Terme	Description
Spam	E-mails non sollicités envoyés en masse sous forme de chaînes de lettres ou de publicité pour des produits ou services douteux ou spéciaux. Le filtre anti-spam permet de s'en protéger et de filtrer une grande partie du courrier indésirable du courrier régulier.
Commande (API)	Un automate programmable industriel est un appareil utilisé pour commander ou réguler une machine ou une installation et qui est programmé sur une base numérique. (Source Wikipedia)
Spyware	Type de logiciel malveillant utilisé pour espionner les utilisateurs d'ordinateurs et observer leur comportement, notamment sur internet, voir même lire ce qu'ils tapent sur le clavier (vol de mot de passe). Pour s'en protéger, il convient d'utiliser régulièrement un scanner de logiciels espions.
Stakeholder	Les stakeholder ou parties prenantes sont des personnes ou des groupes qui sont concernés par les activités d'une organisation ou qui ont une influence sur celles-ci.
Bus de station	Système de bus dans une sous-station (SS) entre le centre de contrôle de SS et les capteurs dans le champ électrique.
Technique de contrôle des stations	Commande globale dans une sous-station composée d'un poste de commande, de capteurs et d'actions. Est le lien entre le processus et le niveau de gestion du réseau.
OApEI	En Suisse, l'Ordonnance sur l'approvisionnement en électricité (OApEI) règle les conditions-cadres pour l'accès au réseau électrique et la facturation des rétributions pour l'utilisation du réseau.
Compteur d'électricité	Compteur électrique pour la mesure du travail électrique (sommation de la puissance active).
Switch	Appareil qui relie des ordinateurs ou des réseaux entre eux. Est utilisé dans les réseaux locaux (LAN).
Threat Intelligence	La Threat Intelligence désigne la collecte, l'analyse et la compréhension d'informations sur les cybermenaces afin de réagir de manière proactive aux risques de sécurité et d'améliorer les mesures de protection.
Total Quality Management (TQM)	Le Total Quality Management (TQM) est une méthode globale de gestion de la qualité qui vise à intégrer la qualité dans tous les processus de l'entreprise et à l'améliorer en permanence.
Cheval de Troie	Programme malveillant dangereux qui est généralement enregistré et exécuté sur son propre ordinateur sans être détecté et sans autorisation. Il se signale généralement à un attaquant (cracker) et permet le contrôle total de l'ordinateur par l'attaquant. Un antivirus devrait être utilisé comme protection minimale.
Tunneling	Dans un réseau, le tunnelling désigne la conversion et la transmission d'un protocole de communication qui est intégré dans un autre protocole de communication pour le transport.
Update	Routine de mise à jour qui répare les programmes défectueux (par ex.: systèmes d'exploitation). Voir aussi «Patch».
URL	Adresse d'un site sur internet, p. ex. www.electricite.ch
Clé USB	Support de stockage connecté au port USB de l'ordinateur. Utilisé également par les voleurs de données en raison de ses petites dimensions et de sa grande capacité de stockage.
ASI	Signifie «alimentation sans interruption». Appareil placé entre l'alimentation électrique et le consommateur, qui sert de batterie d'appoint pour le consommateur en cas de panne de courant et de filtre pour protéger le consommateur des variations de tension.
Utility	Entreprise d'approvisionnement en énergie
Disponibilité	La disponibilité de services, de fonctions d'un système informatique, d'applications informatiques ou de réseaux informatiques ou encore d'informations est assurée lorsque les utilisateurs peuvent toujours les utiliser comme prévu. (Source BSI)



Terme	Description
Cryptage	Le cryptage (ou chiffrement) est la transformation, à l'aide d'une clé, de données appelées «texte clair» en un «texte secret» (ou «cryptogramme»), de sorte que le texte clair ne peut être récupéré à partir du texte secret qu'en utilisant une clé secrète.
Confidentialité	La confidentialité est la protection contre la divulgation non autorisée d'informations. Les données et informations confidentielles ne doivent être accessibles qu'aux personnes autorisées et de la manière autorisée. (Source BSI)
Scanneur de virus	Programme permettant de détecter et de supprimer les virus informatiques et autres parasites informatiques. Voir aussi «Anti-virus» et «Malware».
Réseaux locaux virtuels (VLAN)	Les réseaux locaux virtuels sont utilisés pour la structuration logique des réseaux. Ils permettent de reproduire une structure de réseau logique à l'intérieur d'un réseau physique en reliant des postes de travail et des serveurs fonctionnellement associés pour former un réseau virtuel.
Réseau privé virtuel (VPN)	Virtual Private Network est un réseau de communication privé virtuel (fermé sur lui-même) qui utilise un réseau de communication existant comme moyen de transport.
Virus	Programme généralement nuisible (malware) qui détruit les données ou empêche l'utilisation de l'ordinateur. Peut se propager par toute forme de transmission de données (Internet, disquette, CD-ROM, clé USB, e-mail, etc.) et exige une action de l'utilisateur pour être activé. Pour se protéger, il convient d'utiliser un antivirus, de l'actualiser et de l'activer régulièrement.
VPN	(Virtual Private Network) Technologie qui, grâce à l'utilisation du cryptage et des contrôles d'accès (login), permet l'utilisation sécurisée de réseaux publics (par ex. internet) à des fins privées.
Wide Area Network (WAN)	Wide Area Network est un réseau d'ordinateurs qui, à la différence d'un LAN, s'étend sur une très grande zone géographique.
Worm / ver informatique	Programme nuisible (malware) qui se propage sur les réseaux sans l'intervention de tiers et en exploitant des points faibles ou des programmes défectueux, bloquant temporairement ces réseaux et les ordinateurs qui y sont connectés. Souvent, les vers contiennent également des commandes qui détruisent les données. Un antivirus devrait être utilisé comme protection minimale.
Compteur	Voir compteur électrique
Zombie	Ordinateur sous le contrôle d'un tiers (par exemple un cracker) qui héberge un cheval de Troie et qui est généralement utilisé pour attaquer d'autres ordinateurs sur internet.



Anhang B: Liste des abréviations

Abréviation	Description
DE-OCF	Dispositions d'exécution de l'ordonnance sur les chemins de fer
OFPP	Office fédéral de la protection de la population
OFCS	Office fédéral de la cybersécurité
BDEW	Association fédérale de l'industrie de l'énergie et de l'eau (Allemagne)
OFEN	Office fédéral de l'énergie
BSI	Office fédéral de la sécurité des technologies de l'information (Allemagne)
OFAE	Office fédéral pour l'approvisionnement économique du pays
CERT	Équipe d'intervention en cas d'urgence informatique
CIRT	Équipe de réponse aux incidents cybernétiques
CISO	Chief Information Security Officers (responsables de la sécurité de l'information)
CPSO	Chief Physical Safety Officer (responsable de la sécurité physique)
CRO	Chief Risk Officer (responsable des risques)
CSIRT	Computer Security Incident Response Team (équipe de réponse aux incidents de sécurité informatique)
CSSE	Certified SCADA Security Engineer (ingénieur certifié en sécurité SCADA)
DMZ	Demilitarized Zone (zone démilitarisée)
DPO	Data Protection Officer (responsable de la protection des données ou responsable de la conformité et de la protection des données)
PFPDT	Préposé fédéral à la protection des données et à la transparence
EAE	Entreprise d'approvisionnement en énergie
HMI	Interface homme-machine
HoP	Maison des politiques
ICS	Industrial Control Systems (systèmes de contrôle industriels)
ICT	Information and communication technology (technologie de l'information et de la communication)
IDS	Intrusion Detection System (système de détection des intrusions)
IEC	International Electrotechnical Commission (commission électrotechnique internationale)
IED	Intelligent Electronic Device (dispositif électronique intelligent)
TIC	Techniques d'information et de communication
IPS	Intrusion Prevention System (système de prévention des intrusions)
SGI	Système de gestion intégré
IR	Incident Response (réponse aux incidents)
RSI	Responsable de la sécurité de l'information
ISC	Information Security Coordinator (coordinateur de la sécurité de l'information)
ISP	Politique de sécurité de l'information
ISMS	Système de gestion de la sécurité de l'information
ISO	Organisation internationale de normalisation
ISO	Responsable de la sécurité de l'information
SSI	Stratégie de sécurité de l'information
IT	Technologie de l'information
KVM	Clavier, vidéo et souris



Abréviation	Description
LAN	Local Area Network (réseau local)
Adresse MAC	Media Access Control Address (adresse de contrôle d'accès au média)
MMI	Interface homme-machine
MMS	Interface homme-machine
MPLS	Multiprotokoll Label Switching
MPLS-TP	Multiprotokoll Label Switching - Transport Profile
NAC	Network Access Control (contrôle d'accès au réseau)
NAT	Network Address Translation (traduction d'adresses réseau)
NIST	National Institute of Standards and Technology (États-Unis)
OT	Technologie opérationnelle
PDH	Hiérarchie numérique plésiochrone
PIA	Partner Informations Austausch
PLC	Contrôle logique programmable
RTU	Unité de terminal à distance
SCADA	Supervisory Control And Data Acquisition
SDH	Synchronous Digital Hierarchy
SIEM	Security information and event management
SLA	Service Level Agreement, accord de niveau de service
SN	Normes suisses
SOC	Security Operations Center
API	Automate programmable industriel
UFLS	Délestage en fonction de la sous-fréquence
VLAN	LAN virtuel
VPN	Virtual Private Network
AES	Association des entreprises électriques suisses
WAN	Wide Area Network



Anhang C: Bases légales: lois et règlements obligatoires

- (1) Le résumé suivant donne une vue d'ensemble des bases légales en vigueur sous forme d'articles de loi et d'ordonnance qui doivent être appliqués en relation avec l'augmentation de la résilience TIC chez les fournisseurs d'énergie dans le domaine de l'électricité:

C.0 Niveau national

Code des obligations (RS 220)

Art.	Article / détails
754	<p>¹ Les membres du conseil d'administration et toutes les personnes qui s'occupent de la gestion ou de la liquidation répondent à l'égard de la société, de même qu'envers chaque actionnaire ou créancier social, du dommage qu'ils leur causent en manquant intentionnellement ou par négligence à leurs devoirs.</p> <p>² Celui qui d'une manière licite, délègue à un autre organe l'exercice d'une attribution, répond du dommage causé par ce dernier, à moins qu'il ne prouve avoir pris en matière de choix, d'instruction et de surveillance, tous les soins commandés par les circonstances.</p>

Constitution fédérale de la Confédération suisse (Cst.; RS 101)

Art.	Article / détails
102	<p>Approvisionnement du pays*</p> <p>¹ La Confédération assure l'approvisionnement du pays en biens et services de première nécessité afin de pouvoir faire face à une menace de guerre, à une autre manifestation de force ou à une grave pénurie à laquelle l'économie n'est pas en mesure de remédier par ses propres moyens. Elle prend des mesures préventives.</p> <p>² Elle peut, au besoin, déroger au principe de la liberté économique.</p>

Loi fédérale sur l'approvisionnement économique du pays (loi sur l'approvisionnement du pays LAP; RS 531)

Art.	Article / détails
4	<p>Biens et services vitaux</p> <p>¹ Sont vitaux les biens et services qui sont nécessaires, directement ou dans le cadre des processus économiques, pour faire face à une pénurie grave.</p> <p>² Sont des biens vitaux, notamment:</p> <ol style="list-style-type: none">les agents énergétiques ainsi que les moyens de production et le matériel nécessaires à leur exploitation;les denrées alimentaires, les fourrages et les produits thérapeutiques, ainsi que les semences et les plants;les autres biens d'usage quotidien qui sont indispensables;les matières premières ou auxiliaires destinées à l'agriculture, à l'industrie ou à l'artisanat. <p>³ Sont des services vitaux, notamment:</p> <ol style="list-style-type: none">les transports et la logistique;l'information et la communication;le transport et la distribution d'agents énergétiques et d'énergie;la garantie du trafic des paiements;le stockage de biens et d'énergie. <p>⁴ Le matériel et les ressources requis par les services vitaux sont également considérés comme des services vitaux.</p>
31	<p>Mesures applicables aux biens vitaux</p> <p>¹ En cas de pénurie grave, déclarée ou imminente, le Conseil fédéral peut prendre des mesures d'intervention économique temporaires pour garantir l'approvisionnement en biens vitaux.</p> <p>² Il peut réglementer à cet effet:</p> <ol style="list-style-type: none">les achats, l'attribution, l'utilisation et la consommation;la restriction de l'offre;la transformation et l'adaptation de la production;l'utilisation, la récupération et le recyclage des matières premières;l'accroissement des réserves;la libération des réserves obligatoires et autres réserves;l'obligation de livrer;la promotion des importations;la restriction des exportations.



Art.	Article / détails
	³ En cas de besoin, le Conseil fédéral peut passer des actes juridiques aux frais de la Confédération.
32	<p>Mesures applicables aux services vitaux</p> <p>¹ En cas de pénurie grave, déclarée ou imminente, le Conseil fédéral peut prendre des mesures d'intervention économique temporaires pour garantir l'approvisionnement en services vitaux.</p> <p>² Il peut réglementer à cet effet:</p> <ul style="list-style-type: none"> a. la sauvegarde, l'exploitation, l'utilisation et l'affectation des moyens de transport ainsi que des infrastructures requises par les entreprises opérant dans l'approvisionnement en énergie, l'information, les communications, la logistique des transports; b. le développement, la restriction ou l'interdiction de certains services; c. l'obligation de fournir des services. <p>³ En cas de besoin, le Conseil fédéral peut passer des actes juridiques aux frais de la Confédération.</p>

Ordonnance sur l'approvisionnement économique du pays (OAEP; RS 531.11)

Art.	Article / détails
7	<p>Tâches des domaines</p> <p>¹ Les domaines ont les compétences suivantes:</p> <ul style="list-style-type: none"> a. apporter et exploiter le savoir-faire et l'expérience du secteur privé ainsi que le réseau relationnel des milieux économiques pour en faire bénéficier l'approvisionnement économique du pays; b. assurer un transfert de connaissances; c. évaluer périodiquement la situation; d. préparer et exécuter des prescriptions et des mesures décidées par l'approvisionnement économique du pays. e. <p>² Ils observent et analysent régulièrement l'évolution de l'approvisionnement économique du pays.</p> <p>³ Les domaines ci-après ont les compétences suivantes:</p> <ul style="list-style-type: none"> a. alimentation: aliments et moyens de production agricoles; b. énergie: combustibles et carburants fossiles, électricité, bois de chauffage et eau potable; c. produits thérapeutiques: produits thérapeutiques destinés aux personnes et aux animaux; d. logistique: transports par voies terrestre, fluviale/maritime et aérienne ainsi que circuits logistiques; e. industrie: matières auxiliaires, notamment les matériaux d'emballage; f. technologies de l'information et de la communication: transfert, sécurité et disponibilité des données.
11	<p>Préparatifs incombant aux domaines</p> <p>¹ Les domaines préparent des mesures pour intervenir dans la distribution, la consommation, l'utilisation et la production de biens vitaux ainsi que dans la fourniture de services vitaux; ils veillent à atteindre le degré de préparation requis. Ils coordonnent leurs activités avec les entités fédérales énumérées à l'art. 8, al. 1, qui assument des tâches d'approvisionnement.</p> <p>² Ils veillent à disposer des ressources et de la main-d'œuvre nécessaires pour remplir leurs tâches.</p> <p>³ Ils peuvent défendre leurs intérêts au sein de certaines organisations internationales.</p>

Ordonnance sur l'organisation chargée d'assurer l'approvisionnement économique du pays dans le domaine de l'électricité (OOSE; RS 531.35)

Art.	Article / détails
1	<p>Tâches incombant à l'AES</p> <p>¹ L'Association des entreprises électriques suisses (AES) fait les préparatifs requis dans les secteurs production, achats, transports, distribution et consommation d'électricité pour affronter une pénurie grave.</p> <p>² Elle tient compte des particularités régionales et techniques, notamment des tâches et fonctions de la société nationale du réseau de transport et de la Commission fédérale de l'électricité (EICom).</p> <p>³ Elle coordonne les tâches de ses membres.</p> <p>⁴ Si l'AES crée une organisation particulière pour garantir l'approvisionnement du pays en électricité, les entreprises qui ne sont pas membres de l'AES peuvent se subordonner volontairement à cette organisation.</p>
1a	<p>Système de monitoring: exploitation et accès</p> <p>¹ La société nationale du réseau de transport exploite un système de monitoring visant à suivre la situation en matière d'approvisionnement dans le secteur de l'électricité.</p> <p>² Elle donne au domaine Énergie l'accès au système de monitoring par procédure d'appel et rend périodiquement compte de l'évolution de la situation en matière d'approvisionnement.</p>
1b	Système de monitoring: traitement des données



Art.	Article / détails
	<p>¹ Le système de monitoring recense notamment des données relatives à la production et à la consommation d'énergie électrique ainsi qu'aux capacités d'importation, d'exportation et d'auto-approvisionnement de la Suisse.</p> <p>² Les données sont mises à la disposition du domaine Énergie pendant vingt ans à partir de la date de leur saisie.</p> <p>³ La société nationale du réseau de transport prend des mesures organisationnelles et techniques afin de garantir une journalisation automatique du traitement des données et d'empêcher tout traitement illicite des données. Elle définit les mesures dans un règlement sur le traitement des données.</p> <p>⁴ La transmission des données n'est pas autorisée. Est réservée la transmission de données par le domaine Énergie à l'EiCom, à l'Office fédéral de l'énergie, à d'autres autorités fédérales ou cantonales ainsi qu'à l'AES ou à son organisation pour garantir l'approvisionnement du pays en électricité (art. 1, al. 4), lorsque ces données sont nécessaires à l'exercice de leur mandat légal.</p> <p>⁵ Les destinataires des données prennent des mesures organisationnelles et techniques permettant d'assurer que l'utilisation des données se limite au but indiqué.</p> <p>⁶ La société nationale du réseau de transport, le domaine Énergie et l'AES sont tenus de garder le secret (art. 63 LAP) sur le suivi de la situation en matière d'approvisionnement en électricité et sur les informations qui y sont liées. Ils ne peuvent utiliser les données provenant du système de monitoring que pour servir les intérêts de l'approvisionnement économique du pays.</p>
2	<p>Tâches incombant au domaine Énergie</p> <p>¹ Le domaine Énergie fixe le type et l'étendue des préparatifs et définit les exigences applicables au système de monitoring.</p> <p>² Il supervise les préparatifs de l'AES et l'exploitation du système de monitoring et est habilité à donner des directives à l'AES et à la société nationale du réseau de transport en la matière.</p>

Loi sur l'énergie (LEne; RS 730.0)

Art.	Article / détails
7	<p>¹ Un approvisionnement énergétique sûr implique une disponibilité énergétique suffisante en tout temps, une offre d'énergie diversifiée et des systèmes d'approvisionnement et de stockage techniquement sûrs et efficaces. Il implique également la protection des infrastructures critiques, y compris celle des techniques d'information et de communication qui y sont liées.</p>

Loi sur les installations électriques (LIE; RS 734.0)

Art.	Article / détails
15d	<p>¹ L'approvisionnement en énergie électrique revêt un intérêt national.</p>

Loi fédérale sur l'approvisionnement en électricité (LApEI; RS 734.7)

Art.	Article / détails
6	<p>Obligation de fourniture et tarification pour consommateurs captifs</p> <p>¹ Les gestionnaires d'un réseau de distribution prennent les mesures requises pour pouvoir fournir en tout temps aux consommateurs captifs et aux autres consommateurs finaux de leur zone de desserte qui ne font pas usage de leur droit d'accès au réseau la quantité d'électricité qu'ils désirent au niveau de qualité requis et à des tarifs équitables.</p>

Ordonnance sur l'approvisionnement en électricité (OApEI; RS 734.71)

Art.	Article / détails
5	<p>⁶ L'Office fédéral de l'énergie (OFEN) peut fixer des exigences techniques et administratives minimales concernant un réseau sûr, performant et efficace; il peut déclarer obligatoires des dispositions internationales techniques ou administratives et des normes ou des recommandations édictées par des organisations techniques reconnues.</p>
5a	<p>¹ Afin d'assurer une protection adéquate des installations contre les cybermenaces, notamment en protégeant les technologies de l'information et de la communication (TIC), les recommandations de la norme minimale pour améliorer la résilience informatique de mai 2023 (norme minimale TIC) sont contraignantes conformément au niveau de protection applicable selon l'annexe 1a pour:</p> <ul style="list-style-type: none"> a. les gestionnaires de réseau; b. les producteurs, à l'exception des exploitants de centrales nucléaires, et les exploitants de stockage s'ils exploitent des installations d'une puissance totale d'au moins 100 MW et qu'ils peuvent les piloter via un seul système; c. les prestataires qui peuvent durablement piloter:



Art.	Article / détails
	<ol style="list-style-type: none"> des installations de gestionnaires de réseau, ou des installations de producteurs, à l'exception des exploitants de centrales nucléaires, ou d'exploitants de stockage s'ils ont de ce fait accès via un seul système à une puissance d'au moins 100 MW. <p>² Les standards reconnus internationalement cités dans la norme minimale TIC ne sont pas contraignants.</p> <p>³ La preuve que le niveau de protection requis est atteint doit être fournie à l'EICOM à sa demande.</p>

Loi fédérale sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, LSI; RS 128)

Art.	Article / détails
5	<p>Définitions</p> <p>On entend par:</p> <p>c. infrastructure critique: l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports ainsi que d'autres installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population.</p>
74	<p>Tâches de la Confédération</p> <p>¹ La Confédération apporte un soutien aux exploitants d'infrastructures critiques pour garantir que les interruptions de réseau et de système et que les utilisations abusives soient rares, de courte durée, maîtrisables et peu dommageables.</p> <p>² Le soutien apporté par la Confédération en matière de sécurité de l'information prend les formes suivantes:</p> <ol style="list-style-type: none"> identification et évaluation précoces des menaces, dangers, vulnérabilités et failles de sécurité; identification des incidents; maintien et rétablissement de la sécurité de l'information après un incident; suivi des incidents. <p>³ La Confédération gère un service national d'alerte et un service d'assistance pour la mise en place de mesures techniques de sécurité à titre préventif ou après un incident.</p> <p>⁴ Elle veille à ce que les exploitants d'infrastructures critiques puissent échanger des informations en toute sécurité, entre elles et avec les services compétents de la Confédération.</p> <p>⁵ Le Conseil fédéral désigne les services fédéraux chargés d'accomplir ces tâches.</p>
76	<p>Coopération sur le plan national</p> <p>¹ Les services visés à l'art. 74, al. 5, peuvent communiquer aux exploitants d'infrastructures critiques des données personnelles au sens de l'art. 75 dans la mesure où elles sont utiles à la sécurité de l'information.</p> <p>² Ils peuvent communiquer aux fournisseurs et exploitants de services informatiques et de communication des données personnelles au sens de l'art. 75 dans la mesure où elles sont nécessaires à la sécurité de l'information d'infrastructures critiques.</p> <p>³ Les exploitants d'infrastructures critiques de même que les fournisseurs et les exploitants de services informatiques et de communication peuvent communiquer aux services visés à l'art. 74, al. 5, des données liées à des incidents, y compris des données personnelles. Les services visés à l'art. 74, al. 5, ne peuvent transmettre ces données à des fins de poursuite pénale qu'avec l'autorisation expresse du fournisseur des données.</p>
77	<p>Coopération internationale</p> <p>¹ Les services visés à l'art. 74, al. 5, peuvent échanger avec des services étrangers ou internationaux chargés de la protection d'infrastructures critiques des données au sens de l'art. 75 lorsqu'elles sont nécessaires pour accomplir des tâches correspondant à celles définies à l'art. 74.</p> <p>² L'échange de données au sens de l'al. 1 n'est autorisé que si les services étrangers ou internationaux garantissent que les données seront utilisées exclusivement aux fins prévues à l'al. 1.</p> <p>³ Si les données sont nécessaires à l'exécution d'une procédure à l'étranger, les dispositions régissant l'assistance administrative et l'entraide judiciaire sont applicables.</p>
78	<p>Système d'information pour le soutien aux infrastructures critiques</p> <p>¹ Les services visés à l'art. 74, al. 5, exploitent un système d'information permettant d'échanger en toute sécurité des informations avec les exploitants des infrastructures critiques.</p> <p>² Le système contient les informations suivantes:</p> <ol style="list-style-type: none"> description et évaluation des menaces et dangers; consignes sur l'identification et la résolution techniques des incidents; analyses des incidents et recommandations pour la sécurité; analyses des vulnérabilités que présentent les moyens informatiques; correspondance.



