



Handbuch

# Leitfaden zur Steigerung der IKT-Resilienz in der Strombranche

Der «Weg zum Ziel» zur Steigerung der IKT-  
Resilienz in der Strombranche

LVR – CH 2024



# Impressum und Kontakt

## Herausgeber

Verband Schweizerischer Elektrizitätsunternehmen VSE  
Hintere Bahnhofstrasse 10  
CH-5000 Aarau  
Telefon +41 62 825 25 25  
Fax +41 62 825 25 26  
info@strom.ch  
www.strom.ch

## Autoren der Erstausgabe

Stefan Mattmann	CKW AG	Autor
Reto Amsler	ALSEC AG	Co-Autor

## Mitarbeit durch folgende VSE Cyber Security Task Force Experten

Mattia Bardelli	AET	Mitglied VSE Cyber Security Task Force
Reto Bondolfi	EWZ	Mitglied VSE Cyber Security Task Force
Marc Engeli	EKZ	Mitglied VSE Cyber Security Task Force
Christian Gubler	VSE	Mitglied VSE Cyber Security Task Force
Stéphane Henry	BFE	Mitglied VSE Cyber Security Task Force
René Hugentobler	BKW	Mitglied VSE Cyber Security Task Force
Dimitri Klimov	Alpiq	Mitglied VSE Cyber Security Task Force
Michael Knuchel	Swissgrid	Mitglied VSE Cyber Security Task Force
Renald Marmet	BKW	Mitglied VSE Cyber Security Task Force
Dominik Märki	Axpo	Mitglied VSE Cyber Security Task Force
Adrian Märklin	Swisspower	Mitglied VSE Cyber Security Task Force
Michele Paganini	Repower	Mitglied VSE Cyber Security Task Force
Markus Riner	VSE	Mitglied VSE Cyber Security Task Force

## Verantwortung Kommission

Für die Pflege und die Weiterentwicklung des Dokuments zeichnet die VSE-Task Force Cyber Security verantwortlich.



# Chronologie

Datum	Kurzbeschreibung
15.01.2024	Version 0.1 Erstausgabe im Entwurf
28.02.2024	Versionen 0.1 ... 0.5 Reviews durch VSE Cyber Security Task Force
15.03.2024	Version 1.0 zur Übersetzung und Vernehmlassung / Freigabe
19.09.2024	Version 1.1 Anpassungen nach Rückmeldungen / Review

Das Dokument wurde unter Einbezug und Mithilfe von VSE und Branchenvertretern erarbeitet.

Der VSE verabschiedete das Dokument am 21.10.2024.

---

**Druckschrift** Nr. LVR/DE, Ausgabe 2024

## Copyright

© Verband Schweizerischer Elektrizitätsunternehmen VSE

Alle Rechte vorbehalten. Gewerbliche Nutzung der Unterlagen ist nur mit Zustimmung vom VSE/AES und gegen Vergütung erlaubt. Ausser für den Eigengebrauch ist jedes Kopieren, Verteilen oder anderer Gebrauch dieser Dokumente als durch den bestimmungsgemässen Empfänger untersagt. Die Autoren übernehmen keine Haftung für Fehler in diesem Dokument und behalten sich das Recht vor, dieses Dokument ohne weitere Ankündigungen jederzeit zu ändern.

## Sprachliche Gleichstellung der Geschlechter.

Das Dokument ist im Sinne der einfacheren Lesbarkeit in der männlichen Form gehalten. Alle Rollen und Personenbezeichnungen beziehen sich jedoch sowohl auf Frauen wie auch auf Männer. Wir danken für Ihr Verständnis.



# Inhaltsverzeichnis

Vorwort .....	10
Einleitung .....	11
1. Ausgangslage .....	12
1.1 Ziel, Zweck und Umfang .....	13
1.2 Zielpublikum .....	14
1.3 Struktur des Dokuments .....	15
1.4 Tips, Hinweise, Aufforderungen und Informationen .....	15
2. Einführung .....	16
2.1 Kontinuierliche Verbesserung der IKT-Resilienz .....	16
2.2 Abgrenzung .....	17
2.3 Hintergrund .....	17
2.4 Bedrohungen und Risiken .....	18
3. Umfeld Stromversorgung zur Steigerung der IKT-Resilienz .....	19
3.1 VSE-Regelwerk für die Strombranche zur Steigerung der IKT-Resilienz .....	19
3.2 Player / Stakeholder .....	19
3.2.1 Stakeholder auf Bundesebene .....	19
3.2.2 Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) .....	20
3.2.3 Energieversorger EVU (Bereich Strom) .....	20
3.2.4 CERT, CIRT, CSIRT und SOC .....	20
3.2.5 Hersteller und Lieferanten .....	21
3.3 Gesetzliche Grundlagen: Verpflichtende Gesetze und Verordnungen .....	23
3.3.1 Übersicht der gesetzlichen Gesetze, Verordnungen und Bestimmungen in Zusammenhang mit der Versorgungs- und Informationssicherheit .....	23
3.3.2 BABS Nationale Strategie zum Schutz kritischer Infrastrukturen .....	24
3.3.3 BABS Leitfaden Schutz kritischer Infrastrukturen .....	25
3.3.4 BWL IKT-Minimalstandard zur Verbesserung der IKT-Resilienz .....	25
3.3.5 BWL IKT-Minimalstandard - Assessment Tool nach NIST CSF 1.1 .....	26
3.3.6 BFE Verpflichtung des IKT-Minimalstandards zur Steigerung der IKT-Resilienz .....	28
3.3.6.1 Schutzniveau gemäss BFE .....	29
3.3.6.2 Zuweisung der Checkpoints auf Stufe Subkategorie zu den einzelnen Kategorien und festgelegt Schutzniveauwerte für die einzelnen Maturitäten (Tiers) .....	30
3.3.7 ElCom: Überwachung des Vorgehens und der Ergebnisse zur Steigerung der IKT- Resilienz .....	31
3.3.8 Bundesamt für Cybersicherheit (BACS): Meldepflicht und Unterstützung .....	32
3.3.8.1 Meldepflicht für kritische Infrastrukturen .....	32
3.3.8.2 Pflicht des Bundes zur Unterstützung bei Cyberangriffen .....	32
3.4 Institutionen, Frameworks, Normen, Standards, Spezifikation und Anleitungen (Guidelines) zur Steigerung der IKT-Resilienz .....	33
3.4.1 Frameworks, Normen, Standards und Spezifikationen .....	33
3.4.2 Guidelines und spezielle Publikationen .....	33
3.5 Zertifizierungen und Weiterbildungen zur Steigerung der IKT-Resilienz .....	34
3.5.1 Aus- und Weiterbildungen mit Zertifizierungen .....	35
3.5.1.1 VSE IT-/OT-Cyber-Security für System-Engineers .....	35
3.5.1.2 Ausbildungsangebot des VSE im Rahmen des Leitfadens .....	35
3.5.1.3 Weitere Aus- und Weiterbildungsmöglichkeiten .....	35
3.5.2 Sicherheitszertifizierungen für Unternehmen und Organisationseinheiten .....	36
3.5.2.1 Zertifizierung des ISMS nach ISO 27001 .....	36
3.5.2.2 Zertifizierung der Anwendung des NIST Cyber Security Frameworks .....	36
4. Basis die für Effektivität zur Verbesserung der IKT-Resilienz .....	37
4.1 Das Integrierte Management System IMS .....	37
4.2 Informationssicherheitsmanagement (ISM) als Basis zur Steigerung der IKT-Resilienz .....	38
4.3 Managementsystem für Sicherheit und Gesundheit bei der Arbeit zur Unterstützung der Steigerung der IKT-Resilienz .....	39



4.4	Prozess-, Risiko-, Business Continuity- und Notfallmanagement als weitere Grundlagen zur Steigerung der IKT-Resilienz .....	39
4.4.1	Prozessmanagement .....	39
4.4.2	Risikomanagement .....	40
4.4.3	Business Continuity Management (BCM) .....	41
4.4.3.1	Business Impact Analyse (BIA) .....	42
4.4.4	Notfallmanagement .....	43
4.5	Cyber-Security-Strategie nach Defense in Depth .....	43
5.	Grundlagen zur Steigerung der IKT-Resilienz .....	44
5.1	Grundsätzliches Verständnis zur Vorgehensweise .....	44
5.2	Komplexität und Umfang der Informationssicherheit zur Steigerung der IKT-Resilienz .....	45
5.3	Aufwand für die Informationssicherheit zur Steigerung der IKT-Resilienz .....	45
5.4	Grundlagen einer erfolgreichen Steigerung der IKT-Resilienz .....	47
5.4.1	Notwendige Elemente einer erfolgreichen Steigerung der IKT-Resilienz .....	47
5.4.2	Ausreichende Ressourcen zur Steigerung der IKT-Resilienz .....	47
5.4.3	Integriertes Managementsystem (IMS) .....	48
5.4.4	Steigerung der IKT-Resilienz nach dem Deming-Zyklus .....	49
5.4.5	Informationssicherheit: Politik und Strategie .....	50
5.4.5.1	Informationssicherheitspolitik (ISP) .....	50
5.4.5.2	Informationssicherheitsstrategie (ISS) .....	51
5.4.6	Informationssicherheit: Verantwortung .....	52
5.4.6.1	Verantwortlichkeiten nach dem RASCI-Modell .....	53
5.4.7	Informationssicherheit: Organisation und Organigramm .....	54
5.4.7.1	Funktionen des Sicherheitsorganigramms auf strategischer Ebene: .....	55
5.4.7.2	Funktionen des Sicherheitsorganigramms auf taktischer Ebene: .....	55
5.4.7.3	Funktionen des Sicherheitsorganigramms auf operativer Ebene: .....	56
5.4.7.4	Übergreifende Elemente der Sicherheitsorganigramm über alle Ebenen: .....	60
5.4.8	Informationssicherheit: House of Processes .....	61
5.4.8.1	Aufbau des House of Processes .....	62
5.4.8.2	Verantwortlichkeiten und Zuständigkeiten im House of Processes .....	65
5.4.9	Informationssicherheit: House of Policies .....	65
5.4.9.1	Aufbau des House of Policies .....	65
5.4.9.2	Verantwortlichkeiten und Zuständigkeiten im House of Policies .....	67
5.4.9.3	Vorgaben und Nachweise .....	67
5.4.9.4	Dokumentenlenkung im House of Policy .....	67
5.4.9.5	Übersicht der Dokumente im House of Policy zur Steigerung der IKT Resilienz auf Level 0 - 3 .....	68
5.4.9.6	Mapping des House of Policies mit dem NIST CSF 1.1 .....	69
5.4.9.7	Mapping der ISO 27001:2022 Annex A mit den Dokumenten im House of Policy .....	70
5.4.9.8	Aufgelistete Vorgaben und Nachweise im House of Policy .....	70
5.4.10	Information Security Management System (ISMS) .....	70
5.4.10.1	Gründe für den Aufbau eines ISMS: .....	70
5.4.10.2	Der Aufbau eines ISMS .....	71
5.4.10.3	ISMS nach ISO 27001 .....	72
5.4.10.4	Die VSE Phasen für die Einführung eines ISMS .....	73
5.4.11	Informationssicherheit: NIST CSF Version 1.1 .....	74
5.4.12	Informationssicherheit: Vernetzung des ISMS mit dem NIST CSF 1.1 .....	74
5.4.13	Informationssicherheit: Zusammenarbeit .....	75
5.5	Tools zur Steigerung der IKT-Resilienz .....	76
5.5.1	VSE-Tools zur Steigerung der IKT-Resilienz .....	77
5.5.2	Weitere erhältliche Tools als Hilfe zur Steigerung der IKT-Resilienz .....	78
6.	Vorgehen zur Steigerung der IKT-Resilienz: Einführung des ISMS mit der Vernetzung des NIST CSF 1.1 .....	78
6.1	Phase 1: Basis und Planung; Entschluss ISMS; Ziele festlegen .....	80
6.1.1	Sensibilisierung und Verpflichtung der obersten Führungsebene für die Informationssicherheit .....	80



6.1.2	Identifikation von Interessengruppen (Stakeholder) .....	81
6.1.3	Rechtliche und regulatorische Anforderungen aufzeigen und anwenden .....	81
6.1.4	Anwendbarkeit definieren (Assessment-Tools) .....	82
6.1.5	Geschäftsprozesse aufzeigen und ableiten .....	83
6.1.6	Handlungsfelder für die Informationssicherheit aufzeigen.....	84
6.1.7	Fokus für die Informationssicherheit definieren / anpassen .....	85
6.1.8	Grundsatzentscheid für die Einführung eines ISMS auf Stufe Konzern- oder Geschäftsleitung (C-Level) .....	86
6.1.9	Ziele des ISMS definieren und initiieren .....	87
6.2	Phase 2: Führung und Initialisierung; Standortbestimmung .....	88
6.2.1	Erstellen und Einführen der Politik und Strategie zur Informationssicherheit: Wie ist die Informationssicherheit zu behandeln? .....	88
6.2.2	Rahmen der Informationssicherheit festlegen: Erstellen einer Direktive zur Informationssicherheit und eine Richtlinie zum Rahmen der Informationssicherheit .....	89
6.2.3	Schaffung der Voraussetzungen .....	89
6.2.4	Ermittlung des Status Quo / IST-Analyse im Bereich Informationssicherheit durchführen ..	90
6.2.5	Geltungsbereich des gesamten ISMS festlegen .....	90
6.2.6	Sicherheitsorganisation aufbauen und anpassen.....	91
6.2.7	Verantwortlichkeiten definieren / anpassen .....	91
6.2.8	Leistungsindikatoren (KPI) definieren.....	92
6.2.9	Vorgehen für Audits definieren .....	92
6.3	Phase 3: Planung Aufbau und Ablauf; Sensibilisierung und Schulungen; Definition 'SOLL' .....	93
6.3.1	ISMS einführen, anpassen und erweitern.....	93
6.3.2	Dokumentenlenkung einführen / anpassen .....	94
6.3.3	Baseline-Dokumente mit Fokus auf die Baseline des ISMS (Richtlinien, Guidelines, Arbeitsanleitungen usw.) erstellen, ergänzen und anpassen .....	94
6.3.4	Sicherheitsorganisation etablieren / befähigen / anpassen .....	96
6.3.5	Einbinden aller Mitarbeitenden für die Etablierung einer unternehmensweiten Sicherheitskultur .....	97
6.3.6	Awareness & Schulungen einführen / erweitern / anpassen .....	97
6.3.7	Das 'Soll' für die Informationssicherheit definieren (Definition des "Ziel") .....	98
6.3.8	Massnahmenkatalog erstellen, Festlegen der anzuwendenden Massnahmen.....	99
6.3.9	Audits planen .....	100
6.4	Phase 4: Bestandesaufnahme; Bestimmung 'IST' .....	101
6.4.1	Detailliertes Inventar erheben .....	101
6.4.2	Identifizierung der Wirkungskette .....	102
6.4.3	Umgesetzte Massnahmen zur Informationssicherheit ermitteln.....	103
6.4.4	«IST-Audits» Ist-Zustand der Informationssicherheit ermitteln.....	103
6.4.5	IST-Assessment durchführen .....	104
6.4.6	Risikoregister erstellen.....	105
6.4.7	Baseline für KPI ermitteln .....	105
6.5	Phase 5: IST-SOLL-Gap-Analyse; Schutzbedarf- und Risikoanalyse .....	106
6.5.1	IST-SOLL-Gap-Analyse .....	106
6.5.2	Schutzbedarf für zusätzlichen Geltungsbereich im ISMS definieren.....	107
6.5.3	Risikomanagement-Methodik festlegen.....	107
6.5.4	Risikokategorien und -kriterien festlegen.....	108
6.5.5	Bestimmung der Risikoeigentümer (Risk-Owner) .....	108
6.5.6	Risikomanagement durchführen .....	109
6.5.7	Risikoanalyse auf TOP-Bedrohungen .....	109
6.6	Phase 6: Priorisierung, Etablierung und Umsetzung der Massnahmen; Betrieb .....	110
6.6.1	Massnahmenplan aus GAP- oder Risikoanalyse erarbeiten .....	110
6.6.2	Massnahmen priorisieren .....	111
6.6.3	Personelle Anforderungen und Kompetenzen festlegen .....	112
6.6.4	Massnahmenumsetzung gemäss Priorisierung durchführen .....	112
6.6.5	Kommunikations-, Trainings- und Awareness Massnahmen umsetzen.....	113
6.6.6	Kontinuierlichen Umsetzung der Massnahmen .....	113
6.7	Phase 7: Feststellen der Wirksamkeit; Messen und Steuern .....	115



6.7.1	Umgesetzte Massnahmen auf ihre Wirksamkeit überprüfen .....	115
6.7.2	Interne sowie Lieferanten-Audits durchführen .....	115
6.7.3	Überwachung des ISMS .....	116
6.7.4	Leistungsindikatoren (KPI) behandeln .....	117
6.7.5	Regelbetrieb mit Monitoring und Reporting etablieren .....	117
6.7.6	Dokumentationsprozesse sicherstellen .....	118
6.8	Phase 8: Verbesserungen .....	119
6.8.1	Korrektur und Vorbeugungsmassnahmen .....	119
6.8.2	Prüfung von Verbesserungsmöglichkeiten .....	119
6.8.3	Kontinuierlicher Verbesserungsprozess leben .....	120
7.	Zusammenspiel der VSE Dokumente und der VSE-Tools .....	121
8.	Schlussfolgerung und Zusammenfassung .....	122
Anhang A:	Glossar .....	123
Anhang B:	Abkürzungsverzeichnis .....	131
Anhang C:	Gesetzliche Grundlagen: Verpflichtende Gesetze und Verordnungen .....	133
C.0	Nationale Ebene .....	133
C.1	Internationale Ebene .....	138
Anhang D:	Institutionen, Frameworks, Normen, Standards, Spezifikation und Anleitungen (Guidelines) zur Steigerung der IKT-Resilienz .....	139
D.0	Organisationen und Institutionen .....	139
D.1	Frameworks .....	143
D.2	Spezifische wichtige Standards und Normen .....	146
Anhang E:	VSE-Tools zur Steigerung der IKT-Resilienz .....	149
E.0	VSE & BFE Assessment-Tool NIST CSF 1.1 ++ inkl. SoA, Maturitäten gemäss BFE und Hilfen für Umsetzung .....	149
E.0.1	Ziel und Zweck .....	149
E.0.2	Register "Dokument Owner & History" .....	149
E.0.3	Register "Assessment NIST CSF 1.1 ++" .....	149
E.0.4	Grafische Auswertung in den "Results"-Registern .....	150
E.0.5	Register "Assistance Information" .....	150
E.1	VSE&BFE-Tool for NIST-CSF-1.1 Checkpoints acc.to NIST-SP800-53_CCM_CIS .....	151
E.1.1	Ziel und Zweck .....	151
E.1.2	Register "Dokument Owner & History" .....	151
E.1.3	Register "All Functions", "IDENTIFY (ID)", "PROTECT (PR)", "DETECT (DE)", "RESPOND (RE)" und "RECOVER (RC)" .....	151
E.1.4	Register "Assistance Information" .....	152
E.2	VSE-Tool NIST CSF 1.1 HoP-Mapping .....	152
E.2.1	Register "Dokument Owner & History" .....	152
E.2.2	Register "All Function HoP" .....	153
E.3	VSE Assessment-Tool ISO27001 Annex A incl. Controls acc.to ISO27002 .....	153
E.3.1	Ziel und Zweck .....	153
E.3.2	Register "Dokument Owner & History" .....	153
E.3.3	Register "Assessment Tool ISO 27001" .....	154
E.3.4	Grafische Auswertung in den "Graphics All Area"-Register .....	154
E.3.5	Register "Assistance Information" .....	155
E.4	VSE Assessment-Tool ISO27001 ISMS-Goals incl. HoP-Mapping .....	155
E.4.1	Ziel und Zweck .....	155
E.4.2	Register "Dokument Owner & History" .....	155
E.4.3	Register "Assessment ISMS Goals" .....	155
E.4.4	Grafische Auswertung in den "Graphics ISMS Goals"-Register .....	156
E.4.5	Register "Assistance Information" .....	156
E.5	VSE-Tool ISO27001 Annex A HoP-Mapping .....	157
E.5.1	Register "Dokument Owner & History" .....	157
E.5.2	Register "All Function HoP" .....	157



E.6	VSE-Tool IMS HoP-Dokumentenverzeichnis .....	157
Anhang F:	Beschreibung der Vorgaben im House of Policy Level 0 bis 3 .....	158
F.0	House of Policy auf Level 0: Politik (Verwaltungsrat / Konzernleitung) .....	158
F.1	House of Policy auf Level 1: Weisungen und Direktiven (Geschäftsleitung, C-Level) .....	158
F.2	House of Policy auf Level 2: Richtlinien und Guidelines (CISO, CRO, DPO) .....	159
F.3	House of Policy auf Level 3: Arbeitsanleitungen und Instructions (ISO, ISC und Cyber Security Team) .....	161
Anhang G:	Weiterführende Literatur .....	171

## Abbildungsverzeichnis

<b>Abbildung 1:</b>	Der Weg zum Ziel (Quelle BFE)	11
<b>Abbildung 2:</b>	Top 10 Geschäftsrisiken weltweit 2022 von Allianz (Quelle Allianz)	12
<b>Abbildung 3:</b>	VSE-Regelwerk für die Strombranche zur Steigerung der IKT-Resilienz (Quelle VSE)	19
<b>Abbildung 4:</b>	Steigerung der Cybersicherheit (Quelle BWL)	26
<b>Abbildung 5:</b>	Auszug aus dem Assessment-Tool zum BWL IKT-Minimalstandard (Quelle BWL)	27
<b>Abbildung 6:</b>	BWL IKT-Minimalstandard Maturitäten (Quelle BWL)	28
<b>Abbildung 7:</b>	Ablaufschema Umsetzung Cybersicherheit-Minimalanforderungen (Quelle ElCom)	32
<b>Abbildung 8:</b>	Integriertes Management System IMS (Quelle TÜV Süd)	37
<b>Abbildung 9:</b>	Die notwendigen Elemente für eine erfolgreiche Steigerung der IKT-Resilienz (Quelle VSE)	47
<b>Abbildung 10:</b>	IMS (Quelle TÜV NORD)	48
<b>Abbildung 11:</b>	PDCA Deming-Zyklus (Quelle VSE)	49
<b>Abbildung 12:</b>	Verantwortung (Quelle weka.ch)	51
<b>Abbildung 13:</b>	Verantwortung (Quelle meinekrankenkasse.de)	52
<b>Abbildung 14:</b>	Prinzipielle Struktur eines möglichen Sicherheitsorganigramms (Quelle VSE)	54
<b>Abbildung 15:</b>	Struktur im House of Prozess (Quelle VSE)	62
<b>Abbildung 16:</b>	Prozesse im House of Processes (Quelle VSE)	64
<b>Abbildung 17:</b>	Prinzipieller Aufbau des House of Policy mit dem Mapping zum NIST CSF 1.1 (Quelle VSE)	66
<b>Abbildung 18:</b>	Vorgaben und Nachweise mit fließendem Übergang (Quelle VSE)	67
<b>Abbildung 19:</b>	Dokumente im House of Policy auf Level 0 bis 3 (Quelle VSE)	68
<b>Abbildung 20:</b>	Maturitätsspirale des ISMS	72
<b>Abbildung 21:</b>	VSE-Phasen für die Einführung des ISMS (Quelle VSE)	73
<b>Abbildung 22:</b>	NIST Cybersecurity Framework	74
<b>Abbildung 23:</b>	Vernetzung ISMS mit NIST CSF	74
<b>Abbildung 24:</b>	Zusammenarbeit (Quelle allegra Blog)	75
<b>Abbildung 25:</b>	Detaillierter Regelkreis der acht VSE-Phasen zur Einführung und Betrieb des ISMS (Quelle VSE)	79
<b>Abbildung 26:</b>	Prozesse in Unternehmen und Organisationseinheiten (Quelle VSE)	84
<b>Abbildung 27:</b>	Festlegen des Fokus gemäss Strom VV (Quelle VSE)	85
<b>Abbildung 28:</b>	Zusammenspiel der VSE-Dokumente mit den VSE-Tools zur Steigerung der IKT-Resilienz (Quelle VSE)	121





## Tabellenverzeichnis

<b>Tabelle 1:</b> Stakeholder auf Bundesebene (Quelle VSE)	20
<b>Tabelle 2:</b> Definition der Unternehmensprofile nach Strom VV (Quelle BFE/VSE)	30
<b>Tabelle 3:</b> Verantwortlichkeiten nach RASCI (Quelle VSE)	53
<b>Tabelle 4:</b> Verantwortlichkeiten und Zuständigkeiten im House of Processes (Quelle VSE)	65
<b>Tabelle 5:</b> Verantwortlichkeiten und Zuständigkeiten im House of Policy (Quelle VSE)	67
<b>Tabelle 6:</b> Mapping House of Policy mit den Ebenen im NIST CSF 1.1	69
<b>Tabelle 7:</b> ISMS Phase 1: Basis und Planung; Entschluss ISMS; Ziele festlegen	80
<b>Tabelle 8:</b> ISMS Phase 2: Führung und Initialisierung; Standortbestimmung	88
<b>Tabelle 9:</b> ISMS Phase 3: Planung Aufbau und Ablauf; Sensibilisierung und Schulungen; Definition 'SOLL'	93
<b>Tabelle 10:</b> ISMS Phase 4: Bestandesaufnahme; Bestimmung 'IST'	101
<b>Tabelle 11:</b> ISMS Phase 5: IST-SOLL-Gap-Analyse; Schutzbedarf- und Risikoanalyse	106
<b>Tabelle 12:</b> ISMS Phase 6: Priorisierung, Etablierung und Umsetzung der Massnahmen; Betrieb	110
<b>Tabelle 13:</b> ISMS Phase 7: Feststellen der Wirksamkeit; Messen und Steuern	115
<b>Tabelle 14:</b> ISMS Phase 8: Verbesserungen	119



## Vorwort

Beim vorliegenden Dokument handelt es sich um ein Branchendokument des VSE. Es ist Teil eines umfassenden Regelwerkes für die Elektrizitätsversorgung im offenen Strommarkt. Branchendokumente beinhalten branchenweit anerkannte Richtlinien und Empfehlungen zur Nutzung der Strommärkte und der Organisation des Energiegeschäftes und erfüllen damit die Vorgabe des Stromversorgungsgesetzes (StromVG) sowie der Stromversorgungsverordnung (StromVV) an die Energieversorgungsunternehmen (EVU).

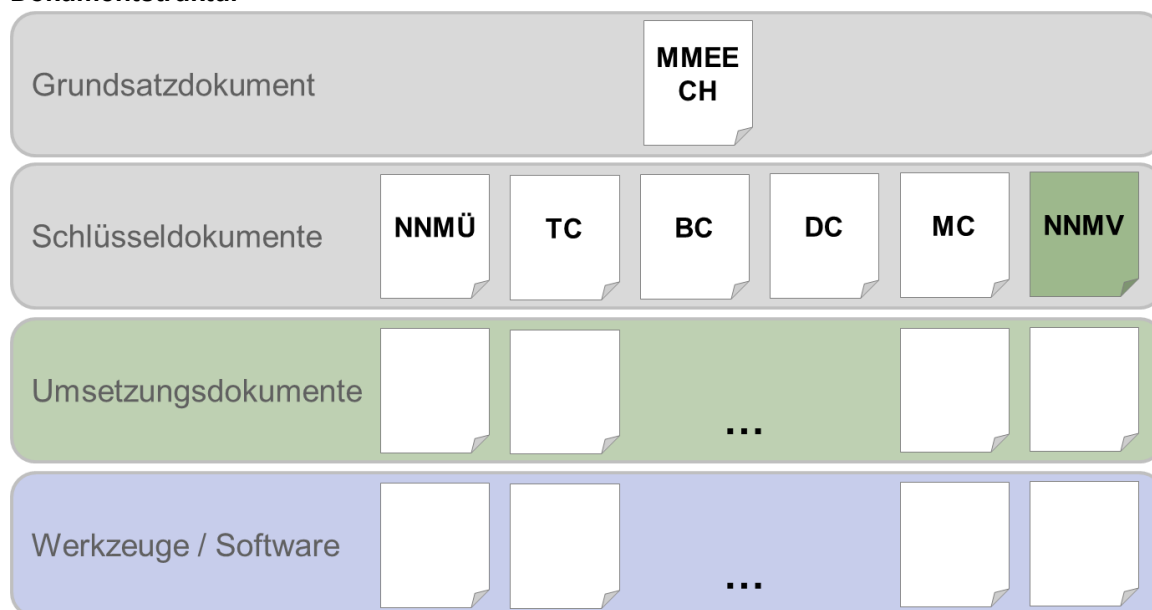
Branchendokumente werden von Branchenexperten im Sinne des Subsidiaritätsprinzips ausgearbeitet, regelmässig aktualisiert und erweitert. Bei den Bestimmungen, welche als Richtlinien im Sinne des StromVV gelten, handelt es sich um Selbstregulierungsnormen.

Die Dokumente sind hierarchisch in vier unterschiedliche Stufen gegliedert

- Grundsatzdokument
- Schlüsseldokumente
- Umsetzungsdokumente: Leitfaden zur Steigerung der IKT-Resilienz in der Strombranche
- Werkzeuge/Software

Beim vorliegenden Dokument «Leitfaden zur Steigerung der IKT-Resilienz in der Strombranche» handelt es sich um ein Umsetzungsdokument.

### Dokumentstruktur



## Einleitung

- (1) In der heutigen digitalen Welt sind Informations- und Kommunikationstechnologien (IKT) von entscheidender Bedeutung für den reibungslosen Betrieb von Unternehmen, Organisationseinheiten und Institutionen aller Art. Obwohl die technologischen Fortschritte uns zahlreiche Vorteile und Möglichkeiten bieten, sind wir gleichzeitig auch immer stärker den Herausforderungen und Risiken ausgesetzt, die mit einer hochgradig vernetzten und digitalen Umgebung einhergehen. IKT-Störungen, Cyberangriffe, Naturkatastrophen und menschliche Fehler können den Betrieb von IKT-Systemen und -Diensten gefährden und schwerwiegende Auswirkungen auf Unternehmen und Organisationseinheiten haben.
- (2) Die Notwendigkeit, unsere IKT-Systeme widerstandsfähiger gegenüber solchen Bedrohungen zu machen, steht daher im Zentrum unserer Bemühungen. Dieser Leitfaden zur Steigerung der IKT-Resilienz wurde entwickelt, um Unternehmen und Organisationseinheiten dabei zu unterstützen, ihre Fähigkeiten zu stärken, auf IKT-Störungen oder Katastrophen zu reagieren und sich davon zu erholen. Die Steigerung der IKT-Resilienz ist nicht nur eine Frage der Geschäftskontinuität, sondern auch der Sicherheit von Informationen, Datenschutz und dem Schutz des Ansehens einer Organisation.
- (3) In diesem Leitfaden werden wir Ihnen bewährte Praktiken und ein systematisches Vorgehen vorstellen, die Ihnen helfen sollen, Ihre IKT-Resilienz zu erhöhen. Wir werden auf die Schaffung einer Sicherheitskultur, die Identifizierung kritischer Ressourcen, die Entwicklung von Notfallplänen, die Schulung von Mitarbeitern und die kontinuierliche Verbesserung eingehen. Dieser Leitfaden ist für Führungskräfte, Cyber Security Verantwortliche, IT/OT-Verantwortliche, Sicherheitsbeauftragte und alle Mitarbeiter, die eine Rolle bei der Gewährleistung der IKT-Resilienz innehaben, konzipiert.
- (4) Die Steigerung der IKT-Resilienz ist keine optionale Massnahme, sondern eine unverzichtbare Verpflichtung gegenüber Ihrer Organisation, Ihren Kunden und Partnern. Sie stellt sicher, dass Sie in der Lage sind, unerwarteten Herausforderungen in der digitalen Welt souverän zu begegnen und den Betrieb aufrechtzuerhalten, selbst wenn die Umstände dies erschweren. Wir laden Sie ein, diesen Leitfaden als Werkzeug zur Stärkung Ihrer IKT-Resilienz zu nutzen und Ihre Organisation widerstandsfähiger und besser vorbereitet zu machen.