Art.	Article / détails
	³ Les informations visées à l'al. 2 peuvent contenir des données personnelles au sens de l'art. 75.

Loi fédérale sur la protection des données (Loi sur la protection des données, LPD; RS 235.1)

Art.	Article / détails
	Lien vers la nouvelle Loi sur la protection des données: https://www.fedlex.admin.ch/eli/cc/2022/491/fr



Les dispositions légales et les ordonnances de la Confédération et des services fédéraux sont contraignantes et doivent être impérativement respectées.

Système de contrôle interne CO 728a, 728b

La tâche de l'organe de révision est de vérifier s'il existe un système de contrôle interne et si le rapport contient des informations sur une évaluation des risques. Quelle que soit la forme de révision à laquelle une société est soumise, le conseil d'administration est tenu de fournir des informations sur la réalisation d'une évaluation des risques dans l'annexe des comptes annuels. L'organe de révision doit vérifier et confirmer formellement qu'une évaluation des risques a été effectuée. Les déclarations de contenu concernant l'évaluation des risques sont attendues exclusivement du conseil d'administration.

Art.	Article / détails
	2. Attributions de l'organe de révision a. Objet et étendue du contrôle ¹ L'organe de révision vérifie: 1. si les comptes annuels et, le cas échéant, les comptes consolidés sont conformes aux dispositions légales, aux statuts et au cadre de référence choisi; 2. si la proposition du conseil d'administration à l'assemblée générale concernant l'emploi du bénéfice est conforme aux dispositions légales et aux statuts; 3. s'il existe un système de contrôle interne; 4. lorsque les actions de la société sont cotées en bourse, si le rapport de rémunération est conforme aux dispositions légales et aux statuts. ² L'organe de révision tient compte du système de contrôle interne lors de l'exécution du contrôle et de la détermination de son étendue. ³ La manière dont le conseil d'administration dirige la société n'est pas soumise au contrôle de l'organe de révision.
	b. Rapport de révision ¹ L'organe de révision établit à l'intention du conseil d'administration un rapport détaillé contenant des constatations relatives à l'établissement des comptes, au système de contrôle interne ainsi qu'à l'exécution et au résultat du contrôle. ² L'organe de révision établit à l'intention de l'assemblée générale un rapport écrit qui résume le résultat de la révision. Ce rapport contient: 1. un avis sur le résultat du contrôle; 2. des indications attestant de l'indépendance de l'organe de révision; 3. des indications sur la personne qui a dirigé la révision et sur ses qualifications professionnelles; 4. une recommandation d'approuver, avec ou sans réserve, les comptes annuels et les comptes consolidés, ou de les refuser. ³ Les deux rapports doivent être signés par la personne qui a dirigé la révision.

Rapport de situation CO 961 et 961c

Art.	Article / détails
961	A. Exigences supplémentaires concernant le rapport de gestion



	<p>Les entreprises que la loi soumet au contrôle ordinaire ont les obligations suivantes:</p> <ol style="list-style-type: none"> 1. fournir des informations supplémentaires dans l'annexe aux comptes annuels; 2. intégrer un tableau des flux de trésorerie dans leurs comptes annuels; 3. rédiger un rapport annuel.
961c	<p>D. Rapport annuel</p> <p>¹ Le rapport annuel présente la marche des affaires et la situation économique de l'entreprise, le cas échéant de son groupe de sociétés, à la fin de l'exercice; il souligne les aspects qui n'apparaissent pas dans les comptes annuels.</p> <p>² Le rapport annuel précise en particulier les éléments suivants:</p> <ol style="list-style-type: none"> 1. la moyenne annuelle des emplois à plein temps; 2. la réalisation d'une évaluation des risques; 3. l'état des commandes et des mandats; 4. les activités de recherche et développement; 5. les événements exceptionnels; 6. les perspectives de l'entreprise. <p>³ Le rapport annuel ne doit pas être en contradiction avec la situation économique présentée dans les comptes annuels.</p>

C.1 Niveau international

La collection suivante de lois et de directives internationales est en partie obligatoire pour les entreprises et les unités organisationnelles qui n'opèrent pas uniquement au niveau national:

- **Directive (UE) 2016/1148 du Parlement européen et du Conseil** du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016, p. 1.
- **Directive (UE) 2022/2555 du Parlement européen et du Conseil** du 14 décembre 2022 concernant des mesures relatives à un niveau commun élevé de cybersécurité dans l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972 et abrogeant la directive (UE) 2016/1148 (directive NIS 2), JO L 333 du 27.12.2022, p. 80.



Les entreprises et les unités organisationnelles doivent en partie mettre en œuvre les dispositions légales et les directives internationales, surtout lorsqu'elles opèrent dans un environnement commercial international.



Anhang D: Institutions, cadres, normes, standards, spécifications et lignes directrices pour améliorer la résilience des TIC.

(1) Ce chapitre décrit de manière synthétique les institutions, les *frameworks*, les normes, les standards et la spécification dans le cadre de ce guide sur l'amélioration de la résilience des TIC. Ces descriptions donnent un aperçu général. Pour augmenter la résilience des TIC, il est recommandé de s'orienter vers des *frameworks*, des normes, des standards et des spécifications actuels, établis et introduits, publiés par des organisations et des institutions reconnues. De nombreuses normes, standards et spécifications servent d'aide à la mise en œuvre. Souvent, les publications ne présentent pas d'exemples d'application, elles servent uniquement à orienter, à définir des mesures et à aider à trouver des solutions.

D.0 Organisations et institutions

(2) Le tableau suivant répertorie les organisations et institutions qui apportent une contribution précieuse à l'amélioration de la résilience des TIC sous la forme de cadres, de normes, de spécifications, de guides et d'outils:

Nom	Brève description
SNV (Association suisse de normalisation)	<p>La SNV, ou Association Suisse de Normalisation, est l'organisme national de normalisation en Suisse. Elle est responsable du développement et de la promotion des normes et standards techniques en Suisse. La SNV a son siège à Zurich et travaille en étroite collaboration avec des organisations internationales de normalisation telles que l'Organisation internationale de normalisation (ISO) et le Comité européen de normalisation (CEN). Les principales tâches de la SNV comprennent:</p> <ol style="list-style-type: none"> développement de normes: la SNV élabore des normes techniques et des standards dans un grand nombre de secteurs et de domaines, notamment l'ingénierie mécanique, l'ingénierie électrique, les technologies de l'information, la protection de l'environnement et plus encore. Ces normes ont pour but de promouvoir la qualité et la sécurité des produits et des services et de favoriser l'interopérabilité. harmonisation: la SNV s'efforce d'harmoniser les normes et standards nationaux de la Suisse avec les normes internationales et européennes afin de faciliter le libre échange de biens et de services et d'assurer la conformité avec les réglementations internationales. formation et conseil: la SNV propose des formations, des ateliers et des services de conseil aux entreprises et aux organisations afin de les aider à mettre en œuvre et à respecter les normes. diffusion d'informations: la SNV informe le public de l'importance des normes et des standards ainsi que des développements actuels en matière de normalisation. <p>La SNV joue un rôle important dans le soutien de l'économie et de l'industrie suisses en fournissant une base solide pour la qualité et la sécurité. Elle contribue à renforcer la compétitivité des produits et services suisses sur les marchés internationaux et à promouvoir la sécurité et l'efficacité dans différents secteurs.</p>
NIST (National Institute of Standards and Technology) États-Unis	<p>Le National Institute of Standards and Technology (NIST) aux États-Unis est une agence fédérale qui soutient le développement et la promotion de normes et de directives techniques dans différentes disciplines. Cela comprend des domaines tels que la sécurité de l'information, les techniques de mesure et d'essai et les normes technologiques afin de promouvoir l'innovation et l'interopérabilité. Le NIST joue un rôle central dans le renforcement des bases techniques aux États-Unis et dans la promotion des meilleures pratiques dans diverses industries.</p>
CSA (Cloud Security Alliance)	<p>La Cloud Security Alliance (CSA) est une organisation internationale à but non lucratif qui se concentre sur la promotion des meilleures pratiques et de la recherche en matière de cybersécurité et de protection des données dans les environnements de cloud computing. Fondée en 2009, la CSA a rapidement pris de l'importance et est devenue l'une des principales voix du secteur de la sécurité du cloud.</p>
CIS (Center for Internet Security)	<p>Le Center for Internet Security (CIS) est une organisation à but non lucratif qui se concentre sur l'amélioration de la cybersécurité et la protection des systèmes d'information et des données. Fondé en 2000, le CIS joue un rôle important dans le développement de politiques de cybersécurité, de meilleures pratiques et de contrôles de sécurité pour les organisations, les gouvernements et les individus.</p>
ISACA (Information Systems Audit and Control Association)	<p>L'ISACA (Information Systems Audit and Control Association) est une organisation internationale à but non lucratif spécialisée dans les domaines de la sécurité de l'information, de la gouvernance informatique, de la gestion des risques et de la protection des données. Elle propose des certifications telles que CISA (Certified Information Systems Auditor) et CISM (Certified Information Security Manager) afin de former et de certifier des</p>



Nom	Brève description
	professionnels dans ces domaines. L'organisation promeut les meilleures pratiques et fournit des ressources et des formations pour améliorer la sécurité informatique et des informations dans les entreprises et les organisations du monde entier.
ISO (Organisation internationale de normalisation)	<p>L'Organisation internationale de normalisation (ISO) est une organisation de normalisation mondialement reconnue qui développe des normes pour un large éventail d'industries et de disciplines. L'ISO a été créée en 1947 et compte des pays membres du monde entier. Son objectif est d'établir des normes internationales afin de promouvoir la qualité, la sécurité, l'efficacité et l'interopérabilité des produits, des services et des systèmes. Les normes ISO couvrent un grand nombre de domaines, y compris la gestion de la qualité, l'environnement, la sécurité de l'information, les soins de santé, la technologie, la sécurité et plus encore. Ces normes fournissent des directives et des meilleures pratiques reconnues dans le monde entier pour aider les organisations à améliorer leurs processus, produits et services.</p> <p>L'ISO élabore ses normes en faisant collaborer des experts, des techniciens et des représentants de différents pays afin de garantir que les normes soient acceptées et appliquées à l'échelle mondiale. Dans de nombreux secteurs et pays, la conformité aux normes ISO est une condition préalable à la certification et à l'accès aux marchés internationaux.</p>
IEC (International Electrotechnical Commission)	<p>L'IEC (commission électrotechnique internationale) est un organisme international de normalisation reconnu dans le monde entier. Fondée en 1906, l'IEC a son siège à Genève, en Suisse. Elle est composée de représentants de différents pays et organisations et a pour objectif de développer des normes techniques afin de promouvoir l'interopérabilité, la sécurité et la qualité des produits et systèmes électriques et électroniques.</p> <p>L'IEC développe des normes dans un large éventail de domaines, y compris:</p> <ol style="list-style-type: none"> 1. la production et distribution d'énergie électrique 2. la compatibilité électromagnétique (CEM) 3. la sécurité électrique 4. la technologie informatique 5. les mesures électriques et méthodes d'essai 6. l'électronique et les technologies des semi-conducteurs 7. l'impact environnemental des produits électriques et électroniques <p>Les normes IEC sont adoptées par de nombreux pays dans le monde et sont obligatoires ou recommandées dans de nombreux secteurs industriels. Elles fournissent des lignes directrices claires pour assurer la sécurité, l'interopérabilité et la qualité des produits et systèmes électriques et électroniques. L'IEC joue un rôle important dans le soutien au développement et à l'innovation technologiques et dans la création de normes qui favorisent le commerce mondial et la coopération.</p>
EN (norme européenne)	<p>EN (norme européenne) fait référence aux normes applicables dans l'Union européenne (UE). Ces normes sont spécifiques aux pays européens et ont pour but d'harmoniser et d'uniformiser les exigences et les normes techniques dans différents secteurs industriels. Ils soutiennent l'interopérabilité des produits et des services et contribuent à garantir la qualité et la sécurité.</p> <p>Voici quelques informations importantes sur l'EN:</p> <ol style="list-style-type: none"> 1. développement: les normes EN sont élaborées par différents organismes de normalisation européens, dont le Comité européen de normalisation (CEN) et le Comité européen de normalisation électrotechnique (CENELEC). Ces organisations travaillent en étroite collaboration afin d'établir des normes techniques pour un grand nombre de secteurs et d'industries. 2. reconnaissance: les normes EN sont reconnues par les États membres de l'UE et s'appliquent dans l'ensemble du marché intérieur de l'UE. Elles ne sont généralement pas obligatoires, à moins qu'elles ne soient reprises dans des lois ou des règlements qui rendent obligatoire le respect de certaines normes. 3. harmonisation: les normes EN soutiennent l'harmonisation des réglementations techniques au sein de l'UE. Cela facilite la libre circulation des biens et des services au sein du marché de l'UE et favorise les échanges commerciaux. 4. champs d'application: les normes EN sont applicables dans un large éventail de domaines, notamment l'ingénierie mécanique, l'ingénierie électrique, la construction, les dispositifs médicaux, la protection de l'environnement, les technologies de l'information et bien d'autres encore. 5. référence de la norme européenne: les normes EN sont identifiées par une marque de norme européenne unique indiquant le domaine d'application et l'année d'édition. <p>Les normes EN jouent un rôle crucial dans la création d'une norme uniforme pour les produits et services dans l'UE et sont d'une grande importance pour les fabricants, les prestataires de services et les entreprises opérant sur les marchés européens. Ils soutiennent l'assurance qualité, la sécurité et la conformité aux réglementations européennes.</p>



Nom	Brève description
ISA (International Society of Automation)	<p>L'International Society of Automation (ISA) est une organisation mondiale à but non lucratif qui se concentre sur la promotion des technologies d'automatisation et de contrôle. L'ISA a été fondée en 1945 et son siège social est aux États-Unis. C'est l'une des principales organisations mondiales qui assiste les professionnels dans les domaines de l'automatisation, du contrôle des processus, de l'instrumentation et de la cybersécurité dans l'industrie.</p> <p>L'ISA propose un large éventail de ressources, notamment des formations, des certifications, des publications techniques et des normes, afin d'aider les professionnels à se former et à se développer professionnellement. L'organisation joue un rôle important dans la promotion des bonnes pratiques et des technologies dans les domaines de l'automatisation industrielle, du contrôle des processus et de l'instrumentation.</p> <p>Les principales activités de l'ISA sont les suivantes:</p> <ol style="list-style-type: none"> 1. développement de normes: l'ISA développe des standards et des normes techniques largement utilisés dans l'industrie et qui contribuent à l'interopérabilité et à la sécurité des systèmes d'automatisation. 2. éducation et formation: l'ISA propose des formations, des séminaires et des certifications afin de fournir aux professionnels de l'automatisation et du contrôle les compétences et les connaissances nécessaires. 3. conférences et événements: l'ISA organise des conférences, des salons et des événements au cours desquels les professionnels peuvent partager leurs connaissances et leurs expériences. 4. publication de revues technologiques et d'ouvrages spécialisés: l'ISA publie des revues techniques et des ouvrages spécialisés afin de partager les développements actuels et les meilleures pratiques du secteur. <p>L'ISA joue un rôle important dans la promotion des technologies d'automatisation et de contrôle, et ses efforts contribuent à améliorer l'efficacité et la sécurité dans différents secteurs industriels.</p>
<p>Les liens entre ISA (International Society of Automation), IEC (International Electrotechnical Commission) et EN (normes européennes) sont les suivants:</p> <ol style="list-style-type: none"> 1. ISA et IEC: l'ISA et l'IEC sont toutes deux des organisations internationales qui se concentrent sur le développement de normes et de standards techniques. Alors que l'ISA se spécialise principalement dans les technologies d'automatisation et de contrôle dans l'industrie, l'IEC couvre une gamme plus large de technologies électrotechniques et électroniques. Les deux organisations développent des normes et des standards qui peuvent être appliqués dans le monde entier dans différents secteurs industriels et pays. Dans certains cas, l'ISA et l'IEC collaborent pour développer des normes communes, notamment dans les domaines où l'interface entre l'automatisation et l'ingénierie électrique est importante. 2. Normes EN: les normes EN sont des normes européennes applicables dans l'Union européenne (UE). Ces normes peuvent être développées par différents organismes de normalisation internationaux et nationaux, y compris l'IEC. Les normes EN sont reconnues au niveau européen et s'appliquent dans les États membres de l'UE. Dans certains cas, les normes EN sont des reprises directes des normes IEC, avec des adaptations aux exigences européennes. Les normes ISA sont moins spécifiques aux normes européennes, car l'ISA est une organisation américaine. <p>Globalement, il existe des interactions entre ces organisations et leurs normes, en particulier sur les marchés et industries internationaux qui dépendent de normes mondiales. Les entreprises qui proposent des produits et des services sur les marchés internationaux doivent prendre en compte les normes et standards pertinents afin d'assurer l'interopérabilité et la conformité réglementaire.</p>	
ENISA (European Union Agency for Cybersecurity)	<p>L'ENISA (European Union Agency for Cybersecurity) est une agence de l'UE chargée de promouvoir et de renforcer la cybersécurité dans l'Union européenne. L'ENISA a été créée en 2004 et a son siège en Grèce. Les principales tâches de l'ENISA comprennent:</p> <ol style="list-style-type: none"> 1. conseil en cybersécurité: l'ENISA fournit une expertise et un soutien en matière de cybersécurité aux institutions européennes, aux États membres et à d'autres acteurs en Europe. 2. recherche et développement: l'agence encourage la recherche et le développement de solutions de cybersécurité et de bonnes pratiques dans l'UE. 3. sensibilisation et formation: ENISA s'efforce de sensibiliser aux questions de cybersécurité dans l'UE et de développer des programmes de formation pour les professionnels et le grand public. 4. coordination de la coopération: l'agence favorise la coordination et l'échange d'informations et de bonnes pratiques au sein de l'UE afin de renforcer la cybersécurité. <p>L'ENISA joue un rôle important dans la promotion de la cybersécurité au sein de l'UE et travaille en étroite collaboration avec les États membres, la Commission européenne et d'autres partenaires afin de protéger l'infrastructure et les données numériques contre les menaces.</p>
IEEE (Institute of Electrical and Electronics Engineers)	<p>L'IEEE (Institute of Electrical and Electronics Engineers), est une organisation professionnelle mondialement reconnue qui se concentre sur la promotion et le développement de la technologie et de la science dans les domaines du génie électrique, de l'électronique, des technologies de l'information et des disciplines connexes. L'IEEE est l'une des plus grandes organisations techniques au monde et compte des membres de différents</p>



Nom	Brève description
	<p>pays, notamment des ingénieurs, des scientifiques et des professionnels d'un large éventail de disciplines techniques.</p> <p>L'IEEE joue un rôle important dans le développement de normes et de directives techniques dans différents domaines, notamment les communications sans fil, le matériel informatique, les technologies de réseau et bien d'autres. Ces normes contribuent à l'interopérabilité des technologies et favorisent l'innovation et la qualité.</p> <p>L'organisation organise également des conférences, publie des revues scientifiques et encourage le partage des connaissances et le développement professionnel des professionnels. L'IEEE a plusieurs sociétés techniques qui se concentrent sur des domaines spécifiques tels que l'électronique, les télécommunications, l'informatique et plus encore.</p>
BSI (Office fédéral allemand de la sécurité des technologies de l'information)	<p>L'Office fédéral de la sécurité des technologies de l'information (BSI) est l'autorité nationale en matière de cybersécurité en Allemagne. Il a été créé en 1991 et a son siège à Bonn. Le BSI est responsable de la garantie de la sécurité informatique dans l'administration fédérale et de l'assistance aux entreprises et aux citoyens en Allemagne.</p> <p>Les principales tâches du BSI comprennent:</p> <ol style="list-style-type: none"> 1. conseil et soutien: le BSI fournit des conseils et des ressources pour améliorer la sécurité informatique dans l'administration fédérale, les entreprises et les particuliers. 2. certification et normes: le BSI développe des normes de sécurité et des procédures de certification pour les produits et systèmes informatiques afin de s'assurer qu'ils répondent à des exigences de sécurité élevées. 3. réponse aux incidents: le BSI réagit aux cyber-attaques et coordonne les mesures de défense contre les incidents de sécurité. 4. sensibilisation et éducation: l'autorité informe le public sur les cybermenaces actuelles et promeut la sensibilisation à la sécurité informatique. <p>Le BSI joue un rôle crucial dans la garantie de la cybersécurité en Allemagne et contribue à la protection de l'infrastructure et des données numériques contre les cyberattaques et les menaces.</p>
NERC (North American Electric Reliability Corporation)	<p>La North American Electric Reliability Corporation (NERC) est une organisation nord-américaine à but non lucratif dont l'objectif est de garantir la fiabilité et la stabilité du réseau électrique aux États-Unis, au Canada et au Mexique. La NERC est chargée de développer et de faire appliquer les normes et les réglementations pour le secteur de la distribution d'électricité en Amérique du Nord.</p> <p>Les principales tâches et responsabilités de la NERC comprennent:</p> <ol style="list-style-type: none"> 1. développement de normes: la NERC développe des normes techniques et des standards nécessaires au fonctionnement sûr du réseau électrique en Amérique du Nord. Ces normes couvrent des sujets tels que l'exploitation, la planification, la cybersécurité et la protection des systèmes de transport et de distribution d'électricité. 2. surveillance et application: la NERC surveille et vérifie que les compagnies d'électricité respectent les normes et réglementations qu'elle a développées. Elle applique des sanctions lorsque les entreprises ne respectent pas ces normes. 3. cybersécurité : la NERC joue un rôle important dans la protection du réseau électrique contre les cybermenaces. Elle développe et promeut des normes pour améliorer la cybersécurité dans le secteur de l'énergie. 4. gestion de crise: la NERC soutient la préparation et la réponse aux situations d'urgence et de crise affectant le réseau électrique et encourage la coopération entre les compagnies d'électricité et les autres parties concernées. <p>Le travail de la NERC est crucial, car un réseau électrique fiable est essentiel pour l'économie, la sécurité publique et la vie quotidienne en Amérique du Nord. L'organisation travaille en étroite collaboration avec différentes parties prenantes, y compris les autorités gouvernementales, les services publics, les opérateurs de réseau de transport et d'autres parties concernées, afin de s'assurer que le réseau électrique répond aux normes les plus élevées en matière de sécurité et de fiabilité.</p>

D.1 Frameworks

Nom	Brève description
CSF NIST 1.1 (Cyber-Security Framework version 1.1)	<p>CSF NIST 1.1 est la version actuelle du cadre de cybersécurité du National Institute of Standards and Technology (NIST) aux États-Unis. Ce cadre est destiné à améliorer les pratiques de cybersécurité dans les organisations et les entreprises. La version 1.1 comprend des lignes directrices avancées sur la réduction des risques et l'amélioration de la résilience face aux cybermenaces.</p> <p>Le CSF NIST 1.1 est basé sur cinq éléments clés: l'identification, la protection, la détection, la réaction et la restitution. Ces éléments aident les entreprises et les unités organisationnelles à développer, évaluer et améliorer leurs programmes de cybersécurité en</p>