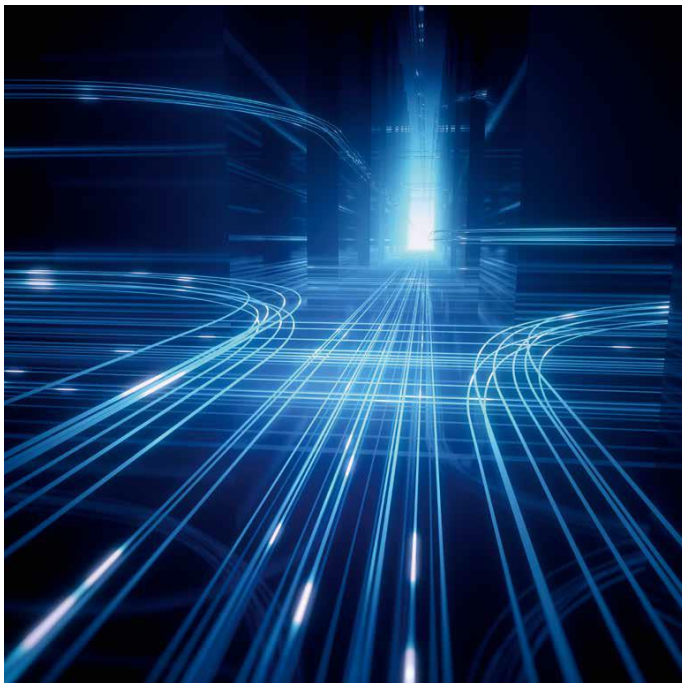


Abbildung 1: Der Weg zum Ziel (Quelle BFE)

Dieser Leitfaden beschreibt explizit

## "Den Weg zum Ziel"

und somit die Vorgehensweise, wie die IKT-Resilienz erhöht werden kann. Es wird bewusst nicht auf explizite Massnahmen an den Umgebungen, Systemen oder Netzwerken eingegangen.





## 1. Ausgangslage

- (1) In einer Ära, die von der rasanten Entwicklung der Informations- und Kommunikationstechnologien (IKT) geprägt ist, stehen Unternehmen und Organisationseinheiten vor beispiellosen Chancen und Herausforderungen. IKT bilden das Rückgrat unserer modernen Welt und sind ein Schlüsselbestandteil nahezu jeder geschäftlichen Aktivität. Die Vernetzung von Systemen, die Verlagerung von Diensten in die Cloud und die Abhängigkeit von digitalen Daten haben den Geschäftsbetrieb revolutioniert und die Effizienz gesteigert. Gleichzeitig haben sie jedoch eine erhöhte Anfälligkeit für Störungen und Cyberangriffe geschaffen, die den Geschäftsbetrieb gefährden und erhebliche Schäden verursachen können.
- (2) Die Ausgangslage ist geprägt von vielfältigen Risiken, darunter:
  - **Cyberangriffe:** Die Bedrohung durch Hacker, Malware und andere Cyberangriffe ist ständig präsent. Diese Angriffe können ein ganzes Unternehmen und Organisationseinheiten lahmlegen, Datenverluste verursachen und das Vertrauen von Kunden und Partnern gefährden.
  - **Naturkatastrophen:** Überschwemmungen, Erdbeben, Stürme und andere Naturkatastrophen können physische Schäden an IKT-Infrastrukturen verursachen und zu erheblichen Ausfallzeiten führen.
  - **Menschliches Versagen:** Selbst menschliche Fehler, sei es durch unachtsame Mitarbeiter oder unsachgemäße Handhabung von Technologien, können zu kritischen IKT-Störungen führen.
  - **Abhängigkeit von Drittanbietern:** Die Auslagerung von Diensten und die Abhängigkeit von Drittanbietern erhöhen das Risiko von Ausfällen und erhöhen die Anforderungen an das Management der Lieferketten.
  - **Gesetzliche und regulatorische Anforderungen:** Regierungen und Aufsichtsbehörden erlassen ständig neue Gesetze und Vorschriften, die Unternehmen und Organisationseinheiten zwingen, bestimmte Sicherheitsstandards und Datenschutzanforderungen einzuhalten.

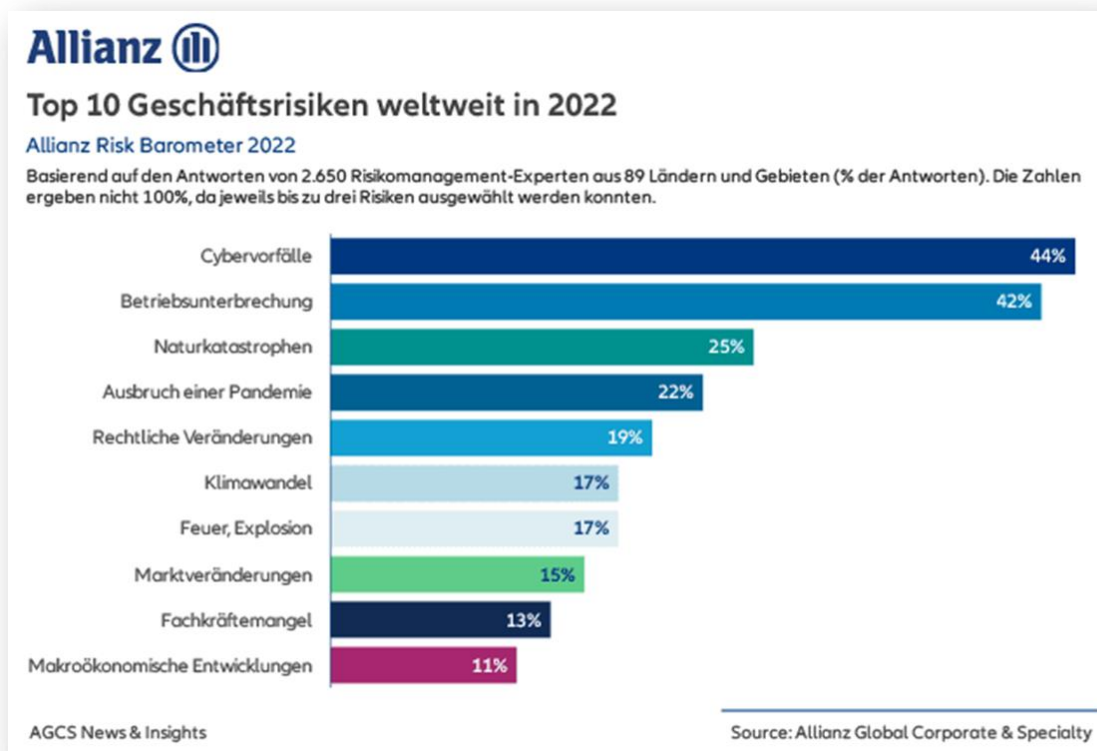


Abbildung 2: Top 10 Geschäftsrisiken weltweit 2022 von Allianz (Quelle Allianz)

- (3) Angesichts dieser Risiken und der unvermeidlichen Unsicherheiten, denen Unternehmen und Organisationseinheiten ausgesetzt sind, ist die Steigerung der IKT-Resilienz von entscheidender Bedeutung. Dies bedeutet, die Fähigkeit zu stärken, auf Störungen oder Katastrophen zu reagieren und den normalen

Betrieb aufrechtzuerhalten. Eine effektive IKT-Resilienz Strategie kann den Unterschied zwischen einem vorübergehenden Ausfall und einem langfristigen Schaden für die Organisation ausmachen.

- (4) Die Steigerung der IKT-Resilienz ist nicht nur eine Massnahme der Vorsicht, sondern eine strategische Notwendigkeit in der heutigen digitalen Welt. Dieser Leitfaden wurde entwickelt, um Unternehmen und Organisationseinheiten bei der Erreichung dieser Ziele zu unterstützen und ihnen die Werkzeuge und das Wissen an die Hand zu geben, um widerstandsfähiger gegenüber den Herausforderungen der digitalen Landschaft zu werden und diese proaktiv managen zu können.

## 1.1 Ziel, Zweck und Umfang

- (1) Der Leitfaden zur Steigerung der IKT-Resilienz (Informations- und Kommunikationstechnologie-Resilienz) hat das übergeordnete Ziel, die systematische Vorgehensweise aufzuzeigen wie die Fähigkeit eines Unternehmens und der Organisationseinheiten, auf IKT-Störungen oder Katastrophen zu reagieren und sich davon zu erholen, zu stärken. Die IKT-Resilienz umfasst die Fähigkeit, den Betrieb von IT-Systemen und -Diensten aufrechterhalten oder rasch wiederherstellen zu können, selbst wenn unerwartete Ereignisse eintreten. Hier sind die Ziele, die mit dem Leitfaden verfolgt werden sollen:
- **Kontinuität sicherstellen:** Die IKT-Resilienz sollte sicherstellen, dass die Organisation auch in Zeiten von Störungen, Cyberangriffen, Naturkatastrophen oder anderen unerwarteten Ereignissen den kontinuierlichen Betrieb ihrer IT/OT-Systeme und -Dienste aufrechterhalten kann.
  - **Risikominderung:** Durch die Umsetzung von Best Practices und Sicherheitsmassnahmen in Bezug auf IKT-Resilienz soll das Risiko von IT-Ausfällen oder Datenverlusten minimiert werden. Dies trägt zur Sicherheit und Integrität der Informationen bei.
  - **Reaktionsfähigkeit verbessern:** Die Organisation sollte in der Lage sein, schnell auf IKT-Störungen zu reagieren und Gegenmassnahmen zu ergreifen, um den Betrieb aufrechtzuerhalten. Hierzu gehören auch klare Notfallpläne und -prozeduren.
  - **Wiederherstellungsfähigkeit gewährleisten:** Selbst wenn Störungen oder Katastrophen eintreten, sollte die Organisation in der Lage sein, ihre IKT-Systeme und -Dienste rasch wiederherzustellen und den normalen Betrieb so schnell wie möglich fortzusetzen.
  - **Compliance und Vorschriften einhalten:** Die IKT-Resilienz-Richtlinien sollten sicherstellen, dass die Organisation alle relevanten gesetzlichen Anforderungen und Branchenstandards in Bezug auf Sicherheit und Datenschutz erfüllt.
  - **Bewusstsein schaffen:** Dieser Leitfaden zur Steigerung der IKT-Resilienz soll das Bewusstsein in der gesamten Organisation für die Bedeutung der IKT-Resilienz und die Verantwortlichkeiten aller Mitarbeiter in diesem Zusammenhang schärfen.
  - **Kontinuierliche Verbesserung:** Dieser Leitfaden soll dazu die Notwendigkeiten aufzeigen, die IKT-Resilienz kontinuierlich zu überwachen, zu bewerten und zu verbessern. Dies umfasst die Anpassung an sich ändernde Bedrohungen und Anforderungen.
  - **Minimierung von Ausfallzeiten:** Ziel ist es, Ausfallzeiten auf ein Minimum zu reduzieren, um die Produktivität der Organisation aufrechtzuerhalten und den finanziellen Schaden zu begrenzen, der durch IT/OT-Ausfälle entstehen kann.
  - **Schutz von Daten und Informationen:** Die IKT-Resilienz soll sicherstellen, dass Daten und Informationen in allen Situationen geschützt und verfügbar sind.
  - **Kommunikation und Zusammenarbeit:** Die Richtlinie soll klare Kommunikations- und Koordinationsmechanismen etablieren, um eine effektive Zusammenarbeit bei der Bewältigung von IKT-Störungen sicherzustellen.
  - **Ressourceneffizienz:** Die Leitlinien sollten sicherstellen, dass die Ressourcen zur Verbesserung der IKT-Resilienz effizient eingesetzt werden und dennoch wirksam sind.
- (2) Die systematische Steigerung der IKT-Resilienz nach diesem Leitfaden ist entscheidend, um sicherzustellen, dass Unternehmen und Organisationseinheiten auf unerwartete Herausforderungen im Zusammenhang mit Informations- und Kommunikationstechnologien vorbereitet sind und effektiv reagieren können.



Die genauen Ziele können je nach den spezifischen Anforderungen und Risiken der Unternehmen und Organisationseinheiten variieren.

- (3) Der Leitfaden dient dazu Unternehmen und Organisationseinheiten eine systematische Vorgehensweise zur Steigerung der IKT-Resilienz aufzuzeigen. Dabei wird als Grundlage das gesamte Umfeld eines Stromversorgungsunternehmens im Zusammenhang mit der IKT-Resilienz beleuchtet, um somit ein gemeinsames Verständnis zu schaffen. Er soll Unternehmen und Organisationseinheiten bei der Entwicklung und Umsetzung von Strategien und Massnahmen unterstützen, um ihre IKT-Resilienz nachhaltig zu erhöhen. Weiter soll es ihre Fähigkeit stärken, auf Cyberangriffe und resultierenden IKT-Fehlverhalten bzw. -Störungen oder Katastrophen angemessen zu reagieren und sich davon zu erholen.
- (4) Zur Stärkung der IKT-Resilienz kann der Umfang je nach den spezifischen Anforderungen und Risiken im Unternehmen und in den Organisationseinheiten variieren. Dieser umfassende Leitfaden zur Steigerung der IKT-Resilienz bietet eine klare Roadmap und eine umfassende Strategie.
- (5) **"Dieser Leitfaden beschreibt den Weg zum Ziel". Das Dokument soll in die Thematik einführen, gemeinsames Verständnis schaffen, Grundlagen aufzeigen und beschreiben, Vorgaben aufzeigen und beschreiben sowie das Vorgehen zur Steigerung der IKT-Resilienz beleuchten. Der Leitfaden wurde bewusst so umfangreich gestaltet, damit die Bedürfnisse aller Bedarfsträger abgedeckt werden können. Wichtige Elemente sind bewusst mehrmals aufgeführt, um unübersichtliche Verweise zu vermeiden.**

## 1.2 Zielpublikum

- (1) Das Zielpublikum für die Steigerung der IKT-Resilienz (Informations- und Kommunikationstechnologie-Resilienz) umfasst eine breite Palette von Akteuren innerhalb einer Organisation. Folgend werden die Hauptzielgruppen, die von Massnahmen zur Steigerung der IKT-Resilienz betroffen sind, beschrieben:
  - **Führungsebene und Geschäftsführung:** Dies sind die obersten Entscheidungsträger in der Organisation. Sie müssen das Engagement für IKT-Resilienz fördern, Ressourcen bereitstellen und die Richtung für die gesamte Organisation vorgeben.
  - **IT/OT-Abteilung und Technologieexperten:** Die IT/OT-Abteilung und technischen Experten haben eine Schlüsselrolle inne bei der Umsetzung der IKT-Resilienz Massnahmen. Sie sind für die Planung, Umsetzung und Überwachung von IKT-Sicherheitsmassnahmen verantwortlich.
  - **Sicherheits- und Compliance-Verantwortliche:** Diese Gruppe ist für die Einhaltung gesetzlicher Vorschriften und Sicherheitsstandards verantwortlich. Sie stellen sicher, dass die IKT-Resilienz im Einklang mit den gesetzlichen Anforderungen steht.
  - **Risikomanagement und Compliance-Experten:** Sie identifizieren und bewerten Risiken im Zusammenhang mit IKT und helfen bei der Entwicklung von Strategien zur Risikominderung.
  - **Mitarbeiter:** Alle Mitarbeiter in der Organisation spielen eine Rolle bei der IKT-Resilienz. Sie müssen die Sicherheitsrichtlinien und -verfahren einhalten und dazu beitragen, sicherheitsbewusstes Verhalten zu leben und zu fördern.
  - **Externe Dienstleister und Lieferanten:** Unternehmen und Organisationseinheiten, die externe Dienstleistungen oder Technologiekomponenten bereitstellen, sind ebenfalls relevant, da sie in den IKT-Resilienz Prozess einbezogen werden müssen.
  - **Interne und externe Prüfer und Auditoren:** Interne und externe Prüfer spielen eine Rolle bei der Überprüfung und Bewertung der IKT-Resilienz, um sicherzustellen, dass die Organisation angemessene Praktiken und Standards einhält.
  - **Kunden und Partner:** Die IKT-Resilienz kann Auswirkungen auf Kunden und Geschäftspartner haben. Daher ist es wichtig, diese Gruppen über geplante Änderungen oder Notfallpläne zu informieren.
  - **Behörden und Regulierungsstellen:** In einigen Branchen unterliegen Unternehmen und Organisationseinheiten speziellen gesetzlichen Anforderungen und Regulierungen im Zusammenhang mit der IKT-Resilienz. Behördliche Stellen können als Auditoren die Einhaltung der gesetzlichen Anforderungen überwachen und durchsetzen.





- **Notfallmanagement- und Notfallteams:** Diese Teams sind für die Bewältigung von IKT-Störungen und Krisen verantwortlich. Sie müssen in die IKT-Resilienz Strategien und Pläne mit einbezogen werden.
- (2) Das Zielpublikum für die Steigerung der IKT-Resilienz ist vielfältig und umfasst verschiedene Abteilungen, Ebenen und Interessengruppen innerhalb und ausserhalb der Organisation. Die Beteiligung und Zusammenarbeit dieser Gruppen sind entscheidend, um die IKT-Resilienz effektiv zu gestalten und sicherzustellen, dass die Organisation in der Lage ist, auf IT/OT-Störungen und Katastrophen angemessen zu reagieren.

### 1.3 Struktur des Dokuments

- (1) Bei der Struktur bzw. dem Aufbau des Dokumentes wurde ein pragmatischer Ansatz gewählt und der Leitfaden ist wie folgt aufgebaut:
- Einführung in die Thematik
  - Gemeinsames Verständnis schaffen
  - Grundsätze und Vorgaben zur Steigerung der IKT-Resilienz
  - Vorgehen zur Steigerung der IKT-Resilienz

### 1.4 Tips, Hinweise, Aufforderungen und Informationen

- (1) Der Leitfaden enthält Hinweiskfelder über welche die Autoren dem Leser hilfreiche Tipps, Hinweise, Empfehlungen oder Zusatzinformationen geben, welche essenziell bei der erfolgreichen Umsetzung des Leitfadens sind. Folgend werden die Hinweiskfelder beschrieben:



**Empfehlung der VSE Cyber Security Task Force Experten:**  
Diese Punkte helfen dem Anwender für eine systematische und effektive Steigerung der IKT-Resilienz aus Sicht der VSE Cyber Security Task Force Experten



Hier gibt es Hilfe durch ein Tool des VSE, welches verwendet werden soll



In den Beilagen gibt es Musterbeispiele, welches angewendet werden können



Hinweise auf weiterführende und ergänzende Dokumente



**Gesetzliche und regulatorische Grundlagen und Vorgaben, welche zwingend erfüllt werden müssen**



**Zusätzliche Informationen als Hilfe**



**Vorgaben und Hinweise, welche beachtet werden sollten**



**Vorgaben und Hinweise die zwingend beachtet und erfüllt werden müssen**



## 2. Einführung

- (1) Der Leitfaden zur Steigerung der IKT-Resilienz dient als umfassendes Handbuch, um Unternehmen und Organisationseinheiten bei der Stärkung ihrer Informations- und Kommunikationstechnologie gegenüber vielfältigen Bedrohungen zu unterstützen. Im Fokus steht eine proaktive Risikomanagement-Strategie, die Integration bewährter Informationssicherheitspraktiken und die Schaffung einer organisatorischen Resilienz Kultur. Der Leitfaden bietet klare Richtlinien, Werkzeuge und Schulungen, um die systematische Widerstandsfähigkeit der IKT-Infrastruktur zu verbessern und effektiv auf die dynamische Bedrohungslandschaft zu reagieren. Generell verfolgt der Leitfaden das Ziel die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (CIA-Triade) sicherzustellen, welche das Fundament der Informationssicherheit bilden. Vertraulichkeit gewährleistet, dass sensible Informationen nur autorisierten Personen zugänglich sind, indem der Zugriff und die Weitergaben kontrolliert werden. Integrität garantiert die Korrektheit und Vollständigkeit von Daten und Systemen, indem Manipulationen oder unerwünschte Änderungen verhindert oder erkannt werden. Verfügbarkeit stellt sicher, dass autorisierte Benutzer jederzeit auf Informationen und Ressourcen zugreifen können, ohne durch Ausfälle oder Angriffe behindert zu werden. Diese drei Ziele bilden die Grundlage für erweiterte Schutzziele wie Zurechenbarkeit, Verbindlichkeit und Authentizität, im Hinblick auf Herkunft und Empfänger im Falle einer Kommunikation. Durch die Berücksichtigung dieser erweiterten Ziele wird eine umfassende Sicherheitsstrategie entwickelt, die die gesamte Bandbreite der Bedrohungen adressiert und die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen gewährleistet.

### 2.1 Kontinuierliche Verbesserung der IKT-Resilienz

- (1) Die kontinuierliche Verbesserung der IKT-Resilienz (Informations- und Kommunikationstechnologie-Resilienz) ist ein Prozess, bei dem eine Organisation ständig bestrebt ist, ihre Fähigkeit zu stärken, auf IKT-Störungen oder Katastrophen zu reagieren und sich davon zu erholen. Dieser Prozess zielt darauf ab, die Widerstandsfähigkeit der IT-Infrastruktur und der technologischen Ressourcen einer Organisation kontinuierlich zu erhöhen. Hier ist eine Beschreibung der kontinuierlichen Verbesserung der IKT-Resilienz:
  - **Ziel und Zweck:** Die kontinuierliche Verbesserung der IKT-Resilienz hat das übergeordnete Ziel, die Organisation widerstandsfähiger gegenüber IKT-Störungen und Katastrophen zu machen. Dies bedeutet, die Fähigkeit zu stärken, den normalen Betrieb aufrechtzuerhalten oder so schnell wie möglich wiederherzustellen, selbst wenn unerwartete Ereignisse eintreten.
  - **Systematische Überprüfung:** Die Organisation führt regelmässige Überprüfungen und Evaluierungen ihrer IKT-Resilienz Praktiken durch. Dies kann interne Audits, Risikobewertungen und externe Prüfungen einschliessen. Ziel ist es, Schwachstellen und Verbesserungspotentiale zu identifizieren.
  - **Anpassung an Veränderungen:** Die kontinuierliche Verbesserung berücksichtigt die sich ändernde IT-Landschaft, technologische Entwicklungen und sich entwickelnde Bedrohungen. Die Organisation passt ihre IKT-Resilienz Strategien an, um auf neue Herausforderungen vorbereitet zu sein.
  - **Lernen aus Erfahrungen:** Jedes Ereignis, sei es ein IT-Ausfall, ein Sicherheitsvorfall oder eine Naturkatastrophe, bietet Lernmöglichkeiten. Die Organisation zieht aus diesen Erfahrungen Lehren und passt ihre Resilienz Strategien entsprechend an.
  - **Umsetzung von Best Practices:** Die kontinuierliche Verbesserung basiert auf bewährten Verfahren und Standards im Bereich der IKT-Resilienz, wie zum Beispiel ISO 27031 oder ISO 22301. Diese Praktiken dienen als Leitfaden für die Implementierung.
  - **Einbindung aller Interessengruppen:** Die kontinuierliche Verbesserung erfordert die aktive Beteiligung und das Engagement aller relevanten Akteure in der Organisation, einschliesslich der Geschäftsführung, IT-Experten, Sicherheitsbeauftragten und Mitarbeiter.
  - **Identifikation von Schlüssellressourcen:** Die Organisation identifiziert und klassifiziert kritische IT-Ressourcen und -Daten, um sicherzustellen, dass angemessene Schutz- und Wiederherstellungsmassnahmen implementiert werden.
  - **Entwicklung von Notfallplänen:** Im Rahmen der kontinuierlichen Verbesserung werden detaillierte Notfallpläne und -prozeduren erstellt, die im Falle von IKT-Störungen oder Katastrophen in Kraft treten.
  - **Schulung und Sensibilisierung:** Die Organisation schult ihr Personal und fördert das Bewusstsein für IKT-Resilienz, um sicherzustellen, dass Mitarbeiter in der Lage sind, sichere und resiliente Praktiken in ihrem täglichen Arbeitsumfeld umzusetzen.



- **Regelmässige Überprüfung und Aktualisierung:** Die IKT-Resilienz Strategien und -pläne werden regelmässig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Anforderungen und Bedrohungen entsprechen.
- (2) Die kontinuierliche Verbesserung der IKT-Resilienz ist ein sich wiederholender Prozess, der sicherstellt, dass eine Organisation flexibel und widerstandsfähig bleibt, um Herausforderungen im Zusammenhang mit Informations- und Kommunikationstechnologien effektiv zu bewältigen. Es handelt sich um einen dynamischen Ansatz zur Sicherung der Geschäftskontinuität und zur Minimierung von Schäden durch IKT-Störungen.

## 2.2 Abgrenzung

- (1) Dieser Leitfaden fokussiert auf jene Business-Prozesse, welche einen direkten Einfluss auf die sichere Regelung und Steuerung der Stromnetze sowie Stromproduktionen und Stromspeicherungen haben. Durch die Verpflichtung des IKT-Minimalstandards zur Steigerung der IKT-Resilienz in der StromVV müssen mit primärem Fokus die gesetzlichen Vorgaben umgesetzt und eingehalten werden. Folgende Definitionen und Abgrenzungspunkte definieren den Umfang dieses Leitfadens:
- IKT-Security für kritische Infrastrukturen schliesst alle IKT-Assets ein, welche für einen sicheren und integren Netzbetrieb im Bereich Strom, für eine sichere Stromproduktionen und sichere Stromspeicherungen notwendig sind oder mit solchen Systemen direkt interagieren.
  - Die Ausprägung für die Unternehmen und Organisationseinheiten sind in der StromVV mit den entsprechenden Schutzniveaus festgelegt.
  - Die Sicherheit der Office-IT und Wirtschaftsinformatik steht nicht im Fokus des Dokuments. Jedoch werden Anforderungen an die Schnittstellen und den Informationsaustausch zu den Bereichen, welche die kritischen IKT-Assets enthalten, gestellt.
  - Die elektrische und betriebliche Sicherheit der Betriebsmittel des Stromnetzes ist nicht Bestandteil dieses Leitfadens.
  - Massnahmen zur Arbeitssicherheit sind nicht Bestandteil dieses Leitfadens. Diesbezüglich gelten die Bestimmungen der Starkstromverordnung.
  - Es soll eine branchenweite Vorgehensweise zur Steigerung der IKT-Resilienz implementiert werden, welche als Basis für ein erhöhtes Sicherheitsniveau dient.
  - Kernkraftwerke unterliegen nicht der StromVV Vorgaben, für sie gelten die ENSI und IAEA Vorgaben.

## 2.3 Hintergrund

- (1) In den letzten 15 Jahren hat es in der Energietechnik eine starke Verlagerung zu IT- bzw. IKT-Systemen gegeben. Dieser technologische Wandel ermöglicht das zentrale Steuern und Regeln von Echtzeitinformationen. Dadurch wird man in der Netzbetriebsführung viel agiler und kann auf zeitnahe, kritische Ereignisse viel schneller und automatisiert reagieren. Doch dieser Wandel hin zur Informationstechnologie bringt auch neue Risiken mit sich, welche die Energieunternehmen anerkennen, bewerten und behandeln müssen, um den gesetzlichen Auftrag gemäss Stromversorgungsgesetz, Stromversorgungsverordnung oder dem Energiegesetz erfüllen zu können.
- (2) Der Energiesektor wird immer stärker durch IT/OT-Komponenten unterstützt. Dies geschieht innerhalb der Organisation von administrativen Tätigkeiten über Berechnungsmodelle für den Stromfluss, bis hin zu den Schaltelementen in einem Unterwerk. Obwohl sich die Vernetzung noch nicht komplett durchgesetzt hat, wird diese über kurz oder lang unumgänglich sein. Bereits heute werden in der Regel Schaltungen in den Unterwerken nicht mehr lokal durchgeführt, sondern zentral von einem Kontrollzentrum aus. Nebst den Schaltungen kann die Zentrale ein Unterwerk komplett per Fernzugriff überwachen und in Echtzeit Messwerte der Stromflüsse ablesen.
- (3) Ebenso führt die lokale Stromproduktion von Photovoltaik- und Windanlagen zu einer immer stärkeren Vernetzung. Da hierdurch jeder Betreiber einer entsprechenden Anlage an das Netz eines Stromproduzenten angeschlossen werden kann, entsteht ein landesweites Energie-Netzwerk von erheblicher Komplexität. Ebenfalls sind diese Produzenten durch Business-Prozesse und Schnittstellen miteinander verbunden.
- (4) Die rasche Integration der schnelllebigen Computer-Technologien führt zu einer Kollision zweier Welten. Da viele der Komponenten mit dem Fokus auf eine möglichst hohe Langlebigkeit gebaut wurden, sind





einige der SCADA Elemente zu einer Zeit gebaut worden als der Fokus der Hersteller noch nicht auf Cybersicherheit lag. Ebenso wurden die meisten Fachkräfte nicht mit einem entsprechenden Fokus auf die heutigen Risiken ausgebildet. Dies führt zu der Herausforderung, immer neuere Sicherheitskonzepte und Technologien in ein mehr oder weniger statisches Umfeld zu integrieren.

## 2.4 Bedrohungen und Risiken

- (1) Das Bundesamt für Bevölkerungsschutz BABS hat eine Risiko- und Verwundbarkeitsanalyse des Teilssektors Stromversorgung durchgeführt und folgende Erkenntnisse zusammengetragen:
- Entlang der gesamten Versorgungskette ist die Produktion von Strom in den Kraftwerken heute weniger stark verwundbar hinsichtlich IKT-Gefährdungen als der Betrieb der Verteil- und Übertragungsnetze.
  - Kraft- und Unterwerke können theoretisch auch immer noch vor Ort bedient werden. Bei einem grossflächigen Ausfall wären die Energieversorgungsunternehmen aber kaum noch in der Lage, alle kritischen Anlagen schnell genug mit ausreichend Personal besetzen zu können.
  - Betrifft die Gefährdung die IKT-Dienstleister der Energieversorgungsunternehmen, so wäre die Kommunikation zwischen den Anlagen und den Leitstellen unter Umständen nur noch über Not-Kommunikationssysteme aufrechtzuerhalten.
  - Der Betrieb der Höchst-, Hoch- und Mittelspannungsnetze erfolgt heute zentral und wird weitgehend durch digitale Systeme überwacht und gesteuert. Der Betrieb der Netze ist deswegen stärker verwundbar gegenüber IKT-Gefährdungen als die eigentliche Stromproduktion. In diesem Bereich sind die SCADA-Systeme von besonderer Bedeutung.
  - Die Gefährdung durch Mitarbeitende, welche absichtliche oder unabsichtliche Fehlmanipulationen an den SCADA-Systemen vornehmen, ist somit ebenfalls signifikant und nimmt durch den Zentralisierungsprozess bei den Leitstellen weiter zu.
  - Mit dem Einbau von „Smart Metern“ und „Smart Grid“-Geräten wird das Schweizer Leitungsnetz zu einem Verbund aus einer Vielzahl kleiner Computer. Dies bietet Vorteile in der Effizienz für den Betrieb der Leitungsnetze, schafft aber neue IKT-Verwundbarkeiten.
  - Insgesamt wird die IKT-Verwundbarkeit der Stromversorgung in Zukunft weiter zunehmen.