Nom	Brève description
	mettant en œuvre les meilleures pratiques et normes. La mise à jour 1.1 comprend également des priorités supplémentaires sur la protection des données et la vie privée, ainsi que la prise en compte des cyber-risques dans la chaîne d'approvisionnement.
NIST SP 800-Serie	<p>La NIST SP 800-Serie est une série de publications spéciales (Special Publications, SP) publiées par le National Institute of Standards and Technology (NIST) des États-Unis. Ces publications couvrent différents aspects de la sécurité de l'information et de la protection des données et proposent des lignes directrices, des bonnes pratiques et des recommandations pour renforcer la sécurité des systèmes d'information et relever les défis en matière de sécurité. La NIST SP 800-Serie est reconnue internationalement et est utilisée par les entreprises et les unités organisationnelles du monde entier comme une ressource précieuse pour améliorer la sécurité de l'information et la protection des données. Ces publications sont régulièrement mises à jour pour répondre à l'évolution des besoins et des menaces en matière de sécurité de l'information et servent de documents de référence essentiels pour les entreprises et les unités organisationnelles, les autorités, les entreprises et les unités organisationnelles qui souhaitent renforcer leurs pratiques de sécurité.</p>
COBIT 5 (Control Objectives for Information and Related Technologies Version 5)	<p>COBIT 5 est un cadre de référence pour la gouvernance et la gestion des technologies de l'information de l'entreprise et des unités organisationnelles. Il a été développé par l'organisation internationale ISACA et constitue la cinquième version du framework COBIT (Control Objectives for Information and Related Technologies). COBIT 5 offre aux entreprises et aux unités organisationnelles une méthode complète pour améliorer leurs processus de gouvernance et de gestion informatiques. Voici quelques caractéristiques et objectifs importants de COBIT 5:</p> <ol style="list-style-type: none"> 1. gouvernance informatique: COBIT 5 établit les principes et les structures d'une gouvernance informatique efficace afin de garantir que la stratégie et les ressources informatiques correspondent aux objectifs de l'entreprise. 2. approche holistique: COBIT 5 propose un modèle holistique qui intègre la gestion informatique, la gestion des risques et la conformité afin d'optimiser la fourniture de services informatiques. 3. orientation vers les processus: le cadre fournit des modèles de processus et des lignes directrices pour les processus de gouvernance et de gestion informatiques afin d'améliorer l'efficacité et l'efficience. 4. orientation vers les valeurs: COBIT 5 met l'accent sur la création de valeur par l'informatique et garantit que les investissements informatiques soutiennent les objectifs de l'entreprise. 5. amélioration continue: le framework favorise la surveillance et l'optimisation continues des pratiques de gouvernance et de gestion informatiques. <p>COBIT 5 est très répandu dans le secteur informatique et est utilisé par les entreprises et les unités organisationnelles pour optimiser leurs structures informatiques, répondre aux exigences de conformité et utiliser efficacement les ressources informatiques. Il fournit des lignes directrices claires et les meilleures pratiques pour améliorer la qualité et la fiabilité des services et des systèmes informatiques et atteindre les objectifs commerciaux.</p>
CSA CCM (Cloud Controls Matrix)	<p>La Cloud Controls Matrix (CCM) est un cadre développé par la Cloud Security Alliance (CSA). La Cloud Security Alliance est une organisation internationale qui se concentre sur la promotion des meilleures pratiques et des normes de sécurité en matière de cloud computing. La CCM est un élément important des efforts de la CSA pour améliorer la sécurité dans le cloud.</p> <p>La CCM est un ensemble de contrôles et de pratiques de sécurité qui s'appliquent à différents domaines du cloud computing. Ces contrôles et pratiques sont structurés dans une matrice qui aide les entreprises et les unités organisationnelles à évaluer et à améliorer la sécurité de leurs environnements de cloud computing. Le CCM est divisé en plusieurs domaines, dont:</p> <ol style="list-style-type: none"> 1. gouvernance et conformité 2. gestion des risques 3. classification et protection des données 4. gestion des identités et des accès 5. infrastructure et virtualisation 6. opérations et réponse aux incidents 7. conformité et audit <p>Les entreprises et les unités organisationnelles peuvent utiliser la CCM pour s'assurer qu'elles mettent en œuvre des contrôles de sécurité appropriés dans leurs environnements de cloud computing et qu'elles respectent les meilleures pratiques. La CCM peut servir de guide pour l'évaluation des fournisseurs de services cloud et la définition des exigences en matière de sécurité et de confidentialité.</p> <p>Dans l'ensemble, la CCM est un outil utile pour améliorer la sécurité dans les environnements de cloud et renforcer la confiance dans les services de cloud.</p>



Nom	Brève description
CIS CSC (Center for Internet Security Critical Security Controls)	<p>Le CIS CSC est un cadre comprenant 20 contrôles de sécurité de base développé par l'organisation à but non lucratif Center for Internet Security (CIS). Conçus comme des bonnes pratiques et des normes de sécurité, ces contrôles visent à renforcer la cybersécurité des entreprises et des unités organisationnelles et à minimiser les vulnérabilités. Les 20 contrôles CIS CSC sont répartis en trois catégories principales:</p> <ol style="list-style-type: none"> 1. Basic Cyber Hygiene (hygiène cybernétique de base): <ul style="list-style-type: none"> - inventaire et contrôle du matériel et des logiciels - configurations de sécurité pour le matériel et les logiciels - surveillance et évaluations de la sécurité 2. Foundational Security Controls (contrôles de sécurité de base): <ul style="list-style-type: none"> - classification et protection des données - protection contre les virus et les logiciels malveillants - segmentation du réseau - sauvegarde et restauration des données - gestion sécurisée des mises à jour et des correctifs - sécurité en fin de ligne - gestion des comptes utilisateurs et des autorisations - authentification multifactorielle - limitation du trafic de données - passerelles e-mail et web sécurisées 3. Organizational Security Controls (contrôles de sécurité organisationnels): <ul style="list-style-type: none"> - Security Awareness and Training (sensibilisation et formation à la sécurité) - Incident Response and Management (réponse et gestion des incidents de sécurité) - Penetration Tests and Red Team Exercises (tests de pénétration et exercices red team) - Continuous Monitoring (surveillance continue) - Security Metrics (métriques de sécurité) <p>Les CIS CSC sont conçus pour aider les entreprises et les unités organisationnelles à se protéger contre les cybermenaces complexes actuelles, à identifier les vulnérabilités et à prendre des contre-mesures. Ils constituent un outil précieux pour améliorer la sécurité des systèmes d'information et minimiser les risques. Les entreprises et les unités organisationnelles peuvent utiliser le CIS CSC pour développer leurs stratégies de sécurité et optimiser leurs programmes de sécurité.</p>
NERC CIP (Cyber Security Permanent)	<p>NERC CIP signifie «North American Electric Reliability Corporation Critical Infrastructure Protection», ce qui se traduit par «protection de l'infrastructure critique de la North American Electric Reliability Corporation». Il s'agit d'un ensemble de règles et de normes de cybersécurité élaborées par la North American Electric Reliability Corporation (NERC) afin de renforcer la cybersécurité dans le secteur de la distribution d'électricité en Amérique du Nord.</p> <p>Le NERC CIP se compose de plusieurs versions, la version actuelle étant la version 6. Les normes et exigences définies dans le NERC CIP visent à protéger le réseau électrique contre les cybermenaces et à assurer la résilience du système d'alimentation électrique. Les normes CIP comprennent des règles pour la protection des systèmes et des informations critiques pour le fonctionnement du réseau électrique, pour la protection contre les accès non autorisés et pour la détection et la gestion des incidents de sécurité. Les exigences du NERC CIP couvrent des sujets comme:</p> <ol style="list-style-type: none"> 1. identifier et classer les actifs et les informations critiques 2. réalisation d'évaluations et de gestion des risques 3. contrôles d'accès physiques et logiques aux infrastructures critiques 4. surveiller, signaler et réagir aux incidents de cybersécurité 5. former et sensibiliser le personnel à la cybersécurité 6. amélioration continue des pratiques de sécurité <p>Les normes NERC CIP s'appliquent aux producteurs d'électricité, aux gestionnaires de réseau de transport, aux gestionnaires de réseau de distribution et aux autres entités du secteur de la distribution d'électricité aux États-Unis, au Canada et au Mexique. Elles visent à garantir que l'approvisionnement en électricité en Amérique du Nord est protégé contre les cyber-attaques et contribuent à assurer la fiabilité et l'intégrité du réseau électrique.</p> <p>La conformité du NERC CIP est essentielle pour les entreprises et les unités organisationnelles du secteur de l'énergie, car le non-respect de ces normes peut avoir de graves conséquences juridiques et financières. Les entreprises et les unités organisationnelles doivent mettre en œuvre des mesures de cybersécurité complètes pour se conformer aux exigences du NERC CIP et protéger le réseau électrique contre les cybermenaces.</p>
Série ISO 27000	<p>La série ISO 27000 est un ensemble de normes et de lignes directrices internationales qui se concentrent sur la gestion de la sécurité de l'information et la sécurité de l'information dans les entreprises et les unités organisationnelles. Développée et mise à jour par l'Organisation internationale de normalisation (ISO), cette série de normes fournit un cadre complet pour la planification, la mise en œuvre et le maintien de la sécurité de</p>



Nom	Brève description
	<p>l'information dans les entreprises et les unités organisationnelles. La série ISO 27000 est d'une grande importance pour les entreprises et les unités organisationnelles de toutes tailles et de tous secteurs, car elle fournit des lignes directrices claires et des bonnes pratiques pour sécuriser l'information et les systèmes d'information. Elle est particulièrement pertinente à une époque où la cybersécurité revêt une importance cruciale et où les entreprises et les unités organisationnelles sont de plus en plus confrontées à des cybermenaces. Le respect de ces normes contribue à renforcer la confiance de la clientèle, des partenaires et des parties prenantes dans la sécurité et l'intégrité des informations et à satisfaire aux exigences légales et réglementaires.</p>
IEC TC 70	<p>TC 70 IEC signifie «Technical Committee 70» de l'International Electrotechnical Commission (IEC). Ce comité technique est spécialisé dans la normalisation des applications et des technologies dans le domaine de la production, du transport, de la distribution et de l'utilisation de l'énergie électrique. Le TC 70 de l'IEC élabore des standards et des normes internationales qui couvrent un large éventail d'aspects liés aux systèmes d'alimentation électrique.</p> <p>IEC TC 70 couvre un large éventail de sujets et d'aspects, notamment:</p> <ol style="list-style-type: none"> 1. générateurs et moteurs électriques: des normes pour la conception et les essais des générateurs et des moteurs utilisés dans les installations de production d'énergie et les applications industrielles. 2. transformateurs de puissance: normes pour la construction, les essais et l'utilisation des transformateurs de puissance utilisés dans les réseaux de transport et de distribution. 3. systèmes de protection et de contrôle: normes pour les relais de protection, les systèmes de contrôle et les solutions d'automatisation dans les systèmes d'alimentation électrique. 4. installations à haute tension: normes pour la construction et les essais des installations à haute tension, y compris les installations de couplage et leurs composants. 5. gestion de l'énergie et contrôle de la qualité: normes traitant de la surveillance de la qualité de l'énergie électrique et de la gestion de l'énergie dans les réseaux d'approvisionnement. <p>IEC TC 70 joue un rôle crucial dans la création de normes qui garantissent la sécurité, l'efficacité et l'interopérabilité des systèmes d'alimentation électrique dans le monde entier. Ces normes sont d'une grande importance pour le secteur de l'énergie, car elles contribuent à garantir la fiabilité de l'approvisionnement énergétique et à faciliter l'intégration des sources d'énergie renouvelables et des nouvelles technologies dans les réseaux.</p>
Normes BSI	<p>L'Office fédéral de la sécurité des technologies de l'information (BSI) en Allemagne développe et publie une série de normes et de directives dans le domaine de la sécurité de l'information. Ces normes sont conçues pour aider les entreprises et les unités organisationnelles à sécuriser leurs systèmes et données d'information. Voici quelques-unes des principales normes BSI:</p> <ol style="list-style-type: none"> 1. «BSI IT-Grundschutz»: une norme complète qui contient des bonnes pratiques et des recommandations pour sécuriser les systèmes d'information. Elle fournit un cadre pour l'identification des besoins de protection et la mise en œuvre de mesures de sécurité. 2. Normes BSI 100-4 à 100-3: ces normes traitent de la gestion des risques liés à la sécurité de l'information et fournissent des lignes directrices pour l'identification, l'analyse et l'évaluation des risques dans les systèmes d'information. 3. Normes BSI 200-1 à 200-4: ces normes traitent de la sécurisation des systèmes informatiques, des réseaux et des technologies de communication. Elles fournissent des recommandations pour la mise en œuvre de mesures de sécurité et pour assurer la confidentialité, l'intégrité et la disponibilité des données et des systèmes. 4. Normes BSI 300-3 et 300-4: ces normes abordent le thème Business Continuity Management (BCM) et fournissent les lignes directrices pour la planification et la mise en œuvre de mesures visant à maintenir la continuité des activités en cas d'incident ou de catastrophe. 5. Normes BSI 100-1 et 100-2: ces normes abordent les thèmes de la sensibilisation et de la formation à la sécurité de l'information et proposent des recommandations pour sensibiliser les employés et les former aux questions de sécurité. 6. Normes BSI 400-1 à 400-3: ces normes traitent des aspects de la gestion des identités et des accès (IAM) et fournissent des recommandations sur la gestion des identités des utilisateurs et des droits d'accès dans les systèmes d'information. <p>Les normes BSI sont des outils importants pour améliorer la sécurité de l'information en Allemagne et sont considérées comme un guide pour les entreprises et les unités organisationnelles dans différents secteurs. Elles visent à minimiser les risques, à garantir la conformité et à renforcer la sécurité des systèmes d'information. Les entreprises et les unités organisationnelles devraient intégrer les normes BSI dans leurs stratégies et pratiques de sécurité afin de prendre les mesures appropriées pour sécuriser leur infrastructure informatique.</p>



D.2 Normes et standards spécifiques importants

Norm	Brève description
NIST SP 800-53	<p>NIST SP 800-53 (Special Publication 800-53) est un document publié par le National Institute of Standards and Technology (NIST) aux États-Unis qui définit les contrôles de sécurité et de confidentialité pour les agences fédérales, les entreprises et les unités organisationnelles qui traitent des informations confidentielles. Ce document fait partie du cadre de cybersécurité du NIST et joue un rôle important dans la définition des normes et des contrôles de sécurité des systèmes et technologies de l'information.</p> <p>La norme NIST SP 800-53 contient un ensemble de contrôles de sécurité, répartis en 18 familles ou catégories, telles que le contrôle d'accès, la gestion des identités, la surveillance et la protection des systèmes de communication. Ces contrôles fournissent des instructions et des recommandations détaillées sur la façon de sécuriser les systèmes informatiques et les données afin de s'assurer qu'ils répondent aux normes de sécurité les plus élevées.</p> <p>L'utilisation du NIST SP 800-53 est très répandue aux États-Unis et s'étend au-delà des agences fédérales, car de nombreuses entreprises et unités organisationnelles le reconnaissent comme une norme éprouvée pour la sécurité de leurs systèmes d'information. Il fournit un cadre clair et structuré pour le développement, la mise en œuvre et le suivi des contrôles de sécurité et contribue à garantir la sécurité et la protection des informations dans un paysage de menaces en constante évolution.</p>
IEC 62351 (Sécurité de l'information dans la technologie de contrôle des réseaux et des stations)	<p>La IEC 62351 est une série de normes qui traite de la «sécurité de l'information dans le domaine de la technologie de contrôle des réseaux et des stations». Cette série de normes a été développée par la International Electrotechnical Commission (IEC) et vise à garantir la sécurité et l'intégrité des systèmes d'information dans le secteur de l'énergie, en particulier dans les domaines de la gestion des réseaux et des stations.</p> <p>La série de normes IEC 62351 se compose de différentes parties qui couvrent des aspects spécifiques de la sécurité de l'information dans les systèmes d'alimentation électrique.</p> <p>Elle vise à renforcer la sécurité de l'information dans les infrastructures critiques du secteur de l'énergie et à les protéger contre les cybermenaces. C'est essentiel, car une perturbation ou une attaque des systèmes d'approvisionnement en énergie peut avoir un impact considérable sur la société et l'économie. Ces normes fournissent des lignes directrices et des bonnes pratiques pour assurer la sécurité, l'intégrité et la disponibilité des systèmes d'information dans ce secteur. Les entreprises et les unités organisationnelles de la branche de l'énergie devraient prendre en compte la série de normes IEC 62351 pour s'assurer qu'elles mettent en œuvre des mesures de sécurité de l'information appropriées.</p>
IEC 62443 (Réseaux de communication industriels – sécurité des réseaux et des systèmes)	<p>L'IEC 62443 est une série de normes internationales qui se concentre sur la sécurité des réseaux et des systèmes dans les réseaux de communication industriels. Ces normes ont été développées par l'ICE et visent à garantir la cybersécurité des systèmes et des réseaux dans le domaine de l'automatisation et du contrôle industriels. Cette série de normes contribue à protéger les infrastructures critiques et les processus industriels contre les cybermenaces.</p> <p>L'IEC 62443 se compose de plusieurs parties qui couvrent différents aspects de la sécurité des réseaux et des systèmes. Elle vise à assurer la sécurité et l'intégrité des systèmes de commande et d'automatisation industriels afin d'éviter les dysfonctionnements, les pannes et les atteintes à la sécurité. Cette série de normes est d'une grande importance car les processus industriels et les infrastructures critiques, comme la production d'énergie, le transport et la fabrication, dépendent fortement des systèmes automatisés. Elle fournit des lignes directrices claires et des bonnes pratiques pour sécuriser ces systèmes contre les cybermenaces et soutient la résilience des réseaux industriels. Les entreprises et les unités organisationnelles du secteur de l'automatisation industrielle devraient intégrer la série de normes ICE 62443 dans leurs stratégies et pratiques de sécurité afin de garantir la fiabilité et la sécurité de leurs opérations.</p>
ISO/IEC 27001, 27002	<p>ISO/IEC 27001 et ISO/IEC 27002 sont des normes internationales dans le domaine de la sécurité de l'information, conçues pour aider les entreprises et les unités organisationnelles à mettre en œuvre et à maintenir un ISMS efficace. Ces normes sont importantes pour garantir la confidentialité, l'intégrité et la disponibilité des informations dans les entreprises et les unités organisationnelles. Voici les principales informations sur ces normes:</p> <p>ISO/IEC 27001:</p> <ul style="list-style-type: none"> - ISO/IEC 27001 est la norme principale pour le système de gestion de la sécurité de l'information. Elle définit les exigences auxquelles une organisation doit satisfaire pour mettre en place, exploiter, maintenir et améliorer en permanence un ISMS efficace.



Nom	Brève description
	<ul style="list-style-type: none"> - La norme propose une approche systématique de l'évaluation et du traitement des risques afin de garantir que les risques de sécurité sont identifiés et traités de manière appropriée. - Les entreprises et les unités organisationnelles qui mettent en œuvre la norme ISO/IEC 27001 adoptent une approche basée sur les risques afin d'identifier et de mettre en œuvre des contrôles et des mesures de sécurité qui répondent à leurs besoins spécifiques. - ISO/IEC 27001 permet la certification, par laquelle des organismes de contrôle indépendants vérifient la conformité à la norme et peuvent délivrer aux entreprises et aux unités organisationnelles une certification ISO/IEC 27001. <p>ISO/IEC 27002:</p> <ul style="list-style-type: none"> - ISO/IEC 27002, également connu sous le nom de «Code of Practice for Information Security Controls», est un document d'accompagnement de la norme ISO/IEC 27001. Il fournit des recommandations et des lignes directrices détaillées pour la mise en œuvre des contrôles de sécurité de l'information. - La norme contient une liste complète de contrôles et de mesures de sécurité qui peuvent être utilisés dans différents domaines de la sécurité de l'information, tels que le contrôle d'accès, le cryptage, la gestion des incidents, et bien plus encore. - ISO/IEC 27002 propose des mesures et des pratiques concrètes pour aider les entreprises et les unités organisationnelles à se conformer aux exigences de la norme ISO/IEC 27001. <p>Ensemble, les normes ISO/IEC 27001 et ISO/IEC 27002 constituent une base importante pour la planification et la mise en œuvre de mesures de sécurité de l'information dans les entreprises et les unités organisationnelles. Ces normes aident à évaluer les risques de sécurité, à définir des objectifs de sécurité et à mettre en place des contrôles efficaces pour sécuriser les informations. Elles concernent les entreprises et les unités organisationnelles de toutes tailles et de tous secteurs et contribuent à la sécurisation des données et des systèmes de l'entreprise. La certification ISO/IEC 27001 est un signe reconnu d'un niveau de sécurité élevé et peut renforcer la confiance de la clientèle, des partenaires et des parties prenantes.</p>
ISO/IEC 27019	<p>Élaborée spécialement pour le secteur de l'énergie, ISO/IEC 27019 est une norme internationale axée sur la sécurité de l'information dans ce secteur. Elle fournit des directives et des recommandations pour la sécurisation des systèmes et données d'information dans la production, le transport et la distribution d'énergie.</p> <p>Voici les caractéristiques et objectifs principaux de la norme ISO/IEC 27019:</p> <ol style="list-style-type: none"> 1. Champ d'application: la norme ISO/IEC 27019 s'adresse aux entreprises et aux unités organisationnelles du secteur de l'énergie, y compris les entreprises d'approvisionnement, les gestionnaires de réseau, les producteurs d'énergie et les autres acteurs de la chaîne d'approvisionnement énergétique. 2. Protection des infrastructures critiques: la norme vise à protéger les infrastructures critiques du secteur de l'énergie contre diverses menaces, y compris les cyberattaques. Elle contribue à garantir la stabilité et la fiabilité du réseau électrique. 3. Application de la norme ISO/IEC 27001: la norme ISO/IEC 27019 s'appuie sur les principes et les exigences de la norme internationale ISO/IEC 27001 relative aux systèmes de gestion de la sécurité de l'information (ISMS). Elle garantit que les entreprises et les unités organisationnelles du secteur de l'énergie prennent en compte les exigences spécifiques de la branche et respectent les meilleures pratiques en matière de sécurité de l'information. 4. Contrôles et mesures de sécurité: la norme ISO/IEC 27019 contient une liste de contrôles et de mesures de sécurité pertinents dans les domaines du contrôle d'accès, du cryptage, de la protection des installations et des systèmes, de la gestion des incidents et d'autres aspects de la sécurité de l'information. 5. Approche basée sur les risques: la norme encourage l'application d'une approche basée sur les risques pour identifier, évaluer et traiter les risques de sécurité dans le secteur de l'énergie. <p>Elle aide les entreprises et les unités organisationnelles du secteur de l'énergie à renforcer la sécurité de leurs systèmes d'information et à accroître leur résilience face aux cybermenaces. C'est essentiel car le secteur de l'énergie est une infrastructure critique qui a un impact considérable sur la société et l'économie. Grâce à la norme ISO/IEC 27019, les entreprises et les unités organisationnelles du secteur de l'énergie peuvent s'assurer qu'elles appliquent des mesures appropriées pour sécuriser leurs systèmes informatiques et leurs données dans un paysage de menaces en constante évolution.</p>
Code de réseau de l'ENISA sur la cybersécurité	<p>Le code de réseau de l'ENISA sur la sécurité vise à créer une norme européenne pour la cybersécurité des flux électriques transfrontaliers. Il contient des règles pour l'évaluation des cyberrisques, des exigences minimales communes, la certification des produits et services de cybersécurité, la surveillance, le reporting et la gestion de crise. Ce code de réseau définit clairement les tâches et les responsabilités des différents acteurs pour chaque activité.</p>





Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.



Anhang E: Outils de l'AES pour accroître la résilience des TIC

E.0 Outil «VSE & BFE Assessment-Tool NIST CSF 1.1 ++» y compris SoA, maturités selon l'OFEN et aides à la mise en œuvre



En collaboration avec le groupe de travail chargé de l'augmentation de la résilience des TIC, l'OFEN et l'AES ont développé un outil qui aide les entreprises et les unités organisationnelles de la branche électrique à accroître la résilience des TIC et à mettre en œuvre les mesures nécessaires.