3. Umfeld Stromversorgung zur Steigerung der IKT-Resilienz

3.1 VSE-Regelwerk für die Strombranche zur Steigerung der IKT-Resilienz

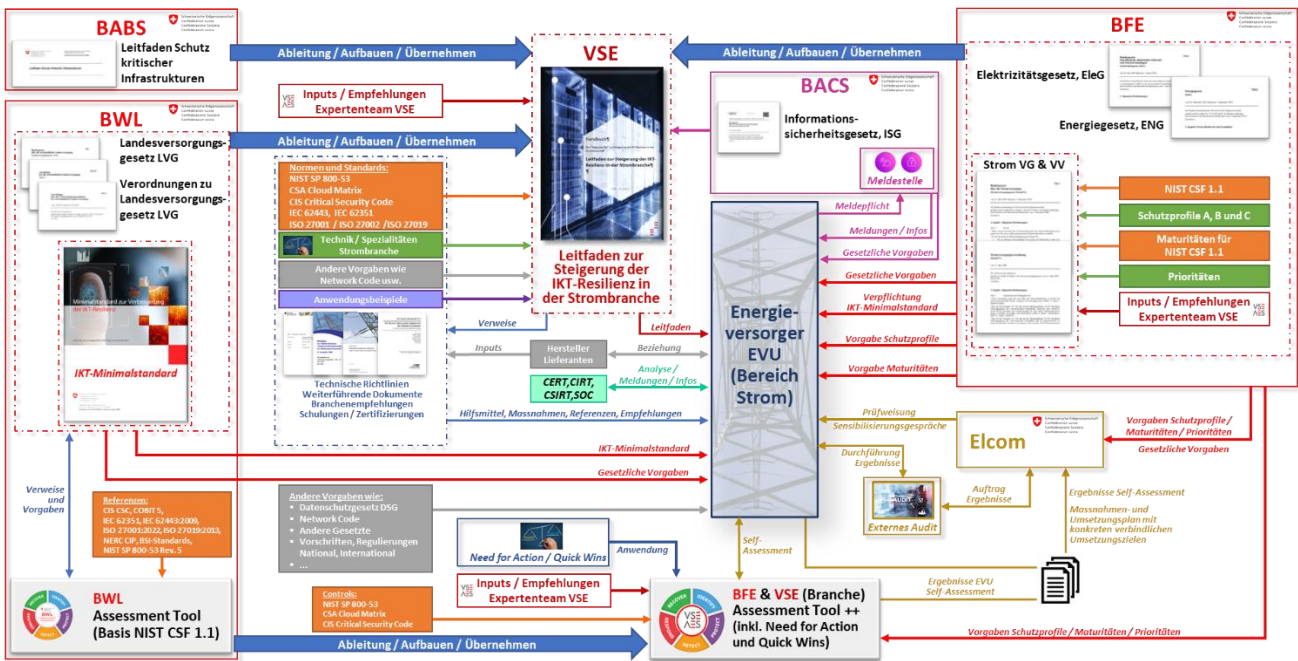


Abbildung 3: VSE-Regelwerk für die Strombranche zur Steigerung der IKT-Resilienz (Quelle VSE)

(1) Im VSE-Regelwerk für die Strombranche zur Steigerung der IKT-Resilienz sind sämtliche wichtige Elemente abgebildet, welche zur vollumfänglichen Umsetzung notwendig sind. Die einzelnen Elemente und deren Zusammenspiel werden folgend beschrieben und beleuchtet.

3.2 Player / Stakeholder

3.2.1 Stakeholder auf Bundesebene

(1) Folgende Stellen auf Bundesebene sind in diesem Leitfaden zur Steigerung der IKT-Resilienz involviert:

Bundesstelle	Kurzbeschreibung
Bundesamt für Bevölkerungsschutz (BABS)	Das Bundesamt für Bevölkerungsschutz (BABS) ist die schweizerische Bundesbehörde, die für die Planung und Koordination von Massnahmen im Bereich der zivilen Sicherheit und des Bevölkerungsschutzes zuständig ist.
Bundesamt für wirtschaftliche Landesversorgung (BWL)	Das Bundesamt für wirtschaftliche Landesversorgung (BWL) ist die schweizerische Bundesbehörde, die für die Sicherstellung der wirtschaftlichen Versorgung des Landes in Notfallsituationen verantwortlich ist. Das BWL hat durch die Erstellung des IKT-Minimalstandards eine entscheidende Rolle bei der Festlegung der Vorgehensweise und des Rahmens zur Steigerung der IKT-Resilienz bei versorgungskritischen Anlagen übernommen.
Bundesamt für Energie BFE	Das Bundesamt für Energie (BFE) ist die Bundesbehörde, die für die Energiepolitik und -regulierung in der Schweiz zuständig ist und die nachhaltige Nutzung von Energie fördert. Das BFE legt im Rahmen des Strom VV die gesetzlich verpflichteten Minimalanforderungen zur Steigerung der IKT-Resilienz auf Bundesebene fest.
Eidgenössischen Elektrizitätskommission (ElCom)	Die Eidgenössische Elektrizitätskommission (ElCom) ist die schweizerische Regulierungsbehörde für den Strommarkt, welche die Stromversorgung, Tarife und den Netzzugang in der Schweiz überwacht. Im Rahmen der gesetzlichen Bestimmungen zur Stärkung der Cyber-Resilienz überprüft und kontrolliert die ElCom die Einhaltung der rechtlichen Vorgaben.
Bundesamt für Cybersicherheit (BACS)	Das Bundesamt für Cybersicherheit (BACS) ist die zuständige schweizerische Behörde für nationale Cybersicherheit, die die Koordinierung von Massnahmen zur Abwehr von Cyberbedrohungen und zur Verbesserung der IKT-



Bundesstelle	Kurzbeschreibung
	Sicherheit verantwortet. Mit dem neuen Informationssicherheitsgesetz (ISG) in der Schweiz gibt es eine gesetzliche Vorschrift zur Meldung von Vorfällen im Bereich Cybersecurity an das BACS. Die Meldepflicht wird mit der 1. Revision des ISG eingeführt.

**Tabelle 1:** Stakeholder auf Bundesebene (Quelle VSE)

### 3.2.2 Der Verband Schweizerischer Elektrizitätsunternehmen (VSE)



(1) Der VSE ist der national und international anerkannte Branchendachverband der Schweizer Stromwirtschaft. Er koordiniert und bündelt die gemeinsamen Interessen und Kompetenzen seiner Mitglieder und vertritt diese gegenüber Politik, Wirtschaft und Gesellschaft. Dadurch sorgt er für verlässliche Rahmenbedingungen für eine sichere, markt- und wettbewerbsfähige und nachhaltige Stromversorgung in der Schweiz. Die über 400 Mitglieder sind über die gesamte Wertschöpfungskette verteilt (Produzenten, Verteilnetzbetreiber, Querverbundunternehmen) und produzieren über 90% des Schweizer Stroms.

#### Expertenteam VSE



#### Expertenteam VSE

(1) Zur Behandlung der verschiedenen Themen im Bereich Strom sind beim VSE diverse Arbeitsgruppen aktiv. In diesen Arbeitsgruppen sind Vertreter aus den verschiedenen Bereichen der Strombranche tätig. Für den Bereich Cyber-Security wurde eine spezielle Arbeitsgruppe gebildet, welche sich um alle Themen im Bereich Cyber-Security in der Strombranche widmet. Ein Expertenteam aus dieser Arbeitsgruppe befasst sich mit dem Thema "Steigerung der IKT-Resilienz in der Strombranche".

### 3.2.3 Energieversorger EVU (Bereich Strom)



(1) Ein Energieversorgungsunternehmen im Bereich Strom, auch als Stromversorger oder Elektrizitätsunternehmen bezeichnet, sind Unternehmen und Organisationseinheiten, die die Erzeugung, Speicherung, Übertragung und Verteilung von elektrischer Energie an private, gewerbliche und industrielle Kunden sicherstellt.

(2) Die Volkswirtschaft funktioniert nicht ohne Strom, so dass Stromversorgungsunternehmen als systemrelevant eingestuft sind. Stromnetze, Stromkraftwerke und Stromspeicher, deren Abschaltung zu einer erheblichen Gefährdung oder Störung der Energiesicherheit und -zuverlässigkeit des Stromversorgungssystems führen, sind als systemrelevant einzustufen, deren Eigentümer werden vom Bund zum Weiterbetrieb verpflichtet.

### 3.2.4 CERT, CIRT, CSIRT und SOC

(1) CIRT, CERT, CSIRT und SOC sind Begriffe, die in der Welt der Cybersicherheit verwendet werden, um verschiedene Arten von Teams und Einrichtungen zu beschreiben, die auf die Identifizierung und Bewältigung von Sicherheitsvorfällen abzielen. Zusammenfassend kann gesagt werden, dass CIRT, CERT und CSIRT in erster Linie auf die Reaktion auf Sicherheitsvorfälle ausgerichtet sind, während ein SOC auf die proaktive Überwachung und den Schutz der IKT-Infrastruktur abzielt. Die Wahl, welcher Ansatz in einer Organisation am besten geeignet ist, hängt von den spezifischen Anforderungen, Zielen und Risiken der Organisation ab. Oft arbeiten diese Teams jedoch zusammen, um eine umfassende Cybersicherheitsstrategie zu gewährleisten.

#### CERT:

- (2) Ein **Computer Emergency Response Team (CERT)** ist eine spezialisierte Organisation oder Gruppe von Experten, die sich auf die Erkennung, Bewertung und Reaktion auf Cybersecurity-Vorfälle spezialisiert haben. CERTs sind darauf ausgerichtet, die Sicherheit von Computersystemen und Netzwerken zu stärken, Bedrohungen zu erkennen und effektive Massnahmen zur Bewältigung von Sicherheitsvorfällen zu ergreifen.
- (3) Es gibt sowohl private als auch staatliche CERTs, und sie können auf nationaler, regionaler oder Unternehmensebene existieren. In vielen Ländern gibt es auch nationale CERT-Organisationen, die speziell für





die nationale Cybersecurity verantwortlich sind und eng mit anderen CERTs zusammenarbeiten. Das Ziel eines CERT ist es, die Cybersicherheit zu stärken, die Resilienz gegenüber Cyberangriffen zu erhöhen und die Auswirkungen von Sicherheitsvorfällen zu minimieren. **Es ist wichtig zu beachten, dass CERT eine eingetragene Marke der Carnegie Mellon University (CMU) ist. Organisationen dürfen das CERT-Zeichen verwenden, nachdem sie eine Genehmigung erhalten haben. Einige Organisationen, die wahrscheinlich nicht wissen, dass es sich um ein Warenzeichen handelt, verwenden es dennoch, um ihre Incident Response Teams zu definieren.**

#### **CIRT und CSIRT:**

- (4) CIRT und CSIRT sind beide Arten von Teams, die sich mit der Reaktion auf Cyber-Vorfälle befassen, aber sie haben unterschiedliche Schwerpunkte. Insgesamt kann man sagen, dass ein CIRT eher auf die internen Sicherheitsbedürfnisse eines Unternehmens oder einer Organisationseinheit ausgerichtet ist, während ein CSIRT eine breitere Perspektive hat und möglicherweise über spezialisiertere Ressourcen verfügt, um auf unterschiedliche Arten von Cyber-Bedrohungen zu reagieren.

#### **CIRT:**

- (5) Ein **Computer Incident Response Team (CIRT)** ist typischerweise intern und konzentriert sich auf die Reaktion auf Cyber-Vorfälle innerhalb eines Unternehmens oder einer Organisationseinheit. Es besteht aus Mitarbeitern des Unternehmens oder der Organisationseinheiten, die für die Sicherheit verantwortlich sind, wie z. B. IT/OT-Sicherheitsexperten, Netzwerkadministratoren und Forensiker. Die Hauptaufgabe eines CIRT besteht darin, auf Sicherheitsvorfälle zu reagieren, die die internen Systeme, Netzwerke oder Daten der Organisation betreffen. Ein CIRT kann auch präventive Massnahmen entwickeln, um zukünftige Vorfälle zu verhindern, und Richtlinien und Verfahren zur Verbesserung der allgemeinen Sicherheit der Organisation umsetzen.

#### **CSIRT:**

- (6) Ein **Computer Security Incident Response Team (CSIRT)** kann entweder intern oder extern sein und konzentriert sich auf die Reaktion auf Cyber-Vorfälle, die ein breiteres Spektrum von Unternehmen und Organisationseinheiten betreffen können, einschliesslich Bundesbehörden, Unternehmen und anderen Einrichtungen. Es kann von einer Organisation oder einer Branchengruppe betrieben werden und kann oft auf eine bestimmte Region, Branche oder Art von Cyber-Bedrohungen spezialisiert sein. Ein CSIRT kann auch über spezialisierte Ressourcen und Expertise verfügen, um auf komplexe oder weitreichende Cyber-Angriffe zu reagieren, die möglicherweise koordinierte Anstrengungen erfordern. Die Aufgaben eines CSIRT umfassen oft auch die Überwachung von Bedrohungen, die Analyse von Sicherheitsvorfällen und die Bereitstellung von Informationen und Empfehlungen zur Verbesserung der allgemeinen Cybersicherheit.

#### **SOC:**

- (7) Ein **Security Operation Center (SOC)** ist eine spezialisierte Einrichtung oder Abteilung innerhalb oder ausserhalb des Unternehmens oder Organisationseinheit, deren Hauptaufgabe darin besteht, die Informationssicherheit zu überwachen, zu schützen und auf Sicherheitsvorfälle zu reagieren.
- (8) Ein SOC kann intern in einer Organisation oder als Dienstleistung eines externen Anbieters (MSSP - Managed Security Service Provider) eingerichtet sein. Die Einrichtung eines SOC ist entscheidend, um die Informationssicherheit zu gewährleisten, Bedrohungen in Echtzeit zu erkennen und auf diese angemessen zu reagieren. Es ist ein wesentlicher Bestandteil moderner Sicherheitsmassnahmen für Unternehmen und Organisationseinheiten, um sich vor Cyberangriffen zu schützen und auf diese vorbereitet zu sein.

### **3.2.5 Hersteller und Lieferanten**

- (1) Die Rolle von Herstellern und Lieferanten bei der Steigerung der IKT-Resilienz (Informations- und Kommunikationstechnologie) ist von entscheidender Bedeutung, insbesondere in einer Zeit, in der Technologie eine zentrale Rolle in Wirtschaft und Gesellschaft spielt:

#### **Hersteller:**

- **Produktinnovation:** Hersteller von IKT-Hardware und -Software sind für die Entwicklung und Produktion von robusten und widerstandsfähigen Technologielösungen verantwortlich. Dies umfasst die Schaffung von Produkten, die gegen Störungen und Ausfälle resistent sind, wie zum Beispiel Hardware mit redundanter Stromversorgung oder Software mit integrierten Sicherheitsfunktionen (Security by Design).



- **Qualitätskontrolle:** Hersteller müssen strenge Qualitätskontrollen und Tests durchführen, um sicherzustellen, dass ihre Produkte den Anforderungen hinsichtlich Leistung und Sicherheit entsprechen. Dies ist entscheidend, um die Zuverlässigkeit von IKT-Systemen zu gewährleisten.
- **Bereitstellung von Wartungs- und Reparaturservices:** Hersteller können Wartungs- und Reparaturservices für ihre Produkte anbieten, um im Falle von Störungen oder Ausfällen eine schnelle Wiederherstellung zu gewährleisten.

#### Lieferanten:

- **Lieferkette und Beschaffungssicherheit:** Lieferanten von IKT-Rohstoffen und Komponenten müssen sicherstellen, dass die Lieferkette robust und sicher ist, um die kontinuierliche Verfügbarkeit von kritischen Materialien sicherzustellen. Dies beinhaltet die Identifizierung von Lieferantenalternativen und die Diversifizierung der Beschaffungsquellen.
  - **Notfallvorsorge:** Lieferanten sollten Notfallpläne entwickeln, um auf Naturkatastrophen, geopolitische Konflikte oder andere Krisen reagieren zu können. Dies kann die Einrichtung von Notfalllagern, die Vorratshaltung kritischer Komponenten und die Implementierung von Krisenreaktionsprotokollen umfassen.
  - **Kooperation und Kommunikation:** Lieferanten sollten eng mit ihren Kunden (den Herstellern) zusammenarbeiten und eine klare Kommunikation aufrechterhalten, um potentielle Risiken und Herausforderungen in der Lieferkette frühzeitig zu erkennen und zu bewältigen.
- (2) Die Zusammenarbeit zwischen Herstellern und Lieferanten ist entscheidend, um die IKT-Resilienz zu stärken. Durch die Entwicklung widerstandsfähiger Produkte, die Sicherung der Lieferketten und die Implementierung von Notfallplänen können sie dazu beitragen, Ausfälle und Störungen in der Informations- und Kommunikationstechnologie zu minimieren und die Kontinuität von Geschäftsprozessen sowie die Sicherheit der IKT-Systeme zu gewährleisten. Dies ist insbesondere in sensiblen Bereichen wie Gesundheitswesen, Energieversorgung und Finanzwesen von grosser Bedeutung.
- (3) Hersteller und Lieferanten spielen eine wichtige Rolle bei der Einhaltung von Normen, Vorschriften und Spezifikationen. Diese Regeln und Standards sind entscheidend, um die Qualität, Sicherheit und Leistung von Produkten und Dienstleistungen zu gewährleisten.

#### Rolle der Hersteller:

- **Einhaltung von Qualitätsstandards:** Hersteller müssen sicherstellen, dass ihre Produkte den geltenden Qualitätsstandards und -normen entsprechen. Dies kann branchenspezifische Qualitätszertifizierungen, technische Spezifikationen und Sicherheitsnormen umfassen.
- **Produktdesign und -entwicklung:** Hersteller sind dafür verantwortlich, Produkte so zu entwickeln und zu gestalten, dass sie den einschlägigen Normen und Vorschriften entsprechen. Dies erfordert oft die Integration von spezifischen Anforderungen in den Designprozess.
- **Qualitätskontrolle und Tests:** Hersteller müssen strenge Qualitätskontrollen und Tests durchführen, um sicherzustellen, dass ihre Produkte die festgelegten Spezifikationen erfüllen. Dies kann sowohl interne als auch externe Prüfungen und Zertifizierungen umfassen.
- **Dokumentation und Kennzeichnung:** Hersteller müssen alle erforderlichen Informationen, wie technische Dokumentation, Sicherheitsdatenblätter und Konformitätserklärungen, bereitstellen und sicherstellen, dass ihre Produkte ordnungsgemäss gekennzeichnet sind.

#### Rolle der Lieferanten:

- **Beschaffung von konformen Materialien:** Lieferanten müssen sicherstellen, dass die von ihnen gelieferten Rohstoffe, Komponenten und Dienstleistungen den geltenden Normen und Vorschriften entsprechen. Dies kann die Zusammenarbeit mit qualifizierten Herstellern und Zulieferern umfassen.
- **Detaillierte Spezifikationen:** Lieferanten müssen klare und detaillierte Spezifikationen für die von ihnen gelieferten Materialien und Dienstleistungen bereitstellen, um sicherzustellen, dass sie den Anforderungen entsprechen.
- **Rückverfolgbarkeit und Qualitätssicherung:** Lieferanten sollten Mechanismen zur Rückverfolgbarkeit und Qualitätskontrolle implementieren, um sicherzustellen, dass die gelieferten Produkte den erforderlichen Standards entsprechen.



- **Zertifizierungen und Konformität:** Lieferanten können Zertifizierungen und Konformitätserklärungen bereitstellen, um ihre Produkte und Dienstleistungen als konform mit den geltenden Normen und Vorschriften zu bestätigen.
- (4) Zusammenarbeit zwischen Herstellern und Lieferanten ist entscheidend, um sicherzustellen, dass Produkte und Dienstleistungen den relevanten Normen und Vorschriften entsprechen. Diese Zusammenarbeit hilft, die Qualität und Sicherheit von Produkten zu gewährleisten, das Risiko von Rechtsverstössen zu minimieren und das Vertrauen der Kunden und Aufsichtsbehörden zu stärken. Darüber hinaus können Hersteller und Lieferanten durch die Einhaltung von Normen und Vorschriften auch Wettbewerbsvorteile erzielen und den Zugang zu Märkten erleichtern, die strenge Anforderungen an Produktqualität und -sicherheit stellen.



**Ein aktives Management der Supply-Chain (Dienstleister und Hersteller) ist durch die Unternehmen und Organisationseinheiten zwingend erforderlich. Gerade im Bereich Risiko- und Bedrohungsmanagement muss die Lieferkette aktiv miteinbezogen werden.**



**Es ist unerlässlich Vorgaben im Bereich des Lieferanten Management zu machen und diese in einer Arbeitsanleitung festzuhalten. Die Vorgaben sollen in den Bereichen organisatorischen Kontrollanforderungen, Management von Informationssicherheitsvorfällen, Anforderungen an die Personenkontrolle sowie physische und technologische Kontrollanforderungen enthalten.**



**Hinweise auf weiterführende und ergänzende Dokumente:**

**Vorlage: HoP-01-01-03-22 Arbeitsanleitung Bereich ISMS: Lieferanten Management**

**NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations**

### 3.3 Gesetzliche Grundlagen: Verpflichtende Gesetze und Verordnungen

- (1) Folgende Zusammenfassung ergibt einen Überblick über die geltenden gesetzlichen Grundlagen in Form von Gesetzes- und Verordnungsartikeln, welche in Zusammenhang mit der Steigerung der IKT-Resilienz bei den Energieversorgern im Bereich Strom angewendet werden müssen:

#### 3.3.1 Übersicht der gesetzlichen Gesetze, Verordnungen und Bestimmungen in Zusammenhang mit der Versorgungs- und Informationssicherheit



**In folgenden nationalen Gesetzen und Verordnungen sind Vorgaben in Zusammenhang mit der Versorgung- und Informationssicherheit, welche zwingend erfüllt werden müssen:**

- Bundesverfassung der Schweizerischen Eidgenossenschaft (BV; SR 101): Art. 102
- Obligationenrecht (SR 220): Art. 728a, 728b, 754, 961, 961c
- Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz LVG; SR 531): Art. 4, 31, 32
- Verordnung über die wirtschaftliche Landesversorgung (VWL; SR 531.11): Art. 7, 11
- Verordnung über die Organisation zur Sicherstellung der wirtschaftlichen Landesversorgung im Bereich der Elektrizitäts-wirtschaft (VOEW; SR 531.35): Art. 1, 1a, 1b, 2
- Energiegesetz (EnG; SR 730.0): Art. 7
- Bundesgesetz über die Stromversorgung (Stromversorgungsgesetz StromVG; SR 734.7): Art. 6
- Stromversorgungsverordnung (StromVV; SR 734.71): 5, 5a
- Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz ISG; SR 128): Art. 5, 74, 76, 77, 78
- Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR235.1): Art. ....
- Internes Kontrollsystem OR 728a, 728b



**In folgenden internationalen Gesetzen und Verordnungen sind Vorgaben in Zusammenhang mit der Versorgung- und Informationssicherheit, welche von den betroffenen Unternehmen und Organisationseinheiten zwingend erfüllt werden müssen:**

- Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194 vom 19.7.2016, S. 1
- Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 vom 27.12.2022, S. 80





Die Auflistung oben ist nicht abschliessend. Es gibt noch weitere Artikel in Gesetzen und Verordnungen, welche nicht explizit aufgeführt sind, da sie nur indirekt mit der Informationssicherheit in Verbindung gebracht werden können.



Gesetzliche Bestimmungen und Verordnungen vom Bund und den Bundesstellen sind verpflichtend und müssen zwingend eingehalten werden.



Internationale gesetzliche Vorgaben und Richtlinien müssen teilweise von Unternehmen und Organisationseinheiten umgesetzt werden. Es ist durch die Unternehmen und Organisationseinheiten zu prüfen welche internationalen gesetzlichen Vorgaben einzuhalten sind.



Die Gesetzesartikel sind im Anhang C aufgeführt.

### 3.3.2 BABS Nationale Strategie zum Schutz kritischer Infrastrukturen



(1) Die Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) ist ein wichtiges strategisches Dokument in der Schweiz, das sich auf den Schutz und die Widerstandsfähigkeit entscheidender Einrichtungen und Dienstleistungen konzentriert. Die SKI identifiziert kritische Sektoren, bewertet Risiken, fördert präventive Massnahmen, stärkt die Sicherheit und die Fähigkeit zur Reaktion auf Bedrohungen und betont die Notwendigkeit der Zusammenarbeit zwischen Regierung, Betreibern

und anderen Stakeholdern. Sie zielt darauf ab, die nationale Sicherheit und das Wohlergehen der Bevölkerung zu gewährleisten und die Widerstandsfähigkeit gegenüber Krisen zu erhöhen. Die wichtigsten Punkte der SKI umfassen:

- **Identifizierung und Kategorisierung:** Die SKI beginnt mit der Identifizierung und Kategorisierung von kritischen Infrastrukturen in der Schweiz. Dazu gehören Sektoren wie Energie, Wasser, Telekommunikation, Verkehr, Gesundheitswesen und viele andere, die für das nationale Wohl und die Wirtschaft von entscheidender Bedeutung sind.
  - **Risikobewertung und -management:** Die Strategie legt Wert auf die regelmässige Bewertung der Risiken und Bedrohungen, denen diese kritischen Infrastrukturen ausgesetzt sind. Dies umfasst die Analyse von Naturkatastrophen, technischen Störungen und absichtlichen Angriffen. Auf der Grundlage dieser Bewertungen werden Massnahmen zur Risikominderung entwickelt.
  - **Koordinierte Zusammenarbeit:** Die SKI fördert die enge Zusammenarbeit zwischen verschiedenen Akteuren, darunter Bundes-, Kantons- und Gemeindebehörden, Betreiber kritischer Infrastrukturen sowie private Unternehmen und Organisationseinheiten. Eine koordinierte und partnerschaftliche Herangehensweise wird betont, um eine effektive Reaktion auf Bedrohungen und Notfälle sicherzustellen.
  - **Sicherheits- und Präventionsmassnahmen:** Die Strategie legt Massnahmen zur Erhöhung der Sicherheit und zur Prävention von Störungen und Angriffen fest. Dies beinhaltet die Verbesserung der physischen Sicherheit, die Stärkung der Informationssicherheit und die Schulung des Personals.
  - **Notfallmanagement und Notfallplanung:** Die SKI betont die Notwendigkeit einer umfassenden Notfallmanagementstruktur und einer klaren Notfallplanung, um auf Störungen und Katastrophen angemessen reagieren zu können.
  - **Kommunikation und Sensibilisierung:** Die Strategie fördert die Kommunikation und Sensibilisierung gegenüber der Öffentlichkeit und den Beteiligten, um das Verständnis für die Bedeutung des Schutzes kritischer Infrastrukturen zu stärken.
- (2) Die SKI ist ein wichtiger Rahmen, um die Sicherheit und Resilienz der Schweiz in Bezug auf kritische Infrastrukturen zu gewährleisten. Sie legt die Grundlagen für die Zusammenarbeit zwischen den Behörden und der Privatwirtschaft und betont die Bedeutung von Prävention, Schutz und Notfallmanagement.





### 3.3.3 BABS Leitfaden Schutz kritischer Infrastrukturen



- (1) Der Leitfaden Schutz kritischer Infrastrukturen zeigt auf, wie die Widerstandsfähigkeit (Resilienz) von kritischen Infrastrukturen überprüft und gestärkt werden kann. Er trägt dazu bei, schwerwiegende Ausfälle von kritischen Infrastrukturen zu verhindern respektive im Ereignisfall die Ausfallzeit zu reduzieren. Methodisch orientiert sich der Leitfaden an gängigen und etablierten Konzepten des Risiko-, Krisen- und Kontinuitätsmanagements und kombiniert verschiedene Elemente dieser Ansätze im Sinne eines integralen Schutzes. Der Leitfaden baut auf entsprechenden Planungen und Arbeiten auf, über die viele Unternehmen und Organisationseinheiten bereits verfügen. Während diese in der Regel auf Risiken für die Unternehmen und Organisationseinheiten fokussieren, steht beim Leitfaden SKI die Frage im Vordergrund, inwiefern Ausfälle von kritischen Infrastrukturen die Bevölkerung und ihre (wirtschaftlichen) Lebensgrundlagen beeinträchtigen. Die Umsetzung des SKI-Leitfadens erfordert eine enge Zusammenarbeit zwischen den Betreibern der kritischen Infrastrukturen und den jeweiligen Fach-, Aufsichts- und Regulationsbehörden in den verschiedenen Bereichen der kritischen Infrastrukturen (Energie, Verkehr, Gesundheitswesen usw.).
- (2) Der Leitfaden Schutz kritischer Infrastrukturen bietet einen Rahmen und praktische Empfehlungen für den Schutz wichtiger Einrichtungen und Dienstleistungen in der Schweiz. Hier ist eine Zusammenfassung der Hauptpunkte:
- **Definition kritischer Infrastrukturen:** Der Leitfaden identifiziert und definiert kritische Sektoren und Einrichtungen, die für das Funktionieren der Schweiz von wesentlicher Bedeutung sind, wie Energie, Wasserversorgung, Telekommunikation, Verkehr und Gesundheitswesen.
  - **Risikobewertung und Prävention:** Er betont die Bedeutung der Risikobewertung, um mögliche Bedrohungen und Schwachstellen in kritischen Infrastrukturen zu identifizieren. Präventive Massnahmen werden empfohlen, um diese Risiken zu minimieren.
  - **Schutz und Sicherheit:** Der Leitfaden legt Massnahmen zur Erhöhung der Sicherheit in kritischen Einrichtungen nahe, einschliesslich physischer Sicherheit, Zugangsbeschränkungen und Überwachungssysteme.
  - **Notfallmanagement und Wiederherstellung:** Es werden Leitlinien zur Entwicklung von Notfallplänen und zur Wiederherstellung nach einem Vorfall bereitgestellt, um die Widerstandsfähigkeit kritischer Infrastrukturen zu stärken.
  - **Zusammenarbeit und Informationsaustausch:** Der Leitfaden fördert die Kooperation zwischen staatlichen Stellen, Betreibern kritischer Infrastrukturen, Kantonsregierungen und anderen Beteiligten. Der Informationsaustausch und die Zusammenarbeit sind entscheidend für eine wirksame Reaktion auf Bedrohungen und Notfälle.
  - **Sensibilisierung und Schulung:** Er betont die Sensibilisierung der Öffentlichkeit und der Betroffenen, indem Schulungen und Informationen zur Verfügung gestellt werden, um die Vorbereitung und den Schutz zu verbessern.
- (3) Der Leitfaden Schutz kritischer Infrastrukturen dient als praktisches Werkzeug, um den Schutz und die Widerstandsfähigkeit kritischer Einrichtungen in der Schweiz zu fördern und sicherzustellen, dass sie im Falle von Bedrohungen oder Krisen weiterhin effektiv funktionieren.