Les formations de l'AES expliquent précisément comment utiliser cet outil.

E.0.1 Objectif et but

L'outil «VSE & BFE Assessment-Tool NIST CSF 1.1 ++» aide les membres de l'AES à renforcer la résilience des TIC. Il peut être configuré en fonction des spécifications du profil de protection (défini dans l'OApEI) pour chaque entreprise et unité organisationnelle. Ainsi, l'ensemble des exigences selon les niveaux de protection de l'OApEI sont visibles.



Les commentaires détaillés aident l'utilisateur en lui fournissant des informations supplémentaires utiles.

E.0.2 Onglet «Document Owner & History» (propriétaire et historique du document)

L'onglet «Document Owner & History» donne des renseignements pertinents sur les entreprises ou les unités organisationnelles. En outre, des informations peuvent être fournies sur l'identification précise, la révision, la classification, le champ d'application et l'historique du document.

E.0.3 Onglet «Assessment NIST CSF 1.1 ++» (évaluation NIST CSF 1.1 ++)

VSE & BFE Assessment-Tool NIST CSF 1.1 ++				Organisation protection niveau according to BFE:												Company: Strom AG			
incl. SoA, maturity by BFE, need for action and parameters for prioritization				Grid operator area: <div><div>A</div><div>> 450 GWh/year</div></div> <div><div>A</div><div>> 800 MW</div></div>												Area of validity: Entire Strom AG Group with subsidiaries			
																Status: In Progress			
Function Funktions- Thema	Category Kategorie Category Catégorie	Checkpoints (Subcategory) Kontrollpunkte (Subkategorie) Tâches (Subcatégorie) Missions (Subcatégorie)	Priority Rang BFE	Sating / Bewertung / Application / Soma												Informative References Referenzen Références Referenzen			
				Grid operator area SoA & n/a Comments Commentaires Commentaires				Energy producer area SoA & n/a Comments Commentaires Commentaires				General IT area (Baseline) SoA & n/a Comments Commentaires Commentaires							
				Applicability	Present	Maturity by BFE	Target	Need for action	Applicability	Present	Maturity by BFE	Target	Need for action	Applicability	Present	Target			
Asset Management (ID AM) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are	ID AM-1 Develop an inventory of all of the software platform services and applications within your organization. Erstellen Sie einen Inventar aller Software-Plattformen und -anwendungen innerhalb Ihrer Organisation. Développer un processus d'inventaire logiciel afin de maintenir un recensement exhaustif de vos équipements TIC (Assets). Définir une procédure qui garantisse la création permanente d'un inventaire complet des outils informatiques de votre TIC (Assets).	ID AM-1 Develop an inventory of all of the software platform services and applications within your organization. Erstellen Sie einen Inventar aller Software-Plattformen und -anwendungen innerhalb Ihrer Organisation. Développer un processus d'inventaire logiciel afin de maintenir un recensement exhaustif de vos équipements TIC (Assets). Définir une procédure qui garantisse la création permanente d'un inventaire complet des outils informatiques de votre TIC (Assets).	High	-	0	4	0	-	0	4	0	-	0	4	0	0	VSE-BFE: Zusammenstellung NIST SP 800-53 Rev. 5, CIS und CSC (inkl. SoA) VSE-Leitfaden: Kapitel 1 VSE-Checkliste ISA 62443-3-3:2009 4.2.34 ISA 62443-3-3:2009 SP 7.8 ISO/IEC 27001:2005 7.1.1.1.2 ISO/IEC 27001:2022 A.5.3 BSI-Standard 100-2 Kapitel 4.2 M.2.2.5 COBIT 5.01.01, BA09.02 NISTIR CF-002		
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
Asset Management (ID AM) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are	ID AM-2 Produce an inventory of all of the software platform services and applications within your organization. Erstellen Sie einen Inventar aller Software-Plattformen und -anwendungen innerhalb Ihrer Organisation. Produire un inventaire de toutes les plateformes, licences et applications logicielles dans votre entreprise. Inventariser toutes les plateformes, licences et applications logicielles dans votre entreprise. Inventarizzare tutte le piattaforme e applicazioni di software appartenenti all'organizzazione.	ID AM-2 Produce an inventory of all of the software platform services and applications within your organization. Erstellen Sie einen Inventar aller Software-Plattformen und -anwendungen innerhalb Ihrer Organisation. Produire un inventaire de toutes les plateformes, licences et applications logicielles dans votre entreprise. Inventariser toutes les plateformes, licences et applications logicielles dans votre entreprise. Inventarizzare tutte le piattaforme e applicazioni di software appartenenti all'organizzazione.	High	-	0	4	0	-	0	4	0	-	0	4	0	VSE-BFE: Zusammenstellung NIST SP 800-53 Rev. 5, CIS und CSC (inkl. SoA) VSE-Leitfaden: Kapitel 1 VSE-Checkliste ISA 62443-3-3:2009 4.2.34 ISA 62443-3-3:2009 SP 7.8 ISO/IEC 27001:2005 A.5.3.02 ISO/IEC 27001:2022 7.1.1.1.2 BSI-Standard 100-2 Kapitel 4.2 M.2.2.5 COBIT 5.01.01, BA09.02, BA09.05 NISTIR CF-002			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
Asset Management (ID AM) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are	ID AM-3 Protect the organization's information assets. Schützen Sie die Informationen der Organisation. Protéger les données de l'entreprise. Proteggere i dati dell'organizzazione.	ID AM-3 Protect the organization's information assets. Schützen Sie die Informationen der Organisation. Protéger les données de l'entreprise. Proteggere i dati dell'organizzazione.	High	-	0	4	0	-	0	4	0	-	0	4	0	VSE-BFE: Zusammenstellung NIST SP 800-53 Rev. 5, CIS und CSC (inkl. SoA) VSE-Leitfaden: Kapitel 1 VSE-Checkliste ISA 62443-3-3:2009 4.2.34 ISA 62443-3-3:2009 SP 7.8 ISO/IEC 27001:2005 A.5.3.02 ISO/IEC 27001:2022 7.1.1.1.2 BSI-Standard 100-2 Kapitel 4.2 M.2.2.5 COBIT 5.01.01, BA09.02, BA09.05 NISTIR CF-002			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			
				-	0	4	0	-	0	4	0	-	0	4	0	0			

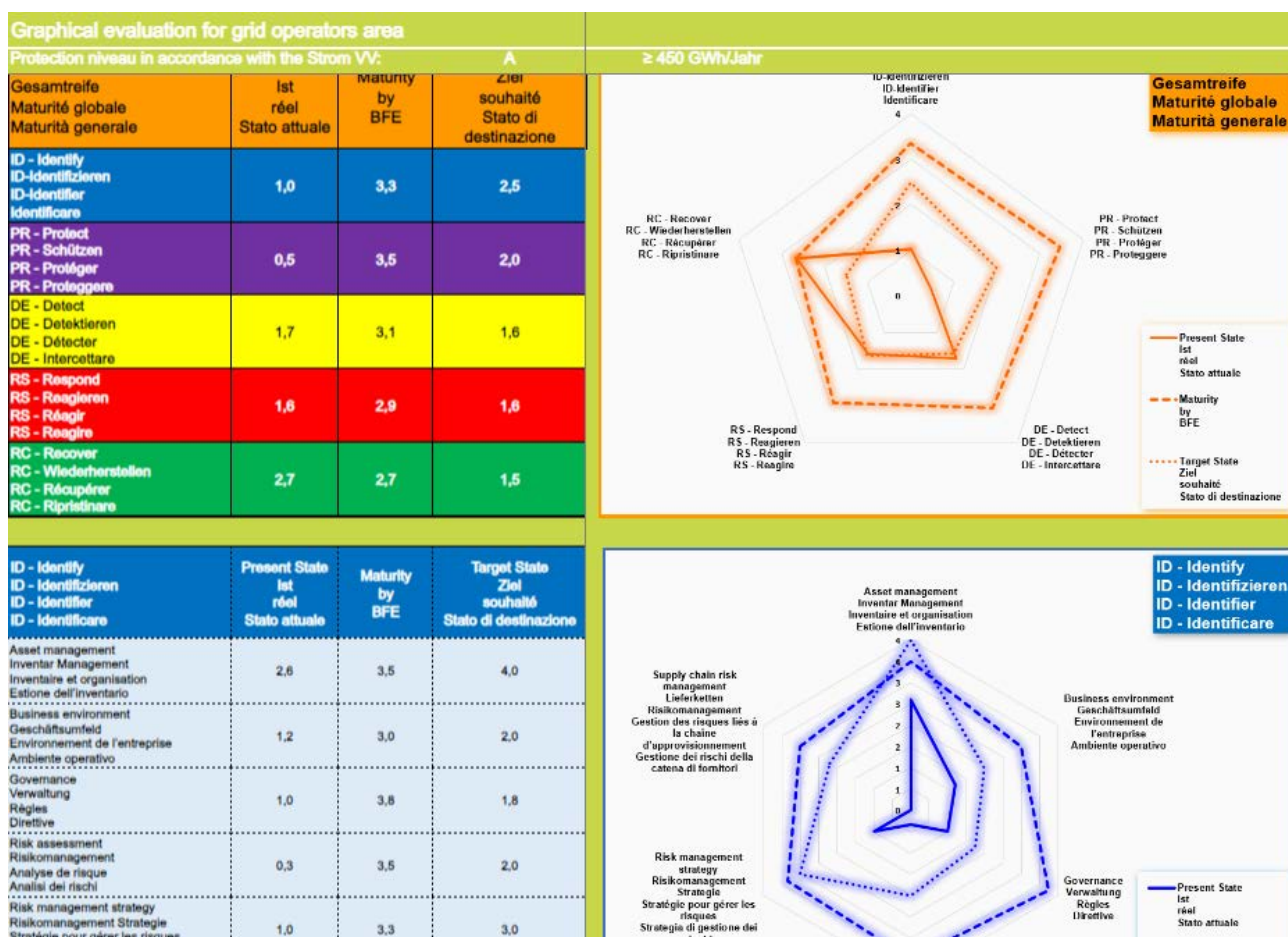
La structure et les fonctions peuvent être résumées de la manière suivante:

- Basé sur le cadre de cybersécurité CFS 1.1 du NIST et l'outil d'évaluation de la norme minimale pour les TIC de l'OFAE
- L'évaluation est divisée en trois parties, qui peuvent être traitées séparément:
 - «Grid operator area» (zone du gestionnaire de réseau)
 - «Energy producer area» (zone de production et de stockage d'énergie)
 - «General IT area» (zone pour l'informatique générale, principalement les zones de bureau ou de business, considérée comme base de référence pour l'ensemble de l'environnement OT/IT)
- L'utilisateur peut sélectionner le niveau de protection qui lui est attribué conformément à l'OApEI.



- Les priorités et les maturités selon les prescriptions de l'OApEI sont indiquées en fonction du choix du niveau de protection.
- L'applicabilité peut être représentée.
- Le niveau actuel de la maturité peut être représenté (auto-évaluation).
- Les maturités souhaitées peuvent être représentées.
- Dans les «Commentaires», il est possible de saisir des commentaires sur les différentes tâches, par exemple la justification de la non-applicabilité.
- Sous «Need for action», l'utilisateur voit la différence entre la maturité prescrite et la maturité réelle. Cette présentation est pensée comme une aide à la priorisation des mesures.
- Les «Quick Wins» indiquent à l'utilisateur, par le biais d'un code couleurs, les domaines dans lesquels les spécialistes de la Task Force Cybersécurité de l'AES estiment que des succès rapides peuvent être obtenus (mesures peu coûteuses et à fort impact)
- Références: affiche des références à des documents supplémentaires ou à des normes et spécifications

E.0.4 Évaluation graphique dans les onglets «Results» (résultats)



Les évaluations graphiques présentent les maturités réelles et souhaitées. Elles permettent à l'utilisateur d'identifier plus facilement les écarts les plus importants entre les différentes maturités. Il existe une évaluation pour l'ensemble du framework ainsi que pour les fonctions individuelles.

E.0.5 Onglet «Assistance Information» (informations d'assistance)

Cet onglet contient toutes les explications et précisions nécessaires concernant les différents points variables de l'onglet «Assessment NIST CSF 1.1 ++» (évaluation NIST CSF 1.1 ++).



BFE & VSE (Branche)
Assessment Tool ++
(inkl. Need for Action
und Quick Wins)

spéciale NIST 800-53 révision 5 CSA Cloud Controls Matrix v3.0.1 et CIS Critical Security Controls v8.



—

La structure et les fonctions de ces onglets peuvent être résumées de la manière suivante:

- Basé sur le cadre de cybersécurité CFS 1.1 du NIST et l'outil d'évaluation de la norme minimale pour les TIC de l'OFAE
- Aux tâches selon le CSF NIST 1.1 correspondent les mesures de la publication spéciale NIST 800-53 révision 5, CSA Cloud Controls Matrix v3.0.1 et CIS Critical Security Controls v8.
- Pour la publication spéciale NIST 800-53 révision 5, CSA Cloud Controls Matrix v3.0.1 et CIS Critical Security Controls v8, le numéro, le titre et la description de chaque mesure sont visibles.
- L'évaluation est divisée en trois parties, qui peuvent être traitées séparément:
 - «Grid operator area» (zone du gestionnaire de réseau)
 - «Energy producer area» (zone de production et de stockage d'énergie)
 - «General IT area» (zone pour l'informatique générale, principalement les zones de bureau ou de business, considérée comme base de référence pour l'ensemble de l'environnement OT/IT)
- La partie «Grid operator area» est divisé en deux catégories partielles: «Grid Domain Core» avec les sous-catégories partielles «Grid Scada» (système de contrôle-commande), «Grid Load Control» (gestion de la demande) et «Grid Field System» (systèmes de terrain, postes de couplage, installations de transformation, etc.), et la catégorie partielle «Grid Domain Support & and Management». Ces catégories partielles sont automatiquement regroupées sous «Grid over all». Cette division offre à l'utilisateur une plus grande granularité.
- La partie «Energy producer area» est divisée en deux catégories partielles: «Energy Domain Core» avec les sous-catégories partielles «Energy producer SCADA» (système de contrôle-commande), «Energy Management System» (systèmes de gestion de l'énergie) et «Energy producer Field System» (systèmes de terrain, centrales électriques, centrales de stockage, etc.), et la catégorie partielle «Energy producer Domain Support & et Management». Ces catégories partielles sont automatiquement regroupées sous «Energy producer over all». Cette division offre à l'utilisateur une plus grande granularité.
- L'utilisateur peut sélectionner le niveau de protection qui lui est attribué conformément à l'OApEI, les mesures à appliquer étant alors automatiquement affichées ou grisées.
- Les maturités au niveau des tâches du CSF NIST 1.1 selon les spécifications de l'ordonnance sur l'électricité sont indiquées en fonction du choix du niveau de protection
- L'applicabilité peut être représentée.
- Le niveau actuel de la maturité peut être représenté (auto-évaluation).
- Les maturités souhaitées peuvent être représentées.
- Dans la partie «SoA, n/a or Evidenz», il est possible de saisir des commentaires sur les différentes tâches, par exemple la justification de la non-applicabilité ou les preuves.

E.1.4 Onglet «Assistance Information» (informations d'assistance)

Cet onglet contient toutes les explications et précisions nécessaires concernant les différents points variables des onglets «All Functions» (toutes les fonctions), «IDENTIFY (ID)» (identifier), «PROTECT (PR)» (protéger), «DETECT (DE)» (détecter), «RESPOND (RE)» (répondre) et «RECOVER (RC)» (restaurer).

E.2 Outil AES CSF NIST 1.1 Mappage HoP

L'outil «VSE-Tool NIST CSF 1.1 HoP Mapping» aide l'utilisateur à créer les documents HoP. Dans cet outil, les différentes tâches du CSF NIST 1.1 sont attribués aux documents correspondants dans le HoP. Cela facilite également la vérification par l'utilisateur.

E.2.1 Onglet «Document Owner & History» (propriétaire et historique du document)

L'onglet «Document Owner & History» donne des renseignements pertinents sur les entreprises ou les unités organisationnelles. En outre, des informations peuvent être fournies sur l'identification précise, la révision, la classification, le champ d'application et l'historique du document.



E.2.2 Onglet «All Function HoP» (toutes les fonctions HoP)

NIST Cyber Security Framework CSF 1.1			Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung
Function	Category	Checkpoints (Subkategorie)	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung	Identifizierung	Schutzbefähigung	Reaktionsfähigkeit	Wiederherstellung
IDENTIFY (ID)	Verständnis der Organisation (Asset Management)	Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
IDENTIFY (ID)	Verständnis der Organisation (Asset Management)	Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
IDENTIFY (ID)	Verständnis der Organisation (Asset Management)	Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																
		Identifizierung der Assets																																

Les différentes tâches selon la norme CSF NIST 1.1 peuvent être attribuées aux documents HoP.

E.3 Outil «VSE Assessment-Tool ISO27001 Annex A incl. Controls acc.to ISO27002»

En collaboration avec le groupe de travail chargé de l'augmentation de la résilience des TIC, l'OFEN et l'AES ont développé un outil destiné à aider intégralement les entreprises et les unités organisationnelles de la branche électrique à accroître la résilience des TIC et à mettre en œuvre les mesures nécessaires dans le cadre de l'annexe A de la norme ISO27001.



Les formations de l'AES expliquent précisément comment utiliser cet outil.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

E.3.1 Objectif et but

Si l'utilisateur le souhaite, l'outil d'évaluation AES ISO27001 Annex A incl. Controls acc.to ISO27002 peut aider les membres de l'AES à accroître la résilience des TIC. Cet outil couvre les différents contrôles de l'annexe A de la norme ISO 27001:2022.



Les commentaires détaillés aident l'utilisateur en lui fournissant des informations supplémentaires utiles.

E.3.2 Onglet «Document Owner & History» (propriétaire et historique du document)

L'onglet «Document Owner & History» donne des renseignements pertinents sur les entreprises ou les unités organisationnelles. En outre, des informations peuvent être fournies sur l'identification précise, la révision, la classification, le champ d'application et l'historique du document.



E.3.3 Onglet «Assessment Tool ISO 27001» (outil d'évaluation ISO 27001)

VSE Assessment Tool ISO27001:2022 Annex A					Organisation protection niveau according to BFE:										Company: Strom AG																			
Grid operator area					Grid operator area										Energy producer area										Area of validity: Entire Strom AG Group with subsidiaries									
Energy producer area					Energy producer area										Status: In Progress																			
Grid operator area					Energy producer area										General IT area (Baseline)																			
SoA					SoA										SoA																			
Present					Present										Present																			
Target					Target										Target																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			
Comments					Comments										Comments																			

Les évaluations graphiques présentent les maturités réelles et souhaitées. Elles permettent à l'utilisateur d'identifier plus facilement les écarts les plus importants entre les différentes maturités.

E.3.5 Onglet «Assistance Information» (informations d'assistance)

Cet onglet contient toutes les explications et précisions nécessaires concernant les différents points variables de l'onglet «Assessment Tool ISO 27001» (outil d'évaluation ISO 27001).

E.4 Outil «VSE Assessment-Tool ISO27001 ISMS-Goals incl. HoP-Mapping»

En collaboration avec le groupe de travail chargé de l'augmentation de la résilience des TIC, l'OFEN et l'AES ont développé un outil qui aide les entreprises et les unités organisationnelles de la branche électrique lors de l'introduction de l'ISMS. Il couvre les 52 objectifs visant une mise en œuvre réussie.



Les formations de l'AES expliquent précisément comment utiliser cet outil.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

E.4.1 Objectif et but

L'outil d'évaluation «VSE Assessment-Tool ISO27001 ISMS-Goals incl. HoP-Mapping» aide les membres de l'AES à renforcer la résilience des TIC. Il soutient l'utilisateur dans la mise en œuvre de l'ISMS au sein de l'entreprise ou des unités organisationnelles. Il permet également d'attribuer des points individuels au HoP du SGI.



Les commentaires détaillés aident l'utilisateur en lui fournissant des informations supplémentaires utiles.

E.4.2 Onglet «Document Owner & History» (propriétaire et historique du document)

L'onglet «Document Owner & History» donne des renseignements pertinents sur les entreprises ou les unités organisationnelles. En outre, des informations peuvent être fournies sur l'identification précise, la révision, la classification, le champ d'application et l'historique du document.

E.4.3 Onglet «Assessment ISMS Goals» (évaluation des objectifs de l'ISMS)

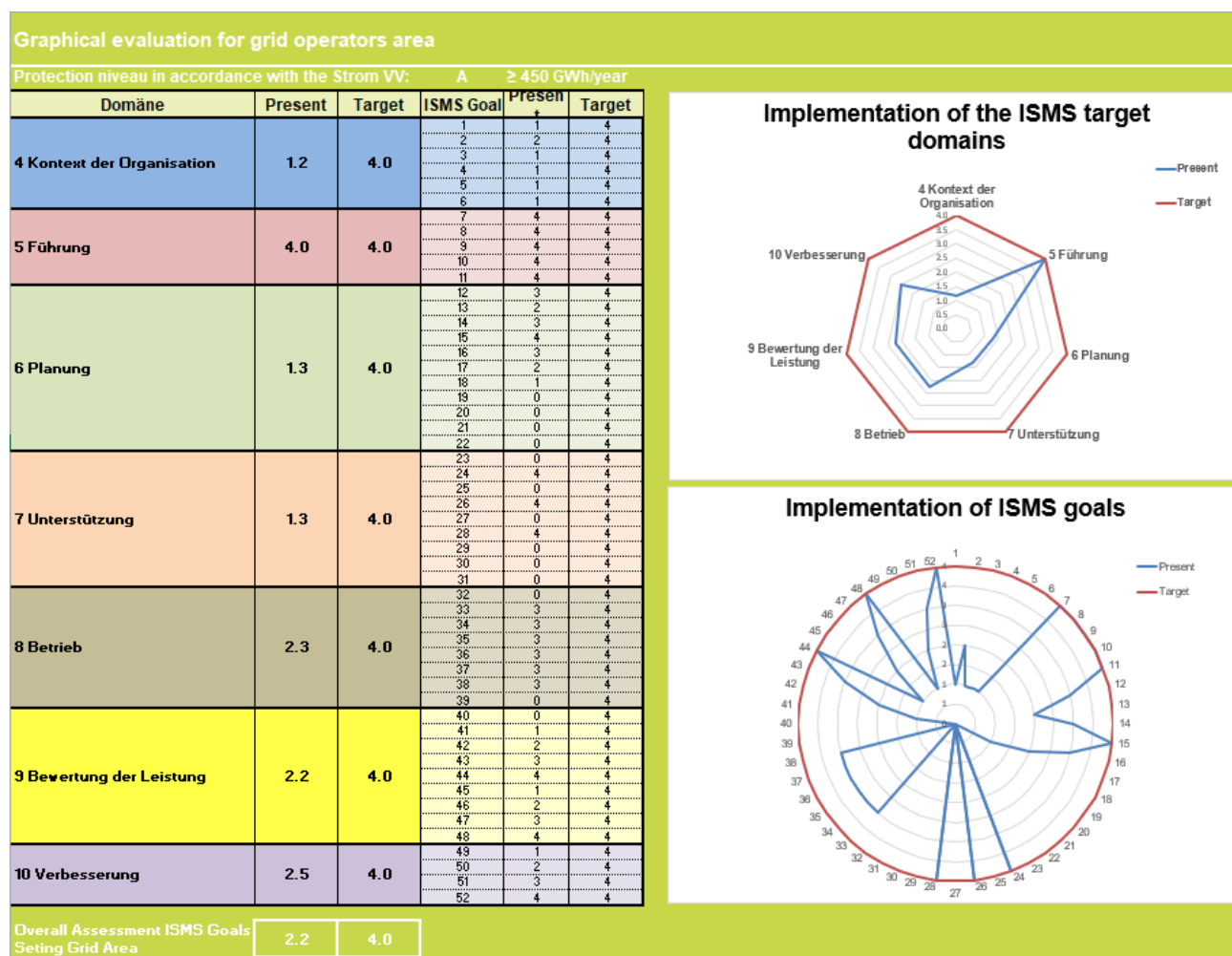
VSE Assessment Tool ISO27001 ISMS Goals				Organisation protection niveau according to BFE				Company: Strom AG				Mapping to HoP Documents (What needs to be created and when?) - Choose the HoP																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
This tool may only be used if you find a valid license for ISO 27001/27002 is available. (incl. VSE HoP-Mapping)				Grid operator area: A > 450 GWh/year Energy producer area: B < 100 MW and < 800 MW				Area of validity: Entire Strom AG Group with subsidiaries Status: In Progress				HoP-06 HoP-07 HoP-08 HoP-09 HoP-10 HoP-11 HoP-12 HoP-13 HoP-14 HoP-15 HoP-16 HoP-17																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
Domain Bereich Domaine Sector Sektor	Chapters Kapitel Chapitre Capítulo	Requirements Anforderungen Exigencias Requisitos Requisiti	Comments Anmerkungen Explanations Commentaires Spiegolung / Commenti	Grid operator area Grid operator area Energieproduktionsbereich Energieproduktionsbereich Energieproduktionsbereich	Energy producer area Energy producer area Energieproduktionsbereich Energieproduktionsbereich Energieproduktionsbereich	General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT area (Baseline)		General IT	

La structure et les fonctions peuvent être résumées de la manière suivante:



- Basé sur les domaines d'application, les chapitres et les exigences de la norme ISO 27001:2022
- Les 52 objectifs de l'ISMS sont présentés.
- Les priorités déterminées par l'utilisateur peuvent être définies.
- L'évaluation est divisée en trois parties, qui peuvent être traitées séparément:
 - «Grid operator area» (zone du gestionnaire de réseau)
 - «Energy producer area» (zone de production et de stockage d'énergie)
 - «General IT area» (zone pour l'informatique générale, principalement les zones de bureau ou de business, considérée comme base de référence pour l'ensemble de l'environnement OT/IT)
- L'utilisateur peut sélectionner le niveau de protection qui lui est attribué conformément à l'OApEI.
- Le niveau actuel de la maturité peut être représenté (auto-évaluation).
- Les maturités souhaitées peuvent être représentées.
- Dans les «Commentaires», il est possible de saisir notamment des informations complémentaires sur les commentaires des différents objectifs.
- Les références aux chapitres et aux références de la norme ISO 27001 sont indiquées.
- La référence aux fonctions du CSF NIST 1.1 est visible.
- Il est possible de procéder à l'attribution aux documents HoP relatifs au SGI.