### 3.3.4 BWL IKT-Minimalstandard zur Verbesserung der IKT-Resilienz



- (1) IKT-Sicherheit bedingt ein risikobasiertes Verhalten und den Einsatz sicherer Systeme im Verantwortungsbereich der jeweiligen Betreiber. Bereits durch die Umsetzung von bewährten Massnahmen, wie sie im IKT-Minimalstandard zur Verbesserungen der IKT-Resilienz dargestellt werden, kann eine Vielzahl von IKT-Angriffen mit vertretbarem Aufwand abgewehrt werden. Der vorliegende Standard hat zum Ziel, Unternehmen und Organisationseinheiten ein vielseitig einsetzbares Hilfsmittel zur Hand zu geben, wodurch sie individuell die Resilienz ihrer IKT-Infrastruktur verbessern können. Durch den risikobasierten Ansatz ermöglicht der Standard die Umsetzung unterschiedlich strenger Schutzniveaus, angepasst an die Bedürfnisse der Organisation.
- (2) Der IKT-Minimalstandard wurde durch das Bundesamt für wirtschaftliche Landesversorgung in Zusammenarbeit mit externen Experten aus dem Bereich der IKT-Sicherheit ausgearbeitet.



Es existieren heute bereits mehrere international anerkannte Standards zur IKT-Sicherheit, die meist deutlich über das vorliegende Dokument hinausgehen. Der IKT-Minimalstandard versteht sich explizit nicht als Konkurrenz zu existierenden internationalen Standards, sondern ist mit diesen kompatibel, bei gleichzeitig reduziertem Umfang. Er soll einen einfacheren Einstieg in die Thematik ermöglichen und trotzdem ein hohes Schutzniveau gewährleisten. Ergänzend zum IKT-Minimalstandard wurden durch das Bundesamt für wirtschaftliche Landesversorgung weitere sektorspezifische Standards erarbeitet, die einen höheren (technischen) Detaillierungsgrad aufweisen. Betreibern von kritischen Infrastrukturen wird empfohlen, sich zusätzlich zum IKT-Minimalstandard auch an den detaillierten sektorspezifischen Vorgaben zu orientieren, sobald diese vorliegen. Gelten in einem Sektor bereits eigene Standards, oder werden internationale Standards wie ISO oder NIST verwendet, so können Unternehmen und Organisationseinheiten anhand der Checkliste in Kapitel «Teil 3 – Prüfungsauftrag» feststellen, ob sie den vorliegenden IKT-Minimalstandard bereits abgedeckt haben.

- (3) Weltweit existiert eine Vielzahl unterschiedlicher Standards und Informationsquellen zum Umgang mit IKT-Risiken. Einige davon sind von der Wirtschaft schon heute anerkannt und werden eingesetzt. Der BWL IKT-Minimalstandard basiert auf dem NIST Cybersecurity Framework Core. Wo sinnvoll, wird er durch weitere international anerkannte Industriestandards ergänzt.

#### Grundsätze des IKT-Minimalstandard zur Verbesserung der IKT-Resilienz sind:

- **Eigenverantwortung:** Betreiber von kritischen Infrastrukturen sind grundsätzlich selbstverantwortlich für das Aufrechterhalten ihrer kritischen IKT-Prozesse.
- **Business Continuity Management:** Alle Aspekte der IKT-Sicherheit sollen in ein übergeordnetes Business Continuity Management eingegliedert werden.
- **Risikomanagement:** Es ist Aufgabe der Betreiber von kritischen Infrastrukturen, mögliche IKT-Risiken wie die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit laufend zu bewerten. Das Unternehmen und die Organisationseinheiten müssen beurteilen, welche Risiken reduziert werden sollen und welche getragen werden können.



**Der IKT-Minimalstandard zur Verbesserung der IKT-Resilienz wird im Strom VV verpflichtet und muss deshalb von allen betroffenen Unternehmen und Organisationseinheiten der Strombranche angewendet und entsprechend dem zugeordneten Schutzprofil umgesetzt werden.**

- (4) Das Ziel des IKT-Minimalstandards ist die Steigerung der Cyber-Resilienz für Unternehmen und Organisationseinheiten in der gesamten Schweiz.

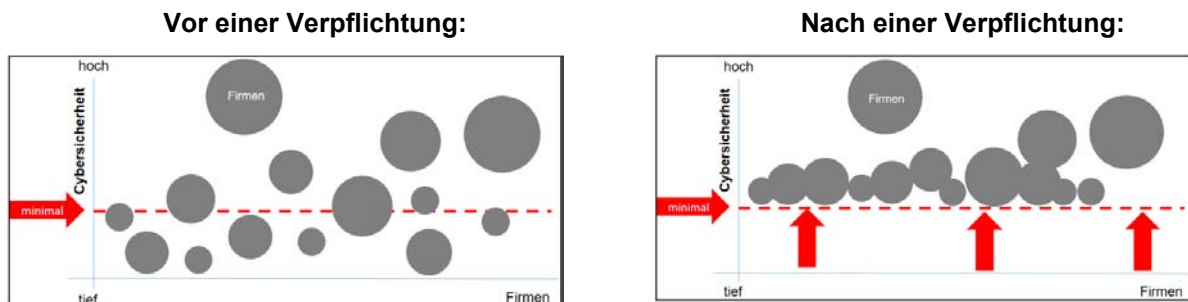


Abbildung 4: Steigerung der Cybersicherheit (Quelle BWL)

### 3.3.5 BWL IKT-Minimalstandard - Assessment Tool nach NIST CSF 1.1



- (1) Das BWL hat zur Standortbestimmung und Überprüfung der umgesetzten Massnahmen ein BWL IKT-Minimalstandard – Assessment Tool publiziert. Dieses Tool basiert auf dem NIST Cybersecurity Framework (CSF) Version 1.1. Dieses Framework ist ein wichtiges Instrument, der Unternehmen und Organisationseinheiten bei der Verbesserung ihrer Cybersicherheitspraktiken und -prozesse unterstützt. Das Framework besteht aus mehreren Hauptkomponenten, die Unternehmen und Organisationseinheiten dabei helfen, ihre Cybersicherheitsstrategien zu entwickeln und umzusetzen.

#### Grundsätzlicher Aufbau des NIST Cybersecurity Framework (CSF) Version 1.1:

##### 1. Framework Core (Kern des Frameworks):



Das Herzstück des Frameworks besteht aus fünf Hauptfunktionen oder Aktivitätsbereichen, die die grundlegenden Ziele der Cybersicherheit darstellen. Diese Funktionen sind:

- **Identify** (Identifizieren): Hierbei geht es darum, die vorhandenen Assets, Schwachstellen und Risiken zu identifizieren und eine umfassende Risikobewertung durchzuführen.
- **Protect** (Schützen): Dieser Bereich behandelt Massnahmen zur Absicherung von Systemen und Daten vor Cyberbedrohungen. Dazu gehören Zugriffskontrollen, Schulungen und Bewusstseinsbildung.
- **Detect** (Erkennen): Hier werden Prozesse und Technologien beschrieben, um Angriffe und Sicherheitsvorfälle frühzeitig zu erkennen.
- **Respond** (Reagieren): Dieser Bereich konzentriert sich auf die angemessene Reaktion auf Sicherheitsvorfälle, um Schäden zu minimieren und die Wiederherstellung zu unterstützen.
- **Recover** (Wiederherstellen): Hierbei geht es um die Wiederherstellung von Systemen und Diensten nach einem Sicherheitsvorfall, um den normalen Betrieb wieder aufzunehmen.

Jede Hauptfunktion oder Aktivitätsbereich ist dabei in Kategorien und Subkategorien aufgegliedert. Auf Stufe Subkategorie kann die Beurteilung (implantierte Tiers auf der Umsetzungsebenen) vorgenommen werden. Weiter werden auf Stufe Subkategorie die Referenzen zu Normen, Richtlinien und Vorgaben gemacht.

## 2. Framework Implementation Tiers (Umsetzungsebenen):

Das NIST Framework kennt vier Implementation Tiers (dt. «Stufen»). Diese beschreiben die Ausbaustufe (Schutzniveau), welche ein Unternehmen oder Organisationseinheit umgesetzt hat. Sie reichen von teilweise (Tier 1) bis dynamisch (Tier 4). Zur Festlegung des eigenen Schutzniveaus (Tier Level) soll eine Organisation ihre Risikomanagementpraktiken, die Bedrohungsumgebung sowie rechtliche und regulatorische Anforderungen, Geschäftsziele und organisatorischen Vorgaben genau kennen.

## 3. Framework Profiles (Framework-Profile):

Ein Framework-Profil ist eine anpassbare Zusammenstellung von Cybersicherheitsaktivitäten und -kategorien, die auf die spezifischen Bedürfnisse und Ziele eines Unternehmens und Organisationseinheiten zugeschnitten sind. Unternehmen und Organisationseinheiten können Profile erstellen, um ihre aktuellen und angestrebten Sicherheitsziele darzustellen.

## 4. Framework Implementation Tiers and Profiles Tool (Tool für Umsetzungsebenen und Profile):

Dies ist ein Hilfsmittel, mit dem Unternehmen und Organisationseinheiten ihre aktuellen Positionen in Bezug auf die Framework-Implementation-Tiers und die Framework-Profile bestimmen können. Es unterstützt bei der Planung und Umsetzung von Verbesserungen.

## 5. Framework Core Informative References (Zusätzliche Referenzen zum Framework-Kern):

Diese Referenzdokumente bieten weitere Informationen und Ressourcen, die Unternehmen und Organisationseinheiten bei der Umsetzung des Framework Core unterstützen können.

- (2) Das NIST CSF 1.1 bietet eine flexible Struktur, die es Unternehmen und Organisationseinheiten ermöglicht, ihre individuellen Cybersicherheitsbedürfnisse anzupassen und zu verbessern. Es dient als Leitfaden für die Entwicklung und Umsetzung einer robusten Cybersicherheitsstrategie und zur Verbesserung der Widerstandsfähigkeit gegenüber Cyberbedrohungen.

## Ausführung des BWL IKT-Minimal-Standard - Assessment Tool:

- (3) Die aktuelle Version des BWL IKT-Minimal-Standard - Assessment Tool basiert grundsätzlich auf dem NIST Cybersecurity Framework (CSF) Version 1.1. Im Tool werden folgen Elemente des NIST CSF 1.1 abgebildet:

Function Funktion Thème Tema	Category Kategorie Categorie Categoria	Subcategory Aktivität Tâches Mansione	Rating Bewertung Appréciation Stima	Comments Kommentare Commentaires Commenti	Empfehlungen BWL Priorisierung	Informative References Referenzen Références Riferimento
		<b>ID.AM-1:</b> 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 Ihrer IKT-Güterbestände (Assets) vorhanden ist. Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC (Assets). Definire una procedura che garantisca la costante presenza di un inventario completo dei vostri strumenti operativi TIC (assets).	na		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 27019:2013 7.11.7.12 NERC CIP-602 BSI Standard 4 100-2:1 April 12 Strukturanalyse, M.2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten. NIST SP 800-53 Rev. 5 CM.6,PM.5

Abbildung 5: Auszug aus dem Assessment-Tool zum BWL IKT-Minimalstandard (Quelle BWL)

- **Funktion:** Hauptfunktionen oder Aktivitätsbereiche des NIST CSF 1.1



- **Kategorie:** Kategorie für die Funktion bzw. Hauptfunktionen oder Aktivitätsbereichen des NIST CSF 1.1
- **Aktivität:** Subkategorie der Hauptfunktionen oder Aktivitätsbereichen des NIST CSF 1.1
- **Bewertung:** Umsetzungs-Maturitäten (Tiers) gemäss Beschreibung unten
- **Empfehlung BWL-Priorisierung:** Priorisierungsempfehlung des BWL
- **Referenzen:** Referenzen zu Umsetzungsmassnahmen (Normen und Standards)

#### Die Umsetzungs-Maturitäten (Tiers) im BWL IKT-Minimalstandard - Assessment Tool:

- (4) Nicht wie im NIST CSF 1.1 werden für die Bewertung der Ziele, Vorgaben oder den Erfüllungsgrad nicht die Tiers verwendet. An dieser Stelle wurden Maturitäten eingeführt, um so die umfassenderen und präziseren Kriterien für die Beurteilung abzubilden. Dabei wird folgendes Rating verwendet:

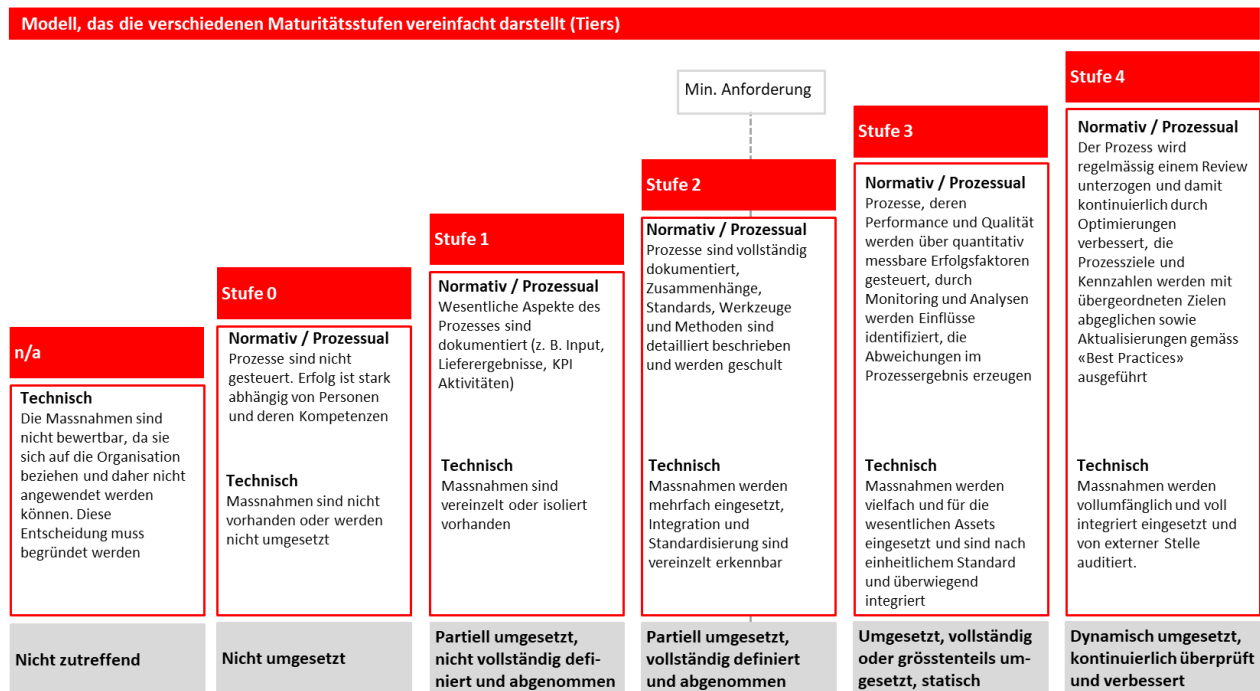


Abbildung 6: BWL IKT-Minimalstandard Maturitäten (Quelle BWL)



Das BWL IKT-Minimalstandard - Assessment Tool nach NIST CSF 1.1 ist Tool, welches für eine Self-Assessment erstellt werden kann. Dabei wird eine Momentaufnahme der vorliegenden Situation gemacht. Das Tool dient nicht als SOLL-IST Gegenüberstellung, somit kann damit auch keine GAP-Analyse gemacht werden. Die Anwendbarkeit bzw. SoA (Statement of Applicability) ist nur bedingt abbildbar, da zwar das einzelne Control als n/a bewertet werden können, aber es ist kein Feld für die Begründung vorgesehen.