E.4.4 Évaluation graphique dans l'onglet «Graphics ISMS Goals» (graphiques des objectifs de l'ISMS)



Les évaluations graphiques présentent les maturités réelles et souhaitées. Elles permettent à l'utilisateur d'identifier plus facilement les écarts les plus importants entre les différentes maturités. L'évaluation est exécutée pour les trois onglets «Grid», «Producer» et «IT-General».

E.4.5 Onglet «Assistance Information» (informations d'assistance)

Cet onglet contient toutes les explications et précisions nécessaires concernant les différents points variables de l'onglet «Assessment ISMS Goals» (évaluation des objectifs de l'ISMS).

E.5 Outil «VSE-Tool ISO27001 Annex A HoP-Mapping»

L'outil «VSE-Tool ISO27001 Annex A HoP-Mapping» aide l'utilisateur à créer les documents HoP. Dans cet outil, chaque tâche de la norme ISO 27001:2022 Annexe A est attribuée aux documents correspondants dans le HoP. Cela aide ensuite l'utilisateur à fournir des preuves.



Les outils, frameworks, normes, standards, guidelines et publications nécessitent très souvent une licence pour être utilisés et appliqués. Ainsi, ils ne peuvent être utilisés par les entreprises et les unités organisationnelles que si une licence valable est disponible. Cela vaut en particulier pour les normes SNV, ISO, ISA, EN, DIN, IEEE.

E.5.1 Onglet «Document Owner & History» (propriétaire et historique du document)

L'onglet «Document Owner & History» donne des renseignements pertinents sur les entreprises ou les unités organisationnelles. En outre, des informations peuvent être fournies sur l'identification précise, la révision, la classification, le champ d'application et l'historique du document.

E.5.2 Onglet «All Function HoP» (toutes les fonctions HoP)

VSE ISO27001:2022 Annex A Mapping to HoP					Mapping to HoP Documents (What needs to be located and where) – choose the letter (s) for a HoP –															
This document may only be used if a valid license for ISO 27001/27002 is available.					HoP-00	HoP-01-00	HoP-01-00-00	HoP-01-00-00-01	HoP-01-00-00-02	HoP-01-00-00-03	HoP-01-00-00-04	HoP-01-01	HoP-01-01-01	HoP-01-01-01-01	HoP-01-01-01-02	HoP-01-01-01-03	HoP-01-01-01-04	HoP-01-01-01-05	HoP-01-01-01-06	HoP-01-01-01-07
Suppl	Ref.	Title	Text	Purpose																
Checkpoint / Checkpunkt / Point de contrôle / Punto di controllo																				
5 Organisatorische Controls	A.5.1	Richtlinien für die Informationssicherheit	Informationssicherheitsrichtlinien und themenspezifische Richtlinien sollten definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem betreffenden Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.	Sicherstellung der fortwährenden Eignung, Angemessenheit und Wirksamkeit der Leitung und Unterstützung der Informationssicherheit in Übereinstimmung mit den geschäftlichen, rechtlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen.																
	A.5.2	Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit	Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit sollten entsprechend den Erfordernissen der Organisation definiert und zugewiesen werden.	Schaffung einer definierten, genehmigten und verständlichen Struktur für die Implementierung, den Betrieb und die Verwaltung der Informationssicherheit innerhalb der Organisation.																
	A.5.3	Trennung der Aufgaben	Sich widersprechende Aufgaben und Verantwortungsbereiche sollten getrennt werden.	Verringerung des Risikos von Betrug, Fehlen und Umgehung von Informationssicherheitskontrollen.																
	A.5.4	Verantwortlichkeiten des Managements	Die Geschäftsleitung sollte von allen Mitarbeitern verlangen, dass sie die Informationssicherheit in Übereinstimmung mit den festgelegten Informationssicherheitspolitiken und den themenspezifischen Richtlinien und Verfahren der Organisation anwenden.	Sicherstellen, dass das Management seine Rolle im Bereich der Informationssicherheit versteht und Massnahmen ergreift, die sicherstellen, dass alle Mitarbeiter ihre Verantwortung für die Informationssicherheit kennen und erfüllen.																
	A.5.5	Kontakt mit Behörden	Die Organisation sollte den Kontakt zu den zuständigen Behörden herstellen und aufrechterhalten.	Geschäftsführung eines angemessenen Informationsflusses in Bezug auf die Informationssicherheit zwischen der Organisation und den zuständigen Rechts-, Regulierungs- und Aufsichtsbehörden.																
	A.5.6	Kontakt mit speziellen Interessengruppen	Die Organisation soll Kontakte zu speziellen Interessengruppen oder anderen spezialisierten Sicherheitsforen und Berufsverbänden aufbauen und pflegen.	Sicherstellung eines angemessenen Informationsflusses in Bezug auf die Informationssicherheit.																
Informationen über Bedrohungen der																				

Les tâches individuelles selon la norme ISO 27001:2022 Annexe A peuvent être attribuées aux documents HoP.

E.6 Outil AES IMS Répertoire de documents HoP

L1: SoSt Punkte										L2: CEO Wirkung										L3: Group Director										L4: Unternehmens										L5: Abteilung, Kompetenz, Prozesse und Leistungen									
Strategische Wirkung										Strategische Wirkung										Strategische Wirkung										Strategische Wirkung										Strategische Wirkung									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name										Name									
Name										Name										Name										Name</																			

Le répertoire des documents IMS HoP de l'AES répertorie les documents nécessaires dans le système IMS-HoP. Tous les documents HoP nécessaires à l'exploitation complète d'un ISMS y sont répertoriés. Ce tableau permet de représenter l'état des documents HoP.



Anhang F: Description des prescriptions de la Maison des politiques Niveau 0 à 3

(1) Cette annexe présente les prescriptions selon les différents niveaux (0 à 3) de la Maison des politiques:

stratégique POURQUOI	Level	Documents de la Maison de la politique									
	0	HoP-00 Politique : la direction et l'activité entrepreneuriale									
tactique QUOI	1	HoP-01-00 Instruction : Directive sur la gestion des affaires									
	2	HoP-01-01 Directive : Sécurité de l'information & gestion de la sécurité de l'information ISM	HoP-01-02 Directive : Santé et sécurité au travail, sécurité physique et gestion de la continuité des opérations (GCA)								
opérationnel COMMENTE	3	HoP-01-01-01 Liens directrices : Cadre de la sécurité de l'information <ul style="list-style-type: none"> Objectifs généraux Principes Définitions Structure Organisation Champs d'action Délimitations 	HoP-01-01-02 Liens directrices : Champ d'application, mise en place et fonctionnement <ul style="list-style-type: none"> Champs d'application Structure Exploitation 	HoP-01-01-03 Liens directrices : Ligne de base dans le SMSI <ul style="list-style-type: none"> Exigences relatives à tous les domaines de la sécurité de l'information 	HoP-01-01-04 Liens directrices : Utilisateurs de valeurs d'information (politique de l'utilisateur) <ul style="list-style-type: none"> Exigences relatives à l'utilisation des systèmes, des appareils et des services 	HoP-01-00-00 Liens directrices : Systèmes de gestion intégrés IMS <ul style="list-style-type: none"> Contexte de l'organisation Leadership et engagement Pratiques de planification Audits Documentation 	HoP-01-02-01 Liens directrices : Sécurité au travail et protection de la santé <ul style="list-style-type: none"> Rôles et responsabilités Planification d'initiatives en matière de santé et de sécurité Exploitation Exigences 	HoP-01-02-02 Liens directrices : Sécurité physique <ul style="list-style-type: none"> Rôles et responsabilités Planification d'initiatives de gestion de la sécurité physique Exploitation Exigences 	HoP-01-02-03 Liens directrices : Gestion de la continuité des opérations (BCM) <ul style="list-style-type: none"> Rôles et responsabilités Planification d'initiatives de gestion de la sécurité physique Exploitation Exigences 	HoP-01-02-04 Liens directrices : Protection des données <ul style="list-style-type: none"> Rôles et responsabilités Objectifs Coordination aspect juridique Surveillance Mesures en cas de blessure 	HoP-01-02-05 Liens directrices : Crise-gestion <ul style="list-style-type: none"> Rôles et responsabilités Objectifs Planification des initiatives de KM Exploitation Exigences
	3	Instructions de travail : Organisation de la sécurité de l'information	Instructions de travail : KPI & Rapports	Instructions de travail : Objectifs 1 Instructions de travail : Objectifs 2 Instructions de travail : Objectifs 3 Instructions de travail : Objectifs n	Instructions de travail : Utilisation d'appareils mobiles Instructions de travail : Utilisation des actifs OT	Instructions de travail : Maison du Instructions de travail : Maison de la Instructions de travail : Audits Instructions de travail : Contrôle des documents	Instructions de travail : Mgmt Incident dans le domaine de la santé et de la Instructions de travail : Objectifs n	Instructions de travail : Incident Mgmt dans le domaine de la sécurité Instructions de travail : Objectifs n	Instructions de travail : Instructions pour la BIA Instructions de travail : Objectifs n	Instructions de travail : Objectifs 1 Instructions de travail : Objectifs 2 Instructions de travail : Objectifs 3 Instructions de travail : Objectifs n	Instructions de travail : Instructions pour la gestion de crise Instructions de travail : Gestion Instructions de travail : Objectifs n

F.0 Maison des politiques au niveau 0: politique (conseil d'administration / direction du groupe)

Titre	Description du contenu
HoP-00 Politique de gestion et d'entrepreneuriat	Le document Politique de gestion et d'entrepreneuriat est un document concis et autoritaire, généralement publié par le conseil d'administration ou le niveau le plus élevé d'une entreprise. Il fournit des prescriptions ou des instructions spécifiques à la direction de l'entreprise sur les décisions, les directives, les mesures ou les principes stratégiques importants, qui sont en accord avec la vision du comité et la direction de l'entreprise. Celles-ci se concentrent généralement sur la direction de l'entreprise, les affaires à l'échelle de l'entreprise, la conformité, la gestion des risques et les grandes initiatives de l'entreprise. Elles permettent au comité de communiquer les attentes et objectifs stratégiques à l'équipe de direction. Des prescriptions stratégiques concernant la sécurité de l'information au sein de l'entreprise et des unités organisationnelles doivent être définies. Le conseil d'administration s'engage clairement en faveur de la sécurité de l'information au sein de l'entreprise et des unités organisationnelles.

F.1 Maison des politiques au niveau 1: instructions et directives (direction, niveau C)

Titre	Description du contenu
HoP-01-00 Directive sur la gestion des affaires	La directive sur la gestion des affaires est un document concis et autoritaire publié par la direction d'une entreprise. Elle fournit des instructions spécifiques à l'entreprise et aux unités organisationnelles concernant les directives, les mesures ou les décisions stratégiques importantes, qui sont en accord avec la vision de la direction. Elle décrit la mise en œuvre des prescriptions dans la politique de la direction et se concentre généralement sur les affaires à l'échelle de l'entreprise, la conformité, la gestion des risques et les grandes initiatives de l'entreprise. Elle permet au comité de communiquer les attentes et objectifs stratégiques à l'équipe de direction. Des prescriptions claires concernant la sécurité de l'information au sein de l'entreprise et des unités organisationnelles doivent être définies par la direction. Celles-ci doivent être conformes aux exigences légales et réglementaires et à la politique de la direction.
HoP-01-01 Directive sur la sécurité de l'information et la gestion de la sécurité de l'information	Cette directive définit les objectifs et principes stratégiques fondamentaux à des fins de protection de l'information au sein d'une organisation. Elle définit le cadre de la mise en œuvre de mesures de sécurité et d'établissement d'un système de gestion de la sécurité de l'information. Le document souligne l'importance de la confidentialité, de l'intégrité et de la disponibilité des informations, ainsi que la nécessité d'une évaluation proactive des risques. Il définit également les responsabilités du personnel et met en avant le fait que l'amélioration continue de la sécurité de l'information fait partie intégrante de la culture d'entreprise. Au minimum, cette directive doit mentionner la



Titre	Description du contenu
	référence et le traitement de la sécurité de l'information avec le système de gestion de l'information correspondant, le système de gestion de la sécurité de l'information (ISMS) selon la norme ISO 27001 et les cadres à appliquer tels que le CSF NIST.
HoP-01-02 Directive sur la sécurité au travail, la protection de la santé, la sécurité physique et la continuité des opérations (BCM)	Cette directive établit des règles claires pour garantir un environnement de travail sûr et sain ainsi que la sécurité physique de notre organisation. L'objectif principal est de protéger la santé et la sécurité de l'ensemble du personnel et d'assurer la continuité des opérations. Il incombe à la direction de définir des normes et des directives afin de s'assurer que l'ensemble du personnel travaille dans un environnement sûr et sain. Cela inclut l'identification, l'évaluation et la minimisation des dangers et des risques sur le lieu de travail. Dans le domaine de la sécurité physique, des instructions claires sont données concernant la protection des ressources, des installations et des informations sensibles. Des mesures de contrôle d'accès, de surveillance et de préparation aux situations d'urgence sont définies afin de minimiser les accès non autorisés et les menaces potentielles. La gestion de la continuité des opérations (BCM) fait partie intégrante de cette directive. Elle établit des processus et des procédures afin de s'assurer qu'en cas de dysfonctionnement ou de catastrophe, les opérations peuvent être rétablies aussi rapidement que possible. Cela inclut la révision et la mise à jour régulières des plans d'urgence, ainsi que la formation du personnel afin de garantir une réponse efficace en cas d'urgence. Cette directive est contraignante pour l'ensemble des collaborateurs et collaboratrices et la direction se réserve le droit de prendre les mesures disciplinaires appropriées en cas de non-respect.
HoP-01-03 Directive sur la gestion des risques	Faisant office de document de base, cette directive définit les objectifs stratégiques, les principes et le cadre de gestion des risques au sein de l'entreprise et des unités organisationnelles. Elle fournit des lignes directrices sur la manière d'identifier, d'évaluer et de traiter les risques afin de protéger les objectifs commerciaux, d'assurer la conformité et d'établir une culture du risque efficace.

F.2 Maison des politiques au niveau 2: directives et lignes directrices (CISO, CRO, DPO)

Titre	Description
HoP-01-00-00 Directive Systèmes de gestion intégrés (SGI)	Cette directive définit les objectifs et principes stratégiques pour la mise en œuvre et le fonctionnement d'un système de gestion intégrée au sein d'une organisation. Elle définit un cadre pour l'intégration de différents systèmes de gestion, y compris la qualité, l'environnement, la santé et la sécurité, et fournit des lignes directrices claires afin d'harmoniser les processus. Elle vise à accroître l'efficacité, à créer des synergies et à améliorer les performances globales de l'entreprise et des unités organisationnelles.
HoP-01-01-01 Directive domaine de la sécurité de l'information et de la gestion de la sécurité de l'information: Cadre de la sécurité de l'information	La directive relative au cadre de la sécurité de l'information esquisse des prescriptions, principes, champs d'action et normes de base afin de créer un cadre clair et cohérent pour la sécurité de l'information au sein de l'entreprise et des unités organisationnelles. Son objectif principal est d'établir des lignes directrices claires qui définissent la portée et les bases du développement et de la mise en œuvre du système de gestion de la sécurité de l'information (ISMS). Le document souligne l'importance d'une analyse contextuelle globale qui prend en compte les objectifs commerciaux, les influences externes et la nature des informations traitées. Sur cette base, le champ d'application de l'ISMS est déterminé et les exigences légales, réglementaires et commerciales pertinentes sont identifiées. Des responsabilités claires sont définies pour la mise en œuvre et le maintien de l'ISMS à différents niveaux de l'organisation. Cela inclut l'attribution de rôles et de responsabilités en matière de sécurité de l'information afin de s'assurer que l'ensemble des parties prenantes concernées sont impliquées de manière adaptée. Cette directive est contraignante pour l'ensemble du personnel et la direction se réserve le droit de prendre les mesures appropriées en cas de non-respect.
HoP-01-01-02: Directive domaine de la sécurité de l'information: champ d'application, mise en place et fonctionnement de l'ISMS	La directive relative au champ d'application, à la mise en place et à l'organisation du système de gestion de la sécurité de l'information (ISMS) établit des principes et des normes de base afin de fournir un cadre clair pour la mise en œuvre et la structuration de l'ISMS au sein de notre organisation. Son objectif principal est d'établir des lignes directrices claires qui définissent la portée de l'ISMS, sa structure et les responsabilités en matière de sécurité de l'information. La directive souligne l'importance d'une analyse approfondie du contexte organisationnel afin de déterminer avec précision le champ d'application de l'ISMS. Cela implique d'identifier les facteurs internes et externes susceptibles d'affecter la sécurité de l'information et de déterminer les domaines d'activité sur lesquels l'ISMS doit se concentrer. Des responsabilités et des rôles clairs sont définis pour la mise en place et le maintien de l'ISMS à différents niveaux de l'organisation. Cela inclut la définition de responsables de la sécurité et l'attribution de tâches spécifiques liées à la sécurité de l'information.
HoP-01-01-03 Directive domaine de la gestion de la sécurité de l'information: scénario de référence dans l'ISMS	La directive consacrée au scénario de référence en matière de sécurité de l'information dans le système de gestion de la sécurité de l'information (ISMS) esquisse des normes claires et fondamentales qui servent de point de départ à la mise en œuvre et au maintien de notre ISMS. Elle vise en priorité à créer un cadre cohérent et stable pour la sécurité de l'information dans l'ensemble de l'organisation. Elle souligne l'importance de l'identification et de la mise en œuvre des contrôles de sécurité du scénario de référence, qui sont considérés comme des exigences minimales pour garantir un niveau adéquat de sécurité de l'information. Les



Titre	Description
	principes fondamentaux tels que la confidentialité, l'intégrité et la disponibilité des informations sont pris en compte. Le scénario de référence sert de base pour tous les domaines de l'organisation et définit des exigences claires pour l'utilisation des informations sensibles. Cela inclut l'accès aux données, la protection contre les logiciels malveillants, la sécurisation des réseaux et la gestion des droits d'accès. La directive souligne également la nécessité de réexaminer et de mettre à jour régulièrement le scénario de référence afin de s'assurer qu'il est adapté à l'évolution des menaces et des exigences en matière de sécurité de l'information. La communication et la formation du personnel sur les normes en matière de scénario de référence sont également des éléments essentiels pour créer une compréhension et une conscience communes des exigences de sécurité.
HoP-01-01-04 Directive domaine de la sécurité de l'information: utilisateurs de valeurs d'information	La directive destinée aux utilisateurs dans le cadre d'un système de gestion de la sécurité de l'information (ISMS) définit des lignes directrices et des normes de bonne pratique claires pour l'ensemble du personnel afin de garantir une utilisation sûre des informations. Elle vise principalement à protéger la confidentialité, l'intégrité et la disponibilité des données tout en sensibilisant les collaborateurs et collaboratrices aux aspects liés à la sécurité. Elle souligne la responsabilité individuelle de chaque utilisateur dans la protection des informations sensibles et définit des attentes claires en matière de respect des directives et procédures relatives à la sécurité. Dans ce cadre, la gestion sécurisée des comptes utilisateurs, des mots de passe et des droits d'accès est un élément clé. Il est rappelé que le personnel est tenu de traiter les données d'accès confidentielles avec soin et de ne pas divulguer d'informations non autorisées. Parallèlement, des mesures de formation sont mises en place pour s'assurer que les collaborateurs et collaboratrices sont informés des dernières pratiques en matière de sécurité et sont en mesure d'identifier les attaques de phishing.
HoP-01-02-01 Directive domaine gestion de la sécurité et de la santé au travail: sécurité et santé au travail	La directive en matière de sécurité et de santé au travail au travail définit les principes et les normes de base pour garantir un environnement de travail sûr et sain au sein de notre organisation. Elle vise principalement à fournir des instructions et des lignes directrices claires afin de minimiser les risques potentiels au poste de travail et de protéger la santé et le bien-être du personnel. La directive souligne l'importance d'une identification et évaluation continues des risques au poste de travail et de la mise en œuvre de mesures préventives. L'objectif est de prévenir les accidents professionnels, de promouvoir la santé des collaborateurs et collaboratrices et d'assurer le respect des dispositions en vigueur. Des responsabilités claires sont définies pour la mise en œuvre des normes de sécurité à tous les niveaux de l'organisation. L'organisation définit des attentes claires en matière de formation du personnel afin de le sensibiliser aux risques de sécurité et d'encourager sa participation active aux mesures de sécurité.
HoP-01-02-02 Directive domaine gestion de la sécurité et de la santé au travail: sécurité physique	La directive relative à la sécurité physique définit les principes et normes de base pour protéger l'intégrité physique de nos ressources, les installations et les informations sensibles. Elle vise principalement à créer des lignes directrices claires afin de minimiser les menaces physiques et de garantir un environnement sûr pour notre personnel et nos actifs. Elle souligne l'importance d'une évaluation globale des risques, y compris l'identification des menaces potentielles pour la sécurité physique. L'objectif est de développer des mesures pour prévenir ou limiter les cambriolages, les vols, les catastrophes naturelles et autres menaces physiques. Des responsabilités claires sont définies pour la mise en œuvre des normes de sécurité physique à tous les niveaux de l'organisation, cela inclut le contrôle d'accès, les systèmes de surveillance et la préparation aux situations d'urgence afin de s'assurer que nos installations sont protégées de manière adaptée.
HoP-01-02-03 Directive domaine gestion de la sécurité et de la santé au travail: gestion de la continuité des opérations (BCM)	La directive relative à la gestion de la continuité des opérations (BCM) établit les principes et les normes de base pour s'assurer que notre organisation est en mesure de maintenir ses processus opérationnels critiques, même dans des conditions défavorables. Elle vise principalement à créer des lignes directrices claires afin de minimiser les perturbations et les interruptions de nos opérations et à permettre une reprise rapide en cas d'urgence. Elle souligne l'importance d'une évaluation globale des risques afin d'identifier les menaces et points faibles potentiels susceptibles de nuire à la continuité des opérations. L'objectif est d'élaborer des stratégies et des mesures pour minimiser ces risques et assurer la continuité des activités. Des responsabilités claires sont définies pour la mise en œuvre des normes BCM à tous les niveaux de l'organisation. Cela inclut l'élaboration de plans d'urgence, la formation du personnel et des exercices d'urgence réguliers afin de s'assurer que les collaborateurs et collaboratrices peuvent réagir efficacement à différents scénarios.
HoP-01-02-04 Directive domaine gestion de la sécurité et de la santé au travail: protection des données	La directive en matière de protection des données définit les principes et les normes de base pour garantir que les données personnelles sont protégées au sein de notre organisation conformément aux dispositions en la matière. Elle vise principalement à fournir des lignes directrices claires afin de garantir la confidentialité, l'intégrité et la disponibilité des données personnelles tout en respectant les droits et la vie privée des personnes concernées. Elle souligne l'importance d'un traitement rigoureux des données à caractère personnel, de leur collecte jusqu'à leur stockage et leur suppression. L'objectif est de s'assurer que seules les personnes autorisées ont accès à ces données et que des mesures de sécurité appropriées sont mises en œuvre pour empêcher tout accès non autorisé ou toute perte de données. Des responsabilités claires sont définies pour la mise en œuvre des normes de protection des données à tous les niveaux de l'organisation. Cela inclut la formation des collaborateurs et



Titre	Description
	collaboratrices en vue d'une sensibilisation aux pratiques de protection des données et la mise en place de mécanismes dans l'optique de garantir le respect des droits des personnes concernées en matière de protection des données. La directive doit également décrire la gestion des incidents liés aux données personnelles et définit des principes et normes clairs afin de garantir que tous les événements potentiels liés aux données personnelles au sein de notre organisation sont traités de manière efficace et appropriée. Son but est également de créer des lignes directrices claires afin qu'il soit possible de réagir rapidement aux violations de données ou aux incidents de sécurité, de préserver la confidentialité et l'intégrité des données personnelles et de respecter les exigences légales. La directive souligne l'importance d'une identification, d'une déclaration et d'une analyse rapides des incidents compromettant la protection des données. L'objectif est de minimiser l'impact potentiel sur les personnes concernées et l'organisation tout en garantissant la transparence en matière d'incidents de sécurité. Des responsabilités claires sont définies pour la gestion des incidents à tous les niveaux de l'organisation. Cela implique la création d'équipes de réponse aux incidents, responsables de la gestion coordonnée des incidents compromettant la protection des données. La directive définit également des mesures pour informer rapidement les personnes concernées, les autorités de contrôle et les autres parties concernées.
HoP-01-02-05 Directive domaine gestion de la sécurité et de la santé au travail: gestion des situations d'urgence	La directive relative à la gestion des situations d'urgence esquisse les principes et normes de base pour assurer une approche structurée et efficace des situations de crise au sein de notre organisation. Elle vise principalement à fournir des lignes directrices claires afin d'assurer une réponse immédiate et coordonnée aux événements imprévus qui pourraient entraver la continuité des activités et la réputation de l'organisation. La directive souligne la nécessité d'une analyse proactive des risques afin d'identifier les scénarios de crise potentiels. L'objectif est d'attribuer de manière univoque les responsabilités en matière de gestion des urgences et d'identifier les ressources qui peuvent être mobilisées en cas de crise. Des structures et des responsabilités de communication claires sont définies afin de garantir que toutes les parties concernées sont correctement informées. L'accent est également mis sur la création d'une équipe de gestion des situations d'urgence chargée de coordonner et de mettre en œuvre la réponse aux crises. Cette directive est contraignante pour l'ensemble du personnel et la direction se réserve le droit de prendre les mesures appropriées en cas de non-respect.

F.3 Maison des politiques au niveau 3: guides de travail et instructions (ISO, ISC et équipe de cybersécurité)

Titre	Description
HoP-01-00-00-01 Instructions de travail domaine SGI: Maison des processus	<p>Les instructions de travail pour le domaine des systèmes de gestion intégrés (SGI) dans le contexte de la Maison des processus fournissent un guide complet pour la conception et l'optimisation des processus au sein d'un SGI. La Maison des processus est un concept qui structure es différents aspects du paysage des processus et les intègre dans une organisation.</p> <p>Le champ d'application de ces instructions définit clairement les processus, services et activités pris en compte au sein du SGI. Cela crée une base claire pour l'optimisation des processus. La structure de la Maison des processus est expliquée en détail, y compris la hiérarchie des processus, sous-processus et activités. Il s'agit d'identifier et de décrire les interfaces entre les différents domaines de processus.</p> <p>Les instructions de travail donnent des consignes précises sur la conception des processus au sein de la Maison des processus. Cela implique la définition d'objectifs de processus, la détermination de responsabilités et de pouvoirs, ainsi que la mise en œuvre de mesures de surveillance et de contrôle du processus. L'intégration des normes de qualité et l'application des meilleures pratiques sont également prises en compte.</p> <p>Les consignes relatives à l'amélioration continue des processus constituent un élément essentiel de ces instructions de travail. Cela comprend une révision et une mise à jour régulières du paysage des processus afin de répondre à l'évolution des exigences et des conditions commerciales. Le document contient également des étapes claires pour les audits et les vérifications dans un souci d'efficacité des processus.</p> <p>Dans l'ensemble, les instructions de travail pour le domaine SGI: Maison des processus offrent une aide globale à la conception, à la mise en œuvre et l'amélioration continue réussies des processus au sein d'un système de gestion intégré.</p>
HoP-01-00-00-02 Instructions de travail domaine SGI: Maison des politiques	<p>Les instructions de travail pour le domaine SGI: Maison des politiques offrent une aide globale à la conception, à la mise en œuvre et au maintien des politiques, des directives et des instructions de travail au sein d'un système de gestion intégré (SGI). Ici, le terme «Maison des politiques» fait référence à la structure et à la gestion des politiques, des directives et des instructions de travail au sein d'une organisation.</p> <p>Les instructions de travail commencent par définir clairement le champ d'application afin de déterminer quelles politiques, directives et instructions de travail sont prises en compte au sein du SGI. Cela fournit un point de départ clair pour la création et la gestion des politiques, directives et instructions de travail. La structure de la Maison des politiques est expliquée en détail. Cela implique</p>



Titre	Description
	<p>la hiérarchie des politiques, directives et instructions de travail, l'identification des politiques, directives, directives et instructions de travail clés, ainsi que leur contexte et leurs interdépendances. Les instructions de travail fournissent des consignes claires sur la manière de catégoriser et d'organiser les politiques, directives et instructions de travail afin d'assurer une gestion efficace. Elles offrent des étapes détaillées pour la création de politiques, de directives et d'instructions de travail. Cela implique la définition de responsabilités, de domaines d'application, de détails de mise en œuvre et d'objectifs clairs. L'intégration des exigences légales, des normes et des meilleures pratiques est également prise en compte. Elles contiennent des politiques, des directives et des instructions de travail claires pour la mise en œuvre de celles-ci au sein de l'organisation. Cela implique la formation, la sensibilisation et des stratégies de communication pour s'assurer que l'ensemble des parties prenantes concernées comprennent et respectent les politiques, les directives et les instructions de travail. Les consignes relatives à la révision et à la mise à jour régulières des politiques, directives et instructions de travail constituent une partie essentielle de ce document. Cela garantit l'adaptation de l'ensemble à l'évolution des exigences et des facteurs externes. Les instructions fournissent des indications claires pour la documentation et la conservation des politiques, des directives et des instructions de travail. Cela inclut la définition des responsabilités pour la mise à jour des politiques, directives et instructions de travail, ainsi que l'accès et la disponibilité pour les parties concernées. Dans l'ensemble, les instructions de travail pour le domaine SGI: Maison des politiques offre une aide globale et axée sur la pratique à l'élaboration, à la mise en œuvre et à la mise à jour des politiques, des directives et des instructions de travail au sein d'un système de gestion intégré.</p>
<p>HoP-01-00-00-03 Instructions de travail domaine SGI: maîtrise des documents</p>	<p>Les instructions de travail dans le domaine de la sécurité de l'information pour la maîtrise des documents définissent les étapes et les principes essentiels pour garantir une création, une approbation, une mise à jour et un archivage en bonne et due forme de l'ensemble des documents pertinents relatifs à la sécurité de l'information. Elles visent à fournir des lignes directrices claires afin d'assurer l'intégrité et l'actualité des documents liés à la sécurité. Elles soulignent la nécessité d'une maîtrise structurée des documents, garantissant que toutes les informations pertinentes sont facilement accessibles et que les versions les plus récentes sont utilisées. Elles comprennent des processus clairs pour la création de nouveaux documents, la révision par des parties compétentes, l'approbation formelle et une mise à jour régulière en fonction de l'évolution des exigences. Des responsabilités claires sont définies pour la mise en œuvre de la maîtrise des documents à différents niveaux de l'organisation. Cela implique la désignation de responsables pour les différentes phases du cycle de vie des documents afin de garantir le respect systématique des procédures établies.</p>
<p>HoP-01-00-00-04 Instructions de travail domaine SGI: audits</p>	<p>Les instructions de travail dans le domaine de la sécurité de l'information pour les audits définissent les principes et étapes de base permettant de s'assurer que les audits sont réalisés de manière efficace, systématique et ciblée dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires permettant un examen régulier de l'ensemble des aspects pertinents de la sécurité de l'information afin de garantir le respect des normes et directives. Elles soulignent l'importance d'une directive d'audit globale de la sécurité de l'information. Il s'agit de définir des processus clairs pour la planification des audits, l'identification des contrôles de sécurité à vérifier, la réalisation des audits ainsi que l'établissement des rapports et le suivi des résultats. Des responsabilités claires sont définies pour la mise en œuvre des directives d'audit à différents niveaux de l'organisation. Cela implique l'identification de responsables d'audit, d'auditeurs internes et de personnes de contact dans les secteurs d'activité concernés. Des mesures de formation sont également prévues pour s'assurer que le personnel comprenne l'importance des audits et coopèrent avec les équipes d'audit si nécessaire.</p>
<p>HoP-01-01-01-01 Instructions de travail domaine SGI: organisation de la sécurité de l'information</p>	<p>Les instructions de travail dans le domaine de la sécurité de l'information concernant la structure organisationnelle décrivent en détail les aspects structurels nécessaires à une sécurité de l'information efficace au sein d'une entreprise et de ses unités organisationnelles. Elles commencent par définir le champ d'application afin de déterminer quels domaines et processus sont couverts par les mesures de sécurité. Il s'agit également de formuler clairement les objectifs afin de s'assurer que l'organisation atteint ses objectifs de sécurité spécifiques. La définition des responsabilités et des rôles dans le contexte de la sécurité de l'information est un élément central. Cela implique la désignation de responsables de la sécurité, de personnes chargées de la sécurité et d'autres rôles pertinents afin de définir des compétences claires. Les instructions de travail expliquent comment les tâches et les responsabilités en matière de sécurité de l'information sont intégrées dans la structure organisationnelle existante. Cela nécessite la coopération avec d'autres services et la mise en place d'une hiérarchie claire pour les questions de sécurité. Elles décrivent les procédures de rapport et les canaux de communication des informations relatives à la sécurité au sein de l'organisation. Cela assure une communication efficace entre les responsables de la sécurité et les autres collaborateurs et collaboratrices. Le document insiste sur la nécessité d'une formation et d'une sensibilisation en cas de modification des rôles ou des responsabilités des employés. Ceci est particulièrement important pour s'assurer que les nouvelles tâches sont effectuées en conformité avec les directives de sécurité. Les instructions définissent la manière dont les directives de sécurité doivent être appliquées au sein de l'entreprise et des unités organisationnelles. Cela peut inclure l'intégration de telles directives dans les processus de travail existants, ainsi que la mise en œuvre de mécanismes de contrôle. Des évaluations régulières de la structure organisationnelle de la sécurité de l'information sont prévues. Cela permet de s'adapter</p>



Titre	Description
	en permanence à l'évolution des menaces et des exigences et de s'assurer que la structure organisationnelle reste efficace. Les instructions de travail dans le domaine de la sécurité de l'information concernant la structure organisationnelle servent de guide afin de garantir la définition claire, l'intégration et l'application des aspects organisationnels de la sécurité de l'information.
HoP-01-01-02-01 Instructions de travail domaine ISMS: indicateurs clés de performance (KPI) et rapports	Les instructions de travail dans le domaine de la sécurité de l'information pour les indicateurs clés de performance (KPI) définissent les étapes et les principes essentiels permettant de développer, de mettre en œuvre et de surveiller des indicateurs de performance efficaces qui mesurent l'efficacité du système de gestion de la sécurité de l'information (ISMS). Elles visent principalement à fournir des lignes directrices claires dans le but d'identifier des KPI pertinents qui reflètent la réalisation des objectifs et les performances en matière de sécurité de l'information. Elles mettent en avant l'importance d'une analyse globale afin d'identifier les KPI pertinents qui peuvent quantifier les progrès par rapport aux objectifs et normes de sécurité définis. Cela comprend la définition d'indicateurs clairs et mesurables reflétant les performances dans le contexte de la sécurité de l'information. Des responsabilités claires sont définies pour la mise en œuvre et le suivi des KPI à différents niveaux de l'organisation. Pour ce faire, il convient d'attribuer des tâches aux responsables de la sécurité concernés et de définir des processus pour l'évaluation et la mise à jour régulières des KPI.
HoP-01-01-03-01 Instructions de travail domaine ISMS: protection de base de la sécurité de l'information	Les instructions de travail dans le domaine de la sécurité de l'information pour la protection de base, notamment en ce qui concerne la sécurité des données, définissent les étapes et les principes de base pour assurer une protection adéquate des données dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires pour assurer la confidentialité, l'intégrité et la disponibilité des informations, tout en respectant les exigences légales et de conformité. Elles soulignent l'importance d'une analyse globale des risques en matière de sécurité des données afin d'identifier les menaces et les points faibles potentiels. Il s'agit de mettre au point des processus clairs pour la classification des données, la protection des accès, le cryptage et la révision régulière des mesures de sécurité. Des responsabilités claires sont définies pour la mise en œuvre des directives de sécurité des données à différents niveaux de l'organisation. Cela implique la formation des collaborateurs et collaboratrices afin de les sensibiliser à l'utilisation responsable des données et de permettre ainsi la mise en place de mécanismes de surveillance et d'amélioration continues des mesures de sécurité des données.
HoP-01-01-03-02 Instructions de travail domaine ISMS: gestion des risques IT/OT	Les instructions de travail dans le domaine de la sécurité de l'information pour l'application de la gestion des risques IT/OT définissent les étapes et principes essentiels pour garantir une identification, une évaluation et une gestion efficaces des risques liés à l'intégration des technologies de l'information (IT) et des technologies opérationnelles (OT). Elles visent principalement à fournir des lignes directrices claires afin de garantir la sécurité et la stabilité des infrastructures opérationnelles critiques. Elles insistent sur la nécessité d'une analyse des risques globale qui tienne compte des défis spécifiques de la convergence des technologies IT et OT. Il s'agit de définir des processus clairs pour l'identification des risques, l'évaluation de leur impact sur les processus opérationnels et le développement de mesures appropriées pour les atténuer. Des responsabilités claires sont définies pour la mise en œuvre de la gestion des risques IT/OT à différents niveaux de l'organisation. Cela implique la création d'une équipe ou d'un comité responsable de la mise en œuvre et du suivi coordonnés du traitement des risques.
HoP-01-01-03-03 Instructions de travail domaine ISMS: gestion des actifs et classification des informations	Les instructions de travail dans le domaine de la sécurité de l'information pour la gestion des actifs et la classification des informations définissent les étapes et les principes de base pour assurer une gestion efficace des actifs et la classification des informations dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires afin de garantir la disponibilité, l'intégrité et la confidentialité des informations et des actifs. Elles soulignent l'importance d'un état des lieux et d'une gestion systématiques des actifs, y compris le matériel, les logiciels et les informations. Il s'agit d'établir des processus clairs pour l'identification, la classification et le suivi des actifs afin de garantir une protection adaptée. Ces instructions mettent également en avant l'importance de la classification des informations, en fonction de leur valeur et de leur sensibilité. L'objectif est de définir des directives claires pour la classification, l'accès et le traitement des informations afin de garantir la mise en œuvre de mesures de sécurité appropriées. Des responsabilités claires sont définies pour la mise en œuvre de la gestion des actifs et de la classification des informations à différents niveaux de l'organisation. Cela implique la formation des collaborateurs et collaboratrices afin de les sensibiliser à l'importance de la gestion des actifs et de la classification des informations, et de permettre ainsi la mise en place de mécanismes de surveillance et d'amélioration continues de ces processus.
HoP-01-01-03-04 Instructions de travail domaine ISMS: formation et sensibilisation	Les instructions de travail dans le domaine de la sécurité de l'information pour la formation et la sensibilisation définissent les étapes et les principes de base pour assurer une bonne préparation des collaborateurs et collaboratrices des entreprises et des unités organisationnelles aux défis de la sécurité de l'information. Elles visent principalement à fournir des lignes directrices claires afin de sensibiliser aux risques de sécurité, de transmettre les connaissances nécessaires et de s'assurer que les collaborateurs et collaboratrices utilisent les informations de manière responsable. Elles soulignent l'importance d'une stratégie de formation globale, adaptée aux besoins spécifiques de l'organisation. Cela inclut des formations sur des thèmes tels que la gestion sécurisée des mots de passe, la prévention du phishing, des dispositions relatives à la protection des données et d'autres aspects pertinents en matière de sécurité. En outre, des responsabilités claires



Titre	Description
	sont définies pour la mise en œuvre des mesures de formation à différents niveaux de l'organisation. Des personnes clés pour la formation, la planification des programmes de formation et le contrôle régulier de l'efficacité de la formation sont également identifiées.
HoP-01-01-03-05 Instructions de travail domaine ISMS: sécurité physique des actifs TIC	Les instructions de travail dans le domaine de la sécurité de l'information pour la sécurité physique des actifs des technologies de l'information et de la communication (TIC) établit des principes et des étapes de base pour garantir une protection adaptée de l'environnement physique dans lequel les équipements et les systèmes TIC sont exploités. Elles visent principalement à fournir des lignes directrices claires afin de garantir la disponibilité, l'intégrité et la confidentialité des actifs TIC tout en minimisant les risques physiques. Elles soulignent l'importance d'une analyse globale des risques dans le domaine de la sécurité physique, en tenant compte des menaces potentielles telles que l'accès non autorisé, le vol ou les catastrophes naturelles. Il s'agit de définir des processus clairs pour l'accès aux locaux, la protection des équipements TIC contre les accès non autorisés et la sécurisation de l'environnement dans lequel ils fonctionnent. Des responsabilités claires sont définies pour la mise en œuvre des directives de sécurité physique à différents niveaux de l'organisation. Dans ce cadre, des personnes chargées de la sécurité sont désignées, des mesures de sécurité font l'objet d'un suivi et le personnel est formé aux directives de sécurité physique.
HoP-01-01-03-06 Instructions de travail domaine ISMS: contrôle d'accès	Les instructions de travail dans le domaine ISMS (Information Security Management System) pour le contrôle d'accès mettent l'accent sur la gestion et la surveillance efficaces de l'accès aux informations et aux systèmes dans une organisation. Elles commencent par une définition claire du champ d'application afin de déterminer les domaines et les ressources couverts par le contrôle d'accès. L'objectif est formulé de manière précise afin de s'assurer que le contrôle d'accès soutient les objectifs de sécurité spécifiques de l'organisation. Une étape essentielle consiste à identifier les exigences en matière d'accès, en déterminant quels groupes d'utilisateurs peuvent accéder à quelles informations et à quels systèmes. Cela constitue la base de la définition des directives d'accès. Les instructions décrivent en détail comment développer des directives d'accès, y compris la définition des autorisations, des rôles et des responsabilités. Les principes de sécurité sont pris en compte afin de respecter les principes de confidentialité, d'intégrité et de disponibilité. La mise en œuvre concrète des contrôles d'accès est décrite, en tenant compte des divers mécanismes et technologies, tels que l'authentification et l'autorisation. L'objectif est de s'assurer que les contrôles d'accès sont à la fois efficaces et conviviaux. Les instructions précisent comment les contrôles d'accès sont surveillés et vérifiés par des audits réguliers. Cela garantit le respect des directives d'accès et permet d'identifier les écarts ou les risques de sécurité potentiels. Des mesures de formation et de sensibilisation du personnel au contrôle d'accès y sont également décrites. Le document comprend des programmes de formation pour s'assurer que l'ensemble des utilisateurs comprend de manière adaptée les pratiques d'accès sécurisé. Il prévoit la manière de réagir aux incidents de sécurité liés aux contrôles d'accès. Cela inclut des mesures de réaction immédiate en cas d'accès non autorisé ou d'atteinte à la sécurité. La documentation des contrôles d'accès mis en œuvre et l'établissement de rapports sur l'état actuel font également partie intégrante des instructions de travail. Cela garantit la transparence et permet une amélioration continue. Ces instructions soulignent la nécessité d'impliquer toutes les parties prenantes concernées, y compris le personnel informatique, la direction et les utilisateurs, dans le processus afin de garantir une mise en œuvre globale et efficace du contrôle d'accès. Les instructions de travail dans le domaine ISMS concernant le contrôle d'accès servent de guide complet et permettent de s'assurer que les contrôles d'accès sont clairement définis, mis en œuvre et continuellement améliorés.
HoP-01-01-03-07 Instructions de travail domaine ISMS: authentification multi-facteur	Les instructions de travail ISMS (Information Security Management System) dans le contexte de l'authentification multi-facteur (AMF) se concentrent sur la manière dont l'organisation peut mettre en œuvre ce concept de sécurité avancé. Elles commencent par une définition claire du champ d'application afin de déterminer quels domaines et systèmes sont couverts par l'AMF. L'objectif est formulé de manière précise afin de s'assurer que l'AMF prend en charge les objectifs de sécurité spécifiques de l'organisation, notamment en ce qui concerne l'authentification et le contrôle d'accès. Le document explique comment l'organisation peut identifier les domaines critiques dans lesquels l'AMF est particulièrement importante. Il pourrait s'agir de bases de données sensibles, d'accès administratifs ou d'autres domaines clés. Ces instructions décrivent comment sélectionner et mettre en œuvre différents facteurs d'authentification à utiliser dans l'AMF. Il s'agit typiquement de facteurs de connaissance (mots de passe), de facteurs de possession (cartes à puce, jetons) et de facteurs biométriques (empreintes digitales, reconnaissance faciale). Il y est expliqué comment l'AMF peut être parfaitement intégrée aux systèmes et méthodes d'authentification existants afin de minimiser les perturbations et de permettre une transition en douceur. Les instructions soulignent l'importance d'une mise en œuvre conviviale de l'AMF afin de favoriser l'acceptation du personnel. Des formations et des mesures de sensibilisation peuvent être proposées pour s'assurer que les utilisateurs puissent comprendre et utiliser correctement les nouvelles méthodes d'authentification. Des mesures de surveillance de la mise en œuvre de l'AMF sont décrites pour que tous les facteurs d'authentification fonctionnent correctement et que les incidents de sécurité potentiels puissent être détectés immédiatement. Les instructions prévoient la manière de réagir aux incidents de sécurité liés à l'AMF. Cela peut inclure le blocage immédiat des accès ou le rétablissement des comptes après avoir été compromis. La manière dont la mise en œuvre de l'AMF est documentée et contrôlée est définie. Des rapports réguliers sur le statut et les améliorations possibles sont mis en avant comme éléments importants de l'amélioration continue. Les



Titre	Description
	instructions de travail soulignent la nécessité d'impliquer l'ensemble des parties prenantes, y compris le personnel informatique, la direction et les utilisateurs, dans le processus de mise en œuvre de l'AMF afin que celui-ci soit complet et efficace. Les instructions de travail dans le domaine ISMS concernant l'authentification multi-facteur servent de guide complet et permettent de s'assurer que l'AMF est clairement définie, mise en œuvre et continuellement améliorée.
HoP-01-01-03-08 Instructions de travail domaine ISMS: gestion des droits d'accès privilégiés	Les instructions de travail dans le domaine de la sécurité de l'information pour la gestion des droits d'accès privilégiés définissent les principes et étapes de base permettant de garantir une gestion sûre des droits d'accès particulièrement privilégiés dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires pour protéger la confidentialité, l'intégrité et la disponibilité des données, tout en contrôlant étroitement l'accès aux comptes utilisateurs privilégiés. Elles soulignent la nécessité de gérer minutieusement les droits d'accès privilégiés afin de minimiser le risque d'abus ou d'utilisation non autorisée. Il s'agit de définir des processus clairs pour l'attribution, la vérification et la surveillance des droits d'accès privilégiés afin de garantir qu'ils ne sont accordés qu'aux personnes autorisées et que leur utilisation est contrôlée de manière adéquate. Des responsabilités claires sont définies pour la mise en œuvre de la gestion des droits d'accès privilégiés à différents niveaux de l'organisation. Cela implique la désignation d'administrateurs et de responsables de la sécurité chargés de la gestion des droits d'accès privilégiés, ainsi que des mesures de formation pour s'assurer que les responsables comprennent et respectent les directives de sécurité.
HoP-01-01-03-09 Instructions de travail domaine ISMS: systèmes (serveur et client)	Les instructions de travail dans le domaine de la sécurité de l'information pour les systèmes – aussi bien serveur que client – définissent les principes et étapes de base permettant de garantir la sécurité et la protection des systèmes informatiques dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires pour assurer la confidentialité, l'intégrité et la disponibilité des informations traitées sur ces systèmes. Elles soulignent l'importance d'une directive de sécurité globale pour les systèmes (serveur et client). L'objectif est de définir des processus clairs pour la configuration, l'exploitation et la surveillance de ces systèmes afin de minimiser les points faibles potentiels et de garantir le respect des normes de sécurité. Des responsabilités claires sont définies pour la mise en œuvre des directives de sécurité à différents niveaux de l'organisation. Cela implique la désignation d'administrateurs système et de responsables de la maintenance des systèmes, ainsi que la formation des collaborateurs et collaboratrices afin de s'assurer qu'ils utilisent en toute conscience les directives de sécurité.
HoP-01-01-03-10 Instructions de travail domaine ISMS: composants contrôle-commande	Les instructions de travail dans le domaine de la sécurité de l'information pour les composants contrôle-commande définissent les principes et étapes de base permettant d'assurer la sécurité et la protection des systèmes de contrôle-commande dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires pour assurer la confidentialité, l'intégrité et la disponibilité des informations dans les composants contrôle-commande. Elles soulignent la nécessité d'une directive de sécurité spécifique pour les systèmes de contrôle-commande. L'objectif est de définir des processus clairs pour la configuration, l'exploitation et la surveillance de ces systèmes afin de minimiser les risques et points faibles potentiels et de garantir le respect des normes de sécurité. Des responsabilités claires sont définies pour la mise en œuvre des directives de sécurité à différents niveaux de l'organisation. Cela implique la désignation d'administrateurs système et de responsables de la maintenance des composants contrôle-commande, ainsi que des mesures de formation afin de s'assurer que les collaborateurs et collaboratrices utilisent en toute conscience les directives de sécurité.
HoP-01-01-03-11 Instructions de travail domaine ISMS: systèmes d'exploitation et applications	Les instructions de travail dans le domaine de la sécurité de l'information pour les systèmes d'exploitation et applications définissent les principes et étapes de base permettant d'assurer la sécurité et la protection des systèmes informatiques dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires pour assurer la confidentialité, l'intégrité et la disponibilité des informations au niveau des systèmes d'exploitation et applications. Elles soulignent l'importance d'une directive de sécurité globale pour les systèmes d'exploitation et applications. L'objectif est de définir des processus clairs pour l'installation, la configuration, l'exploitation et la mise à jour régulière de ces systèmes afin de minimiser les points faibles potentiels et de garantir le respect des normes de sécurité. Des responsabilités claires sont définies pour la mise en œuvre des directives de sécurité à différents niveaux de l'organisation. Cela implique la désignation d'administrateurs système et de responsables de la maintenance des systèmes d'exploitation et applications, ainsi que des mesures de formation afin de s'assurer que les collaborateurs et collaboratrices utilisent en toute conscience les directives de sécurité.
HoP-01-01-03-12 Instructions de travail domaine ISMS: cryptage	Les instructions de travail dans le domaine de la sécurité de l'information pour le cryptage définissent les principes et étapes de base permettant de garantir une gestion sûre des données sensibles dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires afin de garantir la confidentialité des informations par le biais de technologies de cryptage. Elles soulignent la nécessité d'une directive de cryptage globale couvrant différents aspects, de l'identification des données à chiffrer à la sélection et à la mise en œuvre d'algorithmes de cryptage appropriés, en passant par la gestion des clés de cryptage. Des processus clairs sont définis pour le cryptage des données à différents niveaux de l'organisation afin de garantir une protection adaptée de l'ensemble des informations importantes. La formation



Titre	Description
	du personnel à l'utilisation sécurisée des données cryptées est également prise en compte. Les responsabilités pour la mise en œuvre des directives de cryptage sont clairement définies, y compris la désignation d'administrateurs et de responsables de la sécurité chargés de la mise en œuvre et du suivi des technologies de cryptage.
HoP-01-01-03-13 Instructions de travail domaine ISMS: réseaux	Les instructions de travail dans le domaine de la sécurité de l'information pour les réseaux définissent les principes et étapes de base permettant d'assurer la sécurité et la protection des systèmes informatiques dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires pour assurer la confidentialité, l'intégrité et la disponibilité des informations durant la transmission via des réseaux. Elles soulignent la nécessité d'une directive de sécurité du réseau globale couvrant différents aspects de l'architecture et l'utilisation du réseau. L'objectif est de définir des processus clairs pour la configuration, la surveillance et la protection des réseaux contre de potentielles menaces afin de garantir le respect des normes de sécurité. Des responsabilités claires sont définies pour la mise en œuvre des directives de sécurité du réseau à différents niveaux de l'organisation. Cela implique la désignation d'administrateurs réseau et de responsables de la sécurité chargés de la mise en œuvre et de la surveillance des mesures de sécurité au niveau des réseaux.
HoP-01-01-03-14 Instructions de travail domaine ISMS: sauvegarde et liste de contrôle pour la sauvegarde	Les instructions de travail dans le domaine de la sécurité de l'information pour la sauvegarde et la liste de contrôle correspondante pour la sauvegarde définissent les principes et étapes de base permettant d'assurer la sécurité et la disponibilité des données dans les entreprises et les unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires pour la sauvegarde régulière des données ainsi que pour la vérification et la restauration des sauvegardes. Elles soulignent l'importance d'une directive de sauvegarde globale couvrant différents aspects, de l'identification des données critiques à la définition d'intervalles et de méthodes de sauvegarde. L'objectif est de définir des processus clairs pour l'exécution de sauvegardes et la vérification de leur intégrité, afin de garantir une restauration efficace en cas de perte de données ou de défaillance du système. La liste de contrôle correspondante pour la sauvegarde fait office de guide structuré pour la mise en œuvre des directives de sauvegarde. Les instructions de travail comprennent la révision régulière des journaux de sauvegarde, la garantie de sauvegardes complètes et mises à jour, ainsi que la planification de tests de restauration afin de garantir l'efficacité du système de sauvegarde. Des responsabilités claires sont définies pour la mise en œuvre des directives de sauvegarde et la réalisation de contrôles ad hoc à différents niveaux de l'organisation. Cela implique la désignation d'administrateurs sauvegarde et de responsables de la sécurité chargés de la planification, de la mise en œuvre et de la surveillance des activités de sauvegarde et de restauration.
HoP-01-01-03-15 Instructions de travail domaine ISMS: nettoyage des médias	Les instructions de travail dans le domaine de la sécurité de l'information pour le nettoyage des médias définissent les principes et étapes de base permettant de s'assurer que les informations sur les supports physiques dans les entreprises et les unités organisationnelles peuvent être supprimées de manière sûre et définitive. Elles visent principalement à fournir des lignes directrices claires pour protéger la confidentialité des données et pour s'assurer que les médias sont supprimés de manière correcte et irréversible avant qu'ils se diffusent en dehors de l'organisation. Elles soulignent la nécessité d'une directive de nettoyage des médias globale, couvrant différents types de supports physiques, des disques durs aux lecteurs USB. L'objectif est de définir des processus clairs pour la suppression sécurisée des données afin de garantir qu'aucune information confidentielle ne reste sur les médias. Des responsabilités claires sont définies pour la mise en œuvre des directives de nettoyage des médias à différents niveaux de l'organisation. Cela implique la désignation de responsables de la sécurité physique et de la suppression des données, ainsi que des mesures de formation afin de s'assurer que les collaborateurs et collaboratrices utilisent en toute conscience les directives de sécurité en lien avec le nettoyage des médias.
HoP-01-01-03-16 Instructions de travail domaine ISMS: gestion LOG	Les instructions de travail dans le domaine de la sécurité de l'information pour la gestion LOG définissent les principes et étapes de base permettant de s'assurer que les données du journal des entreprises et unités organisationnelles sont saisies, contrôlées et gérées de manière efficace. Elles visent principalement à fournir des lignes directrices claires pour assurer l'intégrité et la disponibilité des données des journaux, tout en identifiant le plus tôt possible les incidents de sécurité potentiels. Elles soulignent l'importance d'une directive de gestion LOG globale couvrant différents aspects, de la définition des événements à consigner au stockage et à la surveillance sécurisés des données des journaux. L'objectif est de définir des processus clairs pour la saisie, l'analyse et l'archivage des données de journaux afin de s'assurer qu'ils respectent à la fois les exigences légales et les normes de sécurité internes. Des responsabilités claires sont définies pour la mise en œuvre des directives de gestion LOG à différents niveaux de l'organisation. Cela implique la désignation d'administrateurs et de responsables de la sécurité chargés de la configuration et de la surveillance des systèmes de journalisation, ainsi que des mesures de formation pour s'assurer que le personnel comprenne l'importance des données des journaux et les utilise de manière adaptée.
HoP-01-01-03-17 Instructions de travail domaine ISMS: gestion des logiciels malveillants	Les instructions de travail dans le domaine de la sécurité de l'information pour la gestion des logiciels malveillants et des vulnérabilités définissent les principes et étapes de base permettant de s'assurer que les entreprises et unités organisationnelles mettent en œuvre des mesures efficaces contre les logiciels malveillants et les potentielles vulnérabilités dans les systèmes informatiques. Elles visent principalement à fournir des lignes directrices claires pour protéger l'intégrité



Titre	Description
et des vulnérabilités	et la disponibilité des données, tout en minimisant le risque de failles de sécurité et d'infection par des logiciels malveillants. Elles soulignent l'importance d'une directive globale de gestion des logiciels malveillants et des vulnérabilités. L'objectif est de définir des processus clairs pour la surveillance régulière de systèmes informatiques concernant les vulnérabilités et pour la mise en œuvre de mesures de protection contre les logiciels malveillants. Cela implique également des mécanismes pour identifier, isoler et supprimer rapidement des infections par des logiciels malveillants. Des responsabilités claires sont définies pour la mise en œuvre des directives de gestion des logiciels malveillants et des vulnérabilités à différents niveaux de l'organisation. Des responsables de la sécurité informatique et des administrateurs chargés de surveiller et de mettre à jour les mécanismes de protection doivent être désignés et des mesures de formation identifiées afin de s'assurer que les collaborateurs et collaboratrices comprennent les risques liés aux logiciels malveillants et adoptent un comportement responsable en matière de sécurité. Ces instructions de travail sont contraignantes pour l'ensemble du personnel et la direction se réserve le droit de prendre les mesures appropriées en cas de non-respect. La révision et l'adaptation continues de ces instructions dans le domaine de la sécurité de l'information pour la gestion des logiciels malveillants et des vulnérabilités permettent de s'assurer que le document est toujours conforme aux normes et exigences actuelles en matière de sécurité de l'information et permet ainsi une protection efficace contre les menaces potentielles.
HoP-01-01-03-18 Instructions de travail domaine ISMS: gestion des incidents liés à la sécurité de l'information (Incident Management)	Les instructions de travail dans le domaine de la sécurité de l'information pour la gestion d'incidents liés à la sécurité (Incident Management) définissent les principes et étapes de base permettant de s'assurer que les entreprises et unités organisationnelles réagissent de manière efficace et coordonnée aux incidents liés à la sécurité. Elles visent principalement à fournir des lignes directrices claires afin d'identifier rapidement les incidents liés à la sécurité, de les évaluer de manière adaptée et d'y répondre afin d'en limiter les impacts. Elles soulignent l'importance d'une directive de gestion d'incidents liés à la sécurité complète, couvrant différents types de d'incidents liés à la sécurité, des fuites de données aux cyber-attaques. L'objectif est de définir des processus clairs pour l'identification, la déclaration, l'enquête et l'escalade des incidents liés à la sécurité afin de garantir une réponse efficace. Des responsabilités claires sont définies pour la mise en œuvre des directives de gestion d'incidents liés à la sécurité à différents niveaux de l'organisation. Cela implique la désignation d'équipes chargées d'apporter une réponse aux incidents et de responsables de la coordination de mesures ainsi que la définition de mesures de formation permettant de s'assurer que les collaborateurs et collaboratrices comprennent l'importance de réagir immédiatement et avec précision aux incidents liés à la sécurité.
HoP-01-01-03-19 Instructions de travail domaine ISMS: gestion de la continuité des opérations (BCM)	Les instructions de travail dans le domaine de la sécurité de l'information pour la gestion de la continuité des opérations (BCM) définissent les principes et étapes de base permettant de s'assurer que les entreprises et unités organisationnelles sont capables de résister aux interruptions et de poursuivre efficacement leurs activités en cas de perturbation ou de catastrophe. Elles visent principalement à fournir des lignes directrices claires afin de garantir la continuité des opérations et à réduire au maximum les répercussions d'interruptions. Elles soulignent l'importance d'une directive BCM globale couvrant différents aspects, de l'identification des processus critiques à la définition de plans d'urgence et de stratégie de restauration. L'objectif est de définir des processus clairs pour l'analyse des risques, la mise en œuvre de mesures de protection et la révision et la mise à jour régulières des plans de BCM. Des responsabilités claires sont définies pour la mise en œuvre des directives de BCM à différents niveaux de l'organisation. Cela implique la désignation de responsables BCM et d'équipes d'intervention d'urgence ainsi que des mesures de formation afin de s'assurer que les collaborateurs et collaboratrices comprennent la nécessité des procédures liées à la BCM.
HoP-01-01-03-20 Instructions de travail domaine ISMS: gestion des situations d'urgence	Les instructions de travail dans le domaine ISMS (Information Security Management System) pour la gestion des situations d'urgence sont axées sur la manière dont l'entreprise et les unités organisationnelles peuvent réagir efficacement aux incidents de sécurité et aux situations de crise. Elles commencent par une définition claire du champ d'application afin de déterminer quels types d'incidents de sécurité et de situations d'urgence doivent être couverts. L'objectif est formulé de manière précise afin de s'assurer que la gestion des situations d'urgence soutient les objectifs de sécurité spécifiques de l'organisation. Le document explique comment procéder à une évaluation globale des risques afin d'identifier les incidents de sécurité potentiels et les scénarios d'urgence. Cela pourrait inclure des menaces telles que les cyberattaques, les catastrophes naturelles ou les erreurs humaines. Les instructions décrivent le processus de planification des mesures d'urgence, y compris l'établissement d'instructions claires et les responsabilités des différentes équipes et du personnel pendant une situation d'urgence. Elles soulignent l'importance de prendre en compte différents scénarios et de développer des concepts flexibles. Des mesures de communication et d'alerte efficaces sont présentées afin de garantir que l'ensemble des parties concernées, y compris le personnel, la direction et les parties prenantes externes, sont informées en temps utile. Cela peut impliquer l'utilisation de différents canaux et moyens de communication. Les instructions de travail expliquent comment les équipes doivent réagir efficacement en cas d'urgence. Cela nécessite de prendre des mesures claires en cas d'escalade, de collaborer avec les autorités externes et de mettre en œuvre des mesures immédiates pour limiter les dommages. Elles couvrent le processus de restauration après une situation d'urgence, y compris le retour progressif aux opérations normales. L'accent est mis sur l'importance d'un suivi complet afin de tirer les leçons de l'incident et d'améliorer les futurs plans d'urgence. Des mesures sont proposées pour



Titre	Description
	<p>organiser régulièrement des exercices en cas de situation d'urgence et des formations pour le personnel afin de s'assurer que la gestion des urgences peut être mise en œuvre de manière efficace. La manière dont la gestion des situations d'urgence est documentée et contrôlée est définie dans ces instructions. Des rapports réguliers sur le statut, l'efficacité des mesures et les améliorations possibles y sont décrits comme des éléments importants de l'amélioration continue. Les instructions soulignent la nécessité d'impliquer l'ensemble des parties prenantes concernées, y compris le personnel informatique, la direction et les équipes d'intervention d'urgence, dans le processus de gestion des urgences afin de garantir une mise en œuvre complète et efficace. Les instructions de travail dans le domaine ISMS servent de guide complet et permettent de s'assurer que l'entreprise et les unités organisationnelles sont bien préparées pour répondre aux situations d'urgence et que la gestion des urgences est clairement définie, mise en œuvre et fait l'objet d'une amélioration continue.</p>
<p>HoP-01-01-03-21 Instructions de travail domaine ISMS: mesures de sécurité pour les prestataires de services</p>	<p>Les instructions de travail dans le domaine ISMS (Information Security Management System) concernant les mesures de sécurité pour les prestataires de services visent à garantir que les partenaires et prestataires de services externes sont intégrés de manière appropriée dans la stratégie de sécurité de l'entreprise et des unités organisationnelles. Elles commencent par une définition claire du champ d'application afin de déterminer quels prestataires de services et partenaires sont couverts. L'objectif est de s'assurer que les mesures de sécurité des prestataires de services sont conformes aux normes de sécurité de l'organisation. Le document explique comment procéder à une évaluation complète des risques pour les prestataires de services afin d'identifier les risques de sécurité et menaces potentiels qui pourraient résulter de leurs activités. Il décrit comment intégrer les exigences de sécurité dans les contrats et accords avec les prestataires de services. L'accent est mis sur l'importance de s'assurer que les prestataires de services respectent les normes de conformité et les directives de sécurité correspondantes. Les mesures de contrôle permanent de la fourniture de garantie des prestataires de services sont présentées. Cela peut inclure la réalisation régulière d'audits, de contrôles de sécurité et d'évaluations de la fourniture. Ces instructions de travail expliquent comment établir et communiquer des consignes de sécurité claires destinées aux prestataires de services, dont la formation aux directives et procédures de sécurité est présentée comme faisant partie intégrante de celles-ci. Les instructions comprennent des mesures visant à garantir que les prestataires de services peuvent réagir de manière appropriée dans les situations d'urgence. Cela inclut la définition de plans d'urgence, de procédures de communication et de mécanismes de réponse coordonnés. Elles précisent comment les prestataires de services doivent rendre compte régulièrement de leur fourniture de garantie et garantir un aperçu transparent de leurs mesures de sécurité. Cela favorise une communication et une collaboration ouvertes. Les instructions soulignent la nécessité de travailler en étroite collaboration avec les prestataires de services en cas d'incident de sécurité. Cela implique des processus clairs pour la déclaration des incidents, des procédures d'escalade et une gestion conjointe des menaces de sécurité. Le document se conclut en mettant l'accent sur l'amélioration continue et l'adaptation des mesures de sécurité pour les prestataires de services. Cela nécessite des vérifications régulières, des interactions et l'intégration de nouvelles normes de sécurité. Les instructions de travail dans le domaine ISMS concernant les mesures de sécurité pour les prestataires de services garantissent une intégration appropriée de ces derniers dans la stratégie de sécurité et contribuent à assurer la sécurité globale de l'entreprise et des unités organisationnelles.</p>
<p>HoP-01-01-03-22 Instructions de travail domaine ISMS: gestion des fournisseurs</p>	<p>Les instructions de travail dans le domaine de la sécurité de l'information pour la gestion des fournisseurs définissent les principes et étapes de base permettant de s'assurer que les entreprises et les unités organisationnelles maintiennent des normes de sécurité appropriées en ce qui concerne leurs fournisseurs et partenaires. Elles visent principalement à fournir des lignes directrices claires afin de minimiser les risques de sécurité posés par les partenaires externes et de protéger la confidentialité, l'intégrité et la disponibilité des informations. Elles soulignent l'importance d'une directive de gestion des fournisseurs globale couvrant différents aspects, de la sélection et le contrôle des fournisseurs à la définition d'exigences de sécurité et de mécanismes de surveillance. Elles déterminent des processus clairs pour l'évaluation des risques, la rédaction des contrats et l'examen régulier des pratiques de sécurité des fournisseurs. Des responsabilités claires sont définies pour la mise en œuvre des directives de gestion des fournisseurs à différents niveaux de l'organisation. Cela implique la désignation de responsables pour la sélection, la surveillance et la fin des relations avec les fournisseurs ainsi que la définition de mesures de formation permettant de s'assurer que les collaborateurs et collaboratrices comprennent l'importance de la sécurité dans le cadre de la collaboration avec des partenaires externes.</p>
<p>HoP-01-01-03-23 Instructions de travail domaine ISMS: sécurité de l'information dans le domaine des ressources humaines</p>	<p>Les instructions de travail dans le domaine de la sécurité de l'information pour la sécurité de l'information dans le domaine des ressources humaines définissent les principes et étapes de base permettant de s'assurer que le personnel des entreprises et unités organisationnelles est qualifié, formé et sensibilisé de manière appropriée et agit en étant conscient de la sécurité. Elles visent principalement à créer des lignes directrices claires afin de minimiser les facteurs humains considérés comme des risques potentiels et de favoriser un environnement de travail sûr.</p> <p>Ces instructions de travail soulignent l'importance d'une directive du personnel globale en matière de sécurité de l'information. L'objectif est de définir des processus clairs pour la formation des collaborateurs et collaboratrices sur les questions de sécurité, la sensibilisation aux menaces potentielles et la promotion d'une sensibilisation à la sécurité sur le lieu de travail. Des responsabilités claires sont définies pour la mise en œuvre des directives de sécurité dans le domaine des</p>



Titre	Description
	ressources humaines à différents niveaux de l'organisation. Cela inclut la désignation de responsables de la sécurité et de la formation, ainsi que la définition de mesures d'évaluation et de mise à jour régulières des formations à la sécurité.
HoP-01-01-03-24 Instructions de travail domaine ISMS: sécurité de l'information dans les projets	Les instructions de travail dans le domaine de la sécurité de l'information pour les projets définissent les principes et étapes de base permettant de s'assurer que les aspects de la sécurité de l'information sont intégrés de manière appropriée dans la planification, la mise en œuvre et l'évaluation des projets des entreprises et des unités organisationnelles. Elles visent principalement à fournir des lignes directrices claires afin de s'assurer que les projets sont conçus et mis en œuvre en tenant compte de la sécurité dès le début. Elles soulignent l'importance d'une directive globale pour la sécurité de l'information dans les projets. L'objectif est de définir des processus clairs pour l'identification des exigences de sécurité, la réalisation d'évaluations des risques et l'intégration des contrôles de sécurité dans toutes les phases du cycle de vie du projet. Des responsabilités claires sont définies pour la mise en œuvre des directives de sécurité de l'information dans les projets à différents niveaux de l'organisation. Cela implique la désignation de responsables de la sécurité et de gestionnaires de projets chargés de l'intégration de pratiques relatives à la sécurité de l'information dans les projets, ainsi que la définition de mesures de formation pour s'assurer que les équipes de projet comprennent l'importance de la sécurité de l'information.
HoP-01-01-03-25 Instructions de travail domaine ISMS: utilisation de services en cloud	Les instructions de travail dans le domaine de la sécurité de l'information pour l'utilisation de services en cloud définissent les principes et étapes de base permettant de s'assurer que l'intégration des services en cloud dans les entreprises et les unités organisationnelles s'effectue de manière sûre et conforme aux normes de sécurité de l'information. Elles visent principalement à fournir des lignes directrices claires pour assurer la confidentialité, l'intégrité et la disponibilité des données dans le cloud. Elles soulignent l'importance d'une directive globale pour l'utilisation de services en cloud. L'objectif est de définir des processus clairs pour la sélection des prestataires de services cloud, l'évaluation des normes de sécurité, la mise en place de contrôles de sécurité et l'examen régulier de la sécurité du cloud. Des responsabilités claires sont définies pour la mise en œuvre des directives d'utilisation de services en cloud à différents niveaux de l'organisation. Cela implique la désignation d'administrateurs informatiques et de responsables cloud chargés de la configuration et de la surveillance des mesures de sécurité du cloud, ainsi que la définition de mesures de formation pour s'assurer que le personnel comprend les aspects de sécurité liés à l'utilisation des services de cloud.
HoP-01-01-03-26 Instructions de travail domaine ISMS: utilisation de l'apprentissage automatique et de l'intelligence artificielle	Les instructions de travail dans le domaine de la sécurité de l'information pour l'utilisation de l'apprentissage automatique et de l'intelligence artificielle (IA) définissent les principes et étapes de base permettant de s'assurer que l'utilisation de technologies d'IA dans les entreprises et les unités organisationnelles s'effectue de manière sûre, éthique et conforme aux normes de sécurité de l'information. Elles visent à fournir des lignes directrices claires afin d'assurer l'intégrité des systèmes d'IA, de prendre en compte les aspects liés à la protection des données et de minimiser les risques éventuels de sécurité. Elles soulignent l'importance d'une directive globale pour l'utilisation de l'apprentissage automatique et de l'intelligence artificielle. L'objectif est de définir des processus clairs pour la sélection et la mise en œuvre de technologies d'IA, l'évaluation des risques liés à la protection des données, la révision régulière des algorithmes et la formation du personnel à l'utilisation des systèmes d'IA. Des responsabilités claires sont définies pour la mise en œuvre des directives d'utilisation de l'apprentissage automatique et de l'IA à différents niveaux de l'organisation. Cela implique la désignation de responsables d'IA, de responsables de la protection des données et d'experts en informatique chargés de la sécurité et de l'utilisation éthique des technologies d'IA.
HoP-01-01-04-01 Instructions de travail domaine Utilisateurs de valeurs d'information: utilisation d'appareils mobiles	Les instructions de travail dans le domaine de la sécurité de l'information pour l'utilisation d'appareils mobiles définissent les étapes et les principes essentiels permettant de garantir que les appareils mobiles sont utilisés de manière sûre et responsable au sein de l'organisation. Elles visent principalement à fournir des lignes directrices claires pour protéger la confidentialité, l'intégrité et la disponibilité des informations accessibles via des appareils mobiles. Elles soulignent la nécessité d'une directive de sécurité claire pour l'utilisation des appareils mobiles, qui tienne compte à la fois des directives de l'entreprise et de l'unité organisationnelle et des exigences légales. Les aspects tels que le contrôle d'accès, la sécurité des données, la perte ou le vol d'appareils et l'utilisation de réseaux publics sont pris en compte. Des responsabilités claires sont définies pour la mise en œuvre de la directive de sécurité pour les appareils mobiles à différents niveaux de l'organisation. Cela implique la formation des collaborateurs et collaboratrices afin de les sensibiliser aux risques de sécurité liés aux appareils mobiles, ainsi que la mise en place de mécanismes de contrôle et d'application des directives de sécurité.
HoP-01-01-04-02 Instructions de travail domaine Utilisateurs de valeurs d'information: utilisation des actifs OT	Les instructions de travail dans le domaine de la sécurité de l'information pour l'utilisation des actifs de technologies opérationnelles (OT) définissent les étapes et les principes de base permettant de garantir une utilisation sûre et responsable des appareils et systèmes OT au sein de notre organisation. Elles visent principalement à fournir des lignes directrices claires pour protéger l'intégrité, la disponibilité et la confidentialité des actifs OT tout en assurant la continuité opérationnelle. Elles insistent sur la nécessité d'une analyse de risque globale qui tienne compte des exigences spécifiques et des particularités des actifs OT. L'objectif est de définir des processus clairs pour l'identification des risques, l'évaluation de leur impact sur les opérations et la mise en œuvre de mesures de sécurité appropriées. Des responsabilités claires sont définies pour la mise



Titre	Description
	<p>en œuvre des directives de sécurité pour les actifs OT à différents niveaux de l'organisation. Cela implique la formation du personnel afin de le sensibiliser aux exigences de sécurité spécifiques des systèmes OT, ainsi que la mise en œuvre de mécanismes de surveillance et d'adaptation continues des mesures de sécurité.</p>



Anhang G: Littérature complémentaire

Titre	An- née	Éditeur et description
Mesures de protection pour les systèmes de contrôle industriels (SCI)	2013	Éditeur: Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI Ces instructions, basées sur des documents américains du <i>Department of Homeland Security, Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT)</i> et du <i>National Institute of Standards and Technology (NIST)</i> , décrivent de manière concise et pragmatique sur 8 pages les 11 principales mesures que les exploitants de SCI doivent garantir.
Analyse des risques et des vulnérabilités du secteur partiel de l'approvisionnement électrique	2016	Éditeur: Office fédéral pour l'approvisionnement économique du pays (OFAE) Cette analyse des risques et des vulnérabilités repose sur la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) et sur la Stratégie nationale pour la protection des infrastructures critiques (PIC). Elle a pour but d'analyser la vulnérabilité aux défaillances ou aux perturbations des TIC dans le secteur partiel critique de l'approvisionnement en électricité.
Guide pour la protection des infrastructures critiques (guide PIC)	2015	Éditeur: Office fédéral de la protection de la population (OFPP) Ce guide constitue un instrument d'examen et, le cas échéant, d'amélioration de la résilience des infrastructures critiques. Il est notamment conçu pour être utilisé dans des sous-secteurs (aussi appelés secteurs partiels) critiques (tels que l'approvisionnement en électricité) par les exploitants, les associations sectorielles (comme l'AES) et les autorités compétentes. Le guide décrit pour l'essentiel une procédure potentielle de gestion des risques: analyse (identification des ressources, vulnérabilités, risques), évaluation, mesures et leur garantie (mise en œuvre, contrôle et amélioration). Cette procédure peut tout à fait ou devrait être intégrée même aux processus de gestion existants ou exécutée sur la base de ces derniers.
Stratégie nationale pour la protection des infrastructures critiques (PIC)	2012	Éditeur: Office fédéral de la protection de la population (OFPP) La stratégie transcrit le champ d'application, désigne les infrastructures critiques (notamment l'approvisionnement en électricité de criticité très importante) et fixe les principes directeurs de la PIC. La stratégie nationale PIC s'adresse à tous les services qui ont des responsabilités dans ce domaine, en particulier aux différentes autorités concernées, aux responsables politiques et aux exploitants d'infrastructures critiques (p. ex. entreprises d'approvisionnement en énergie EAE).
Cyberstratégie nationale (CSN)	2023	Éditeur: Centre national pour la cybersécurité (NCSC) La cyberstratégie nationale suisse (CSN) offre un cadre stratégique qui définit les objectifs et les mesures de la Suisse face aux cybermenaces. Elle vise à renforcer la cybersécurité du pays, à accroître sa résilience face aux cyberattaques et à préserver sa souveraineté numérique. La CSN met l'accent sur la coopération entre le gouvernement, les milieux économiques et scientifiques et la société civile afin de permettre une réponse coordonnée aux cybermenaces. Les domaines clés incluent le renforcement de la cyberdéfense, la promotion des compétences et des innovations ad hoc et la coopération internationale en matière de cybersécurité. La mise en œuvre de la CSN est assurée par différents organismes publics et partenaires afin de garantir une architecture de sécurité globale.
ICT Continuity de l'AES	2011	Éditeur: Association des entreprises électriques suisses (AES) Ce document clé de l'association de branche contient des recommandations pour assurer la disponibilité constante des technologies de l'informatique et des télécommunications dans le contexte de la continuité de l'approvisionnement.
Manuel Protection de base pour les «technologies opérationnelles» (OT) dans l'approvisionnement en électricité	2018	Éditeur: Association des entreprises électriques suisses (AES) Mesures et outils concrets pour réduire à un niveau acceptable les cybermenaces pesant sur l'infrastructure critique que constitue l'approvisionnement en électricité en adoptant une stratégie dite «de défense en profondeur»
BDEW et oe: White Paper et Ausführungshinweise:	2024	Éditeur: Bundesverband der Energie- und Wasserwirtschaft (BDEW) (Association fédérale de l'industrie de l'énergie et de l'eau) et



Titre	An- née	Éditeur et description
Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (en anglais et en allemand)		<p>Österreichs E-Wirtschaft (oe) (Économie électronique autrichienne)</p> <p>Ces deux documents décrivent des mesures de sécurité techniques et opérationnelles pour les systèmes informatisés de contrôle-commande et de télécommunication nouvellement acquis ou introduits dans le domaine des processus des entreprises d'approvisionnement en énergie. L'objectif est d'influencer positivement le développement de produits et de véhiculer une compréhension commune. Ces publications ciblent les mandataires potentiels ainsi que les planificateurs et exploitants internes à l'entreprise. Les références aux normes internationales ISO 27002 et 27019 n'ont qu'une valeur indicative: seules les exigences explicitement énoncées dans les présents documents revêtent un caractère contraignant. Leur structure diffère quelque peu de celle des normes ISO.</p>
Catalogue de sécurité informatique en vertu de l'art. 11, al. 1a, Energiewirtschaftsgesetz (loi relative à l'approvisionnement en électricité et en gaz)	2015	<p>Éditeur: Bundesnetzagentur (BNetzA)</p> <p>En vertu de la loi (art. 11 de l'EnWG 2011), les fournisseurs d'énergie allemands ont jusqu'au 31 janvier 2018 au plus tard pour démontrer qu'ils protègent de manière adéquate leurs systèmes TIC nécessaires à l'exploitation sûre du réseau et présenter à l'Agence fédérale allemande des réseaux (Bundesnetzagentur, BNetzA) un certificat prouvant qu'ils satisfont aux exigences qui leur sont imposées. À cet effet, la BNetzA a publié le catalogue de sécurité informatique, en accord avec l'Office fédéral allemand de la sécurité des technologies de l'information (Bundesamt für Sicherheit in der Informationstechnik, BSI).</p> <p>La revendication majeure de ce catalogue porte sur la mise en place d'un système de gestion de la sécurité de l'information, aussi appelé système de management de la sécurité de l'information (SMSI), selon la norme DIN ISO/IEC 27001. Les exigences du catalogue de sécurité doivent être respectées par tous les gestionnaires de réseau, indépendamment de la taille ou du nombre de clients raccordés. Ce catalogue contient des obligations concrètes pour les gestionnaires de réseau, qui doivent être mises en œuvre conformément aux normes internationales.</p>
ISO/CEI 27001:2022 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences	2022	<p>Éditeur: Organisation internationale de normalisation (ISO) / Commission électrotechnique internationale (CEI)</p> <p>Cette norme détaille les exigences relatives à un système de gestion de la sécurité de l'information (SMSI).</p> <p>La suite ISO/CEI 27 000 (ou ISO 27k) comprend une série de normes concernant la sécurité de l'information, dont les suivantes présentent un intérêt ici:</p> <p>27000:2018 Vue d'ensemble et vocabulaire (:2018 indique l'année de publication.)</p> <p>27001:2022 Exigences: principes de base avec contrôles et objectifs de contrôle en annexe</p> <p>27002:2022 Guide pour les contrôles</p> <p>27003:2017 Lignes directrices pour la mise en œuvre</p> <p>27005:2022 Gestion des risques</p> <p>27019:2017 Rapport technique avec des ajouts spécifiques aux contrôles des procédés dans l'approvisionnement en électricité</p>
ISO/CEI 27002:2022 Technologie de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information		
ISO/CEI TR 27019:2017 Technologie de l'information – Techniques de sécurité – Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/CEI 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie		
NERC CIP – Critical Infrastructure Protection	2006 ss	<p>Éditeur: North American Electric Reliability Corporation (NERC)</p> <p>Nous en sommes actuellement à la version 5 et, pour certaines, à la version 6 des normes de protection des infrastructures critiques (normes CIP) du NERC. Il s'agit des seules normes américaines qui ne doivent pas être appliquées sur une base volontaire, mais impérativement par les «Bulk Electric Systems» (BES) ou leurs exploitants. Il est nécessaire que les BES définissent et mettent en œuvre au</p>



Titre	An- née	Éditeur et description
		moins une politique de sécurité couvrant quatre domaines: sensibilisation à la sécurité, sécurité physique, accès à distance et intervention en cas d'incident. Ce faisant, il ne suffit pas simplement de documenter les politiques, mais il faut aussi mettre en œuvre les processus, les procédures et les contrôles et le vérifier dans le cadre d'un audit.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev.3	2023	Éditeur: National Institute of Standards and Technology (NIST) Ce guide fournit une introduction complète aux ICS, aux topologies et aux architectures, identifie les menaces et les vulnérabilités, et formule des recommandations pour les contre-mesures et l'atténuation des risques. Des contrôles spécifiques aux ICS, basés sur le cadre 800-53 du NIST, sont également présentés.
ISA/CEI 62443 Industrial Communication Networks – Network and System Security	2009 ss	Éditeur: International Society of Automation (ISA) / Commission électrotechnique internationale (CEI) Série d'un total de 13 <i>normes de sécurité et rapports techniques en matière de systèmes de contrôle-commande industriels (IACS)</i> . Ces normes sont généralement applicables dans le domaine de l'automatisation industrielle et ne sont pas spécifiques à l'approvisionnement en électricité. Elles se basent sur les normes ISO 27000 et les étoffent par l'ajout de différences et de particularités propres à l'automatisation industrielle. Il convient de mentionner notamment le traitement de l'architecture réseau et zonale, qui n'est guère ou pas aussi détaillé dans d'autres normes.
CEI 62351 Power Systems Management and Associated Information Exchange – Data and Communications Security (Gestion des systèmes électriques et échanges d'informations connexes – Sécurité des données et des communications)	2007 ss	Éditeur: Commission électrotechnique internationale (CEI) Cette norme spécifique à l'approvisionnement en électricité complète la norme CEI 62443 par l'adjonction de différences et d'extensions en matière de production, de transport et de distribution de courant. Elle s'ajoute à d'autres normes telles que CEI 61850 relative à l'automatisation des sous-stations et CEI 60870 concernant ICCP/TASE.2 avec des protocoles de communication série et IP. Les normes CEI 62351 (il en existe aujourd'hui 13 parties) sont techniquement détaillées et difficiles à comparer avec les normes de sécurité conceptuelles.
IEEE 1686 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities	2022	Éditeur: Institute of Electrical and Electronics Engineers (IEEE) Cette norme définit les fonctions et les configurations qui doivent être fournies dans les dispositifs électroniques intelligents (DEI) en vue d'assurer la sécurité OT de l'infrastructure critique. Les thèmes abordés sont la sécurité concernant l'accès, l'exploitation, la configuration, la révision du microprogramme et la récupération des données d'un DEI, ainsi que le cryptage des données en provenance et à destination de celui-ci. Cette norme ne traite pas des communications à des fins de protection électrique (téléprotection) ni de protection de la vie, de l'intégrité corporelle et de l'environnement. Elle se base dans une certaine mesure sur les normes NERC CIP (Critical Infrastructure Protection) et les complètent au niveau des DEI, de sorte que les dispositifs électroniques ne portent pas atteinte aux exigences NERC CIP.
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies	2016	Éditeur: Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Édition revue et corrigée d'une précédente publication datant de 2006. Introduction complète à la stratégie de défense en profondeur dans le cadre de la sécurité des systèmes de contrôle industriels.
BSI IT-Grundschutz BSI – Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz (V1.2 2014)	2014 ss	Éditeur: Bundesamt für Sicherheit in der Informationstechnik (BSI) À l'aide des normes 100-1 à 100-4 du BSI, l'«IT-Grundschutz» (méthodologie de protection de base des technologies de l'information) décrit une procédure de mise en place et de maintien d'un système de management de la sécurité de l'information (SMSI). Les catalogues et le compendium de l'IT-Grundschutz détaillent la mise en œuvre des mesures et des objectifs qui en découlent. Le SMSI ainsi créé satisfait aux exigences de la norme ISO 27001 et dispose d'un équivalent aux recommandations de la norme ISO 27002. La sécurité peut être introduite et contrôlée selon les procédures de l'IT-Grundschutz développées par le BSI, mais aussi conformément aux normes de la famille ISO 27000. Ces deux options sont



Titre	An- née	Éditeur et description
BSI – Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz		compatibles dans leur approche. Elles sont utilisées pour mettre en place et exploiter un SMSI, qui identifie les risques dans le domaine de la sécurité de l'information et les réduit à un niveau acceptable par le biais de mesures appropriées. Alors que l'analyse et l'évaluation des risques constituent un élément essentiel d'un SMSI conforme à la norme ISO 27001, cette analyse n'est requise que dans certains cas particuliers pour l'IT-Grundschutz du BSI. Les catalogues de cette protection de base décrivent par le menu la procédure permettant de réduire au maximum les risques. Quant aux normes ISO, elles laissent davantage de place à l'interprétation et offrent une plus grande souplesse, mais fournissent également des instructions et un soutien moins détaillés. À l'inverse, l'approche de l'IT-Grundschutz, comme son nom l'indique, offre une «protection de base». L'effort requis pour obtenir la certification ISO est moindre.
BSI IKS Security –Kompendium	2013	Éditeur: Bundesamt für Sicherheit in der Informationstechnik (BSI) Ce compendium est un ouvrage de référence destiné à faciliter l'accès à la sécurité informatique dans les ICS. Les bases ICS nécessaires, les processus y afférents, les normes pertinentes et un lien concret avec l'IT-Grundschutz y sont expliqués, les différences et lacunes des normes établies, et en particulier de l'IT-Grundschutz dans le domaine de la sécurité ICS étant mises en lumière.
BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)	2017	Éditeur: Bundesamt für Sicherheit in der Informationstechnik (BSI) Cette norme décrit les méthodes, les tâches et les activités pertinentes qui font le succès d'un SMSI et précise les tâches qui incombent à la direction. La méthodologie de l'IT-Grundschutz, qui explique pas à pas comment développer un SMSI dans la pratique et mentionne des mesures concrètes pour tous les aspects relevant de la sécurité de l'information, favorise la mise en œuvre des recommandations. La norme 200-1 s'adresse aux responsables de l'exploitation informatique, aux délégués à la sécurité, ainsi qu'aux experts et conseillers en sécurité chargés de la gestion de la sécurité de l'information.
BSI-Standard 200-2 IT-Grundschutz Vorgehensweise	2017	Éditeur: Bundesamt für Sicherheit in der Informationstechnik (BSI) La procédure de l'IT-Grundschutz décrit, étape par étape, comment mettre en place et exploiter un système de management de la sécurité de l'information dans la pratique et à l'aide des catalogues de cette protection de base. Elle se penche de façon très approfondie sur la manière d'élaborer en pratique un concept de sécurité, sur le choix des mesures de sécurité adéquates, ainsi que sur les éléments à prendre en compte lors de la mise en œuvre.
BSI-Standard 200-3 Risikoanalyse	2017	Éditeur: Bundesamt für Sicherheit in der Informationstechnik (BSI) Ce document décrit une méthodologie pour réaliser des analyses de risques, qui complètent un concept de sécurité existant en matière de protection de base des technologies de l'information. Les dangers présentés dans les catalogues de l'IT-Grundschutz sont utilisés comme outils. Une différence essentielle par rapport à la plupart des autres méthodes d'analyse de risques est l'omission totale de la probabilité de survenance des dommages.
BSI-Standard 100-4 Notfallorganisation	2008	Éditeur: Bundesamt für Sicherheit in der Informationstechnik (BSI) Ce document décrit une méthodologie pour mettre en place un système de gestion des cas d'urgence fondée sur les procédures figurant dans la norme 100-2 et les complétant. Il présente tous les processus au sein d'une organisation pour cas d'urgence, de l'analyse d'impact sur les affaires à la gestion de crise, en passant par le retour à l'exploitation normale et les activités continues de processus en dehors des situations de crise.
ISA 95 / CEI/ISO 62264 Intégration du système de commande d'entreprise	2010 ss	Éditeur: International Society of Automation (ISA) / Commission électrotechnique internationale (CEI) Série de cinq normes relatives à l'intégration des systèmes informatiques d'entreprise et de contrôle-commande.
Energy Sector Cybersecurity Framework Implementation Guidance	2015	Éditeur: Department of Energy (DOE) Instructions du Département américain de l'Énergie (DOE) pour la mise en œuvre d'un cadre de cybersécurité des infrastructures critiques basé sur le cadre du NIST.
Report on Cyber-Security Information Sharing in the Energy Sector	2017	Éditeur: Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)



Titre	An- née	Éditeur et description
		Ce rapport a pour objectif de comprendre et d'en savoir plus sur le développement des CSIRT (Computer Security Incident Response Teams) et des ISAC (Information Sharing and Analysis Centres), ainsi que sur les initiatives pertinentes concernant l'échange d'informations sur les incidents de cybersécurité dans le secteur de l'énergie. Il se concentre sur les sous-secteurs de l'électricité, du pétrole et du gaz identifiés dans la directive NIS (Parlement européen et Conseil, 2016: sécurité des réseaux et des systèmes d'information).
Communication network dependencies for ICS/SCADA Systems	2017	Éditeur: Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) Ce rapport se focalise sur les aspects des réseaux de communication et de l'intercommunication entre les systèmes ICS/SCADA et l'identification des vulnérabilités, des risques, des menaces et des conséquences en matière de sécurité pouvant être causés par les systèmes cyber-physiques. Il comporte également un certain nombre de recommandations destinées à réduire les risques détectés. La principale conclusion de l'étude préliminaire est une liste de pratiques et de directives éprouvées visant à limiter autant que possible la surface des systèmes ICS/SCADA exposée aux attaques. Le document a pour objectif principal de fournir un aperçu des dépendances des réseaux de communication des systèmes ICS/SCADA et d'identifier les ressources critiques en matière de sécurité et les scénarios d'attaques et menaces réalistes contre ces réseaux de communication.
VDI/VDE 2182 Informationssicherheit in der industriellen Automatisierung (IT-security for industrial automation)	2011 - 2020	Éditeur: Verein Deutscher Ingenieure (VDI) / Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) Cette directive explique comment atteindre la sécurité de l'information des machines et installations automatisées par la mise en œuvre de mesures de protection concrètes. Pour ce faire, les aspects des dispositifs, systèmes et applications d'automatisation utilisés sont pris en compte. Une procédure uniforme et réalisable précisant comment garantir la sécurité informatique tout au long du cycle de vie des dispositifs, systèmes et applications d'automatisation est décrite, sur la base d'une définition commune des termes convenus entre leurs fabricants et leurs utilisateurs (p. ex. constructeurs de machines, intégrateurs et exploitants). Le cycle de vie couvre les phases de développement, d'intégration, d'exploitation, de migration et de mise hors service. Cette directive définit un modèle de procédure simple pour le traitement et la présentation de la sécurité de l'information, modèle qui comprend plusieurs étapes de processus.