#### 3.3.6 BFE Verpflichtung des IKT-Minimalstandards zur Steigerung der IKT-Resilienz

- (1) Die Revision der Stromversorgungsverordnung vom 14. März 2008 (StromVV; SR 734.71; Stand am 1. Juli 2024) hat zum Ziel, den IKT-Minimalstandard für die wichtigsten Stromversorger für verbindlich zu erklären. Die damit verpflichteten Akteure haben bei der Umsetzung der im Standard vorgesehen Massnahmen ein gewisses Schutzniveau zu erreichen. Im Sinne der Verhältnismässigkeit werden mehrere Schutzniveaus (Schutzprofile) mit abgestuften Anforderungen vorgesehen.
- (2) Der IKT-Minimalstandard legt eine Reihe von Themenbereichen mit Checkpoints der Cybersecurity fest und ist ein wichtiges Instrument, um den Schutz vor Cyberangriffen zu gewährleisten. Der Standard basiert auf dem US-amerikanischen NIST Cybersecurity Framework. Er enthält 108 Checkpoints, die in 23 Kategorien unterteilt sind. Die organisatorische Maturität der Cybersicherheit in einem Unternehmen und in den Organisationseinheiten kann mit Hilfe dieser Struktur bewertet und verbessert werden.
- (3) Die grundlegenden Themenbereiche des BWL IKT-Minimalstandards sind im Wesentlichen unverändert zum NIST CSF, erfordern jedoch für ihre Umsetzung eine gewisse Flexibilität, Anpassung an unternehmens-, organisationseinheiten-spezifische und neue Bedrohungen und Gefährdungen, technische Hilfsmittel und entsprechendes Fachwissen. Es werden darin keine technischen Lösungen vorgeschrieben. Die Unternehmen und Organisationseinheiten werden diese selbständig zu erarbeiten haben. Sie können





sich hierzu auch im Rahmen der bestehenden Verbandsstrukturen zusammenschliessen und einen entsprechenden branchenspezifischen Standard erarbeiten.



**Gemäss Stromversorgungsverordnung (StromVV; SR 734.71) Art. 5a wird der IKT-Minimalstandard mit den Vorgaben des BFE verpflichtet, muss deshalb von allen betroffenen Unternehmen und Organisationseinheiten der Strombranche angewendet und entsprechend umgesetzt werden.**

### 3.3.6.1 Schutzniveau gemäss BFE

- (1) Das Schutzniveau definiert die Anforderungen an das Mass der Umsetzung der im IKT-Minimalstandard festgehaltenen Checkpoints (Werte / Tier Level gemäss Kapitel 3 des BWL IKT-Minimalstandards). Die Netzbetreiber, Erzeuger, Speicherbetreiber und Dienstleister werden abhängig vom Umfang der transportierten Elektrizität beziehungsweise der Leistung in Kategorien eingeteilt. Die höchsten Anforderungen (Schutzniveaus) enthält die Kategorie A, die Kategorien B und C enthalten jeweils etwas geringere Anforderungen (Schutzniveaus). Für die kleinsten Marktakteure werden mit der Kategorie C nur Vorgaben (Schutzniveaus) für eine begrenzte Anzahl von Checkpoints vorgesehen. Checkpoints, für die keine entsprechenden Werte festgelegt werden, müssen nicht zwingend umgesetzt werden und bleiben daher unverbindliche Empfehlungen. Die drei Kategorien für Netzbetreiber, Energie Erzeuger und Dienstleister finden sich im Anhang 1a der Revision 24b des Strom VV's. Die darin festgehaltenen Werte (Schutzniveau) wurden für jede Kategorie auf der Grundlage der Kritikalität der Unternehmen, Organisationseinheiten und unter Berücksichtigung der zur Umsetzung erforderlichen Mittel festgelegt. Sie wurden in einer Arbeitsgruppe des Verband Schweizerischer Elektrizitätsunternehmen (VSE) unter Einbezug von Experten des BFE erarbeitet.
- (2) Um die verpflichteten Unternehmen und Organisationseinheiten einer Kategorie (A, B oder C) zuzuordnen, werden entsprechende Kriterien festgelegt. Sofern ein Unternehmen oder eine Organisationseinheit die Kriterien einer Kategorie erfüllt, ist dieses für das Unternehmen und die Organisationseinheit massgebend. So gilt beispielsweise die Kategorie A für Netzbetreiber, die eine transportierten Elektrizität von mindestens 450 GWh/Jahr erreichen (Ziff. 1.1 Anhang 1a). Bei der Festlegung der Kriterien wurden die Analysen und Praktiken anderer Fachstellen berücksichtigt. So entspricht das Kriterium von 450 GWh/Jahr, mit dem Netzbetreiber dem Schutzniveau A zugeordnet werden, einem vom Bundesamt für Bevölkerungsschutz (BABS) für die kritischen Infrastruktur von nationaler Bedeutung festgelegten Wert. Das Kriterium von 112 GWh/Jahr für die Kategorie B der Netzbetreiber und Dienstleister entspricht im Wesentlichen dem annualisierten Wert, der gemäss VSE eine Krise kennzeichnet.
- (3) Für die Erzeuger und die Speicherbetreiber wurde eine Leistung von 800 MW für die Kategorie A und 100 MW für die Kategorie B gewählt. Letztere entspricht dem in der Energieverordnung definierten Wert für Pumpspeicherkraftwerke von nationalem Interesse.
- (4) Erzeuger, Speicherbetreiber und Dienstleister der beiden Akteure werden unter einer Leistung von 100 MW nicht von der Pflicht zur Einhaltung des IKT-Minimalstandards erfasst. Eine Kategorie C ist für sie nicht vorgesehen. Soweit der Schwellenwert von 100 MW nicht erreicht wird, bleibt für sie der Standard lediglich eine Empfehlung. Dies zum einen, weil ihr Einfluss auf die Versorgungssicherheit weniger hoch ist als bei den direkt via Steuertechnologie auf das Netz zugreifenden Netzbetreibern und zum anderen, weil sie die Kosten der Cybersicherheit im Gegensatz zu den Netzbetreibern nicht in die Tarife einrechnen können.
- (5) Soweit externe Dienstleister, die im Auftrag eines Unternehmens oder einer Organisationseinheit die IKT-Systeme verwalten, dauerhaft Zugriff auf die Steuersysteme (operativen Leitsysteme) der Auftraggeber haben, müssen sie dieselben Vorgaben wie die Auftraggeber einhalten. Als Schwellenwert wird die Energiemenge gewählt, die von allen angeschlossenen Kunden über ein einziges System verteilt oder erzeugt wird.



- (6) Der Geltungsbereich und das zugewiesene Kategorie ist im Anhang 1a des Stromversorgungsverordnung (StromVV; SR 734.71) wie folgt festgelegt:

	Schutzniveau für Kategorie A	Schutzniveau für Kategorie B	Schutzniveau für Kategorie C
1.1 Netzbetreiber mit einer in ihrem Netzgebiet transportierten Elektrizität von:			
1.2 Dienstleister, die dauerhaft Anlagen von Netzbetreibern fernsteuern können, sofern sie dadurch über ein einziges System Zugriff haben auf eine transportierte Elektrizität von:	≥ 450 GWh/Jahr	≥ 112 GWh/Jahr und < 450 GWh/Jahr	< 112 GWh/Jahr
1.3 Erzeuger, mit Ausnahme der Kernkraftwerksbetreiber, und Speicherbetreiber, sofern sie Anlagen von insgesamt folgender Leistung betreiben, die sie über ein einziges System fernsteuern können:			
1.4 Dienstleister, die dauerhaft Anlagen von Erzeugern, mit Ausnahme der Kernkraftwerksbetreiber, oder Speicherbetreibern fernsteuern können, sofern sie dadurch über ein einziges System Zugriff haben auf eine Leistung von:	≥ 800 MW	≥ 100 MW und < 800 MW	-

**Tabelle 2:** Definition der Unternehmensprofile nach Strom VV (Quelle BFE/VSE)



**Gemäss Anhang 1a der Stromversorgungsverordnung (StromVV; SR 734.71) wird jedem betroffenen Unternehmen und allen Organisationseinheiten eine Kategorie mit definierten Schutzniveauwerten zugewiesen. Die Schutzniveauwerte der einzelnen Kategorien sind mit den zu behandelnden Subkategorien (Checkpoints) gemäss NIST CSF 1.1 verknüpft und mit einer minimalen, zu erfüllenden Maturität versehen.**

### 3.3.6.2 Zuweisung der Checkpoints auf Stufe Subkategorie zu den einzelnen Kategorien und festgelegt Schutzniveauwerte für die einzelnen Maturitäten (Tiers)

- (1) Gemäss Anhang 1a der Stromversorgungsverordnung (StromVV; SR 734.71) sind minimale Schutzniveauwerte gemäss Kapitel 3 des IKT-Minimalstandards zu erreichen.
- (2) Die minimalen Schutzniveauwerte sind im Anhang 1a der Stromversorgungsverordnung (StromVV; SR 734.71) festgelegt und auch aufgeführt.



**Im Anhang 1a der Stromversorgungsverordnung (StromVV; SR 734.71) sind die minimalen Werte für die Tiers/Maturitäten auf Stufe Subkategorie (Checkpoints) des NIST CSF 1.1 festgelegt und somit verbindlich bzw. müssen mindesten erreicht werden.**



### 3.3.7 ECom: Überwachung des Vorgehens und der Ergebnisse zur Steigerung der IKT-Resilienz



(1) Die ECom überwacht das Vorgehen und die Ergebnisse der Tätigkeiten zur Steigerung der IKT-Resilienz aufgrund ihrer Generalkompetenz (Art. 22 Abs. 1 StromVG) die Einhaltung von Artikel 8a StromVG und 5a StromVV.

(2) Die entsprechenden Aufsichtstätigkeiten sind in der Weisung 1/2024 «Aufsicht der Cybersicherheit der ECom» aufgeführt. In dieser Weisung wird das Vorgehen und die Anforderungen definiert. Folgende wichtigen Punkte sind aus der Weisung zu entnehmen:

#### Aufsicht:

- (3) Die ECom verfolgt bei der Aufsicht einen risikobasierten Ansatz bezüglich des sicheren Systembetriebs des Schweizer Stromnetzes. Ziel der Aufsicht ist die Steigerung der Resilienz gegenüber Cyberbedrohungen. Somit werden Unternehmen je nach Relevanz und Risikosituation für den sicheren und stabilen Systembetrieb des Schweizer Stromnetzes in unterschiedlicher Tiefe überwacht. Die Aufsichtsinstrumente sollen der ECom eine Beurteilung ermöglichen, ob die getroffenen Massnahmen den Risikoüberlegungen des Unternehmens entsprechen und die rechtlichen Vorgaben eingehalten sind. Dies bedeutet auch, dass die ECom aufgrund ihrer Regulierungstätigkeit Empfehlungen abgeben und / oder Massnahmen anordnen kann. Zur Durchsetzung von Massnahmen stehen der ECom die üblichen Rechtsmittel zur Verfügung. Aktuell sieht die ECom vor, drei Aufsichtsinstrumente ergänzend einzusetzen und zu kombinieren.

#### Umfragen:

- (4) Nach Inkrafttreten der revidierten StromVV haben die Unternehmen bestimmte Minimalanforderungen zu erfüllen. Die ECom wird diese in einer ersten Phase über eine Selbsteinschätzung im Rahmen einer Umfrage auf Basis des BWL-Assessment-Tools erheben. Die eingereichten Selbsteinschätzungen müssen durch ein Schreiben der jeweiligen Geschäftsleitung bestätigt werden. Diese Umfrage wird jährlich bei allen gemäss revidierter StromVV betroffenen Unternehmen durchgeführt. Diese Umfrage erlaubt es der ECom, einerseits eine Übersicht über das Erreichen der rechtlichen Vorgaben zu erstellen und andererseits Informationen über den Stand der Cybersicherheits-Massnahmen einzuholen und auszuwerten.

#### Sensibilisierungsgespräche:

- (5) Sensibilisierungsgespräche werden in erster Linie mit Unternehmen mit besonderer Relevanz für den sicheren und stabilen Systembetrieb des Schweizer Stromnetzes geführt. Ergänzend sind Sensibilisierungsgespräche auch aufgrund auffälliger Antworten in den Umfragen oder einer zufälligen Stichprobe möglich. Ziel dieser Gespräche ist es, konkrete Informationen zur Umsetzung der Cybersicherheits-Massnahmen zu gewinnen und dadurch die Ergebnisse der Umfrage qualitativ zu ergänzen. Die Sensibilisierungsgespräche finden regelmässig vor Ort bei den relevanten Unternehmen statt. Die Erkenntnisse aus den Gesprächen bilden eine Grundlage für die Einschätzung der Cybersicherheit beim Unternehmen sowie der Ableitung allfälliger Empfehlungen für Massnahmen. Deren Umsetzung kann in den nachfolgenden Sensibilisierungsgesprächen geprüft werden.

#### Audits

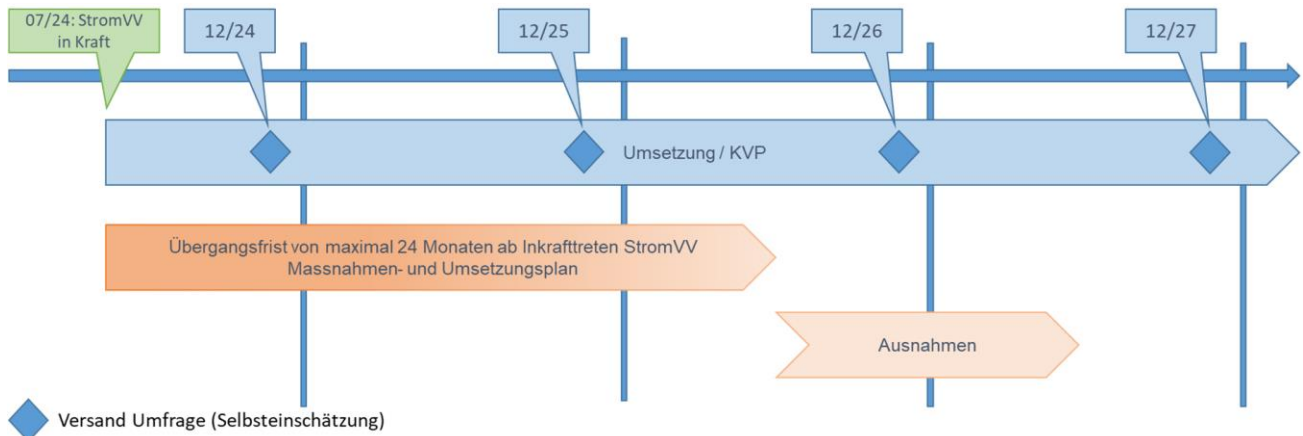
- (6) Als drittes Aufsichtsinstrument kann die ECom individuelle Audits durchführen. Diese sollen bestimmte technische Aspekte aufgrund von Auffälligkeiten bei der Umfrage oder den Sensibilisierungsgesprächen vertiefen. Ebenso können Audits aufgrund von externen Hinweisen oder einer zufälligen Stichprobe durchgeführt werden. Je nach Ziel und Zweck können diese Audits durch die ECom oder durch einen externen Auditor durchgeführt werden.

#### Übergang Minimalanforderungen StromVV

- (7) Die revidierte StromVV sieht zur Erreichung der geforderten minimalen Zielwerte keine Übergangsfrist vor. Damit die Selbsteinschätzungen aus der Umfrage bei den Unternehmen den Ist-Zustand möglichst gut abbilden, erlaubt die ECom eine Übergangsfrist zum Nachweis der Erreichung der geforderten Zielwerte von maximal 24 Monaten nach Inkrafttreten der revidierten StromVV. Für die Kategorien, in denen die Zielwerte nicht erreicht wurden, ist ein von der Geschäftsleitung bestätigter Massnahmen- und Umsetzungsplan mit konkreten verbindlichen Umsetzungszielen einzureichen. Werden aus Sicht der ECom die darin vorgeschlagenen Massnahmen nicht zeitnah umgesetzt, sucht die ECom das Gespräch mit den



betroffenen Unternehmen. Liegen nachvollziehbare Gründe vor, dass die Zielwerte nicht innerhalb der Übergangsfrist erreicht werden konnten, kann die ECom ausnahmsweise eine weitere Frist gewähren.



**Abbildung 7:** Ablaufschema Umsetzung Cybersicherheit-Minimalanforderungen (Quelle ECom)



**Die ECom überwacht das Vorgehen und die Ergebnisse der Tätigkeiten zur Steigerung der IKT-Resilienz aufgrund ihrer subsidiären Generalkompetenz (Art. 22 Abs. 1 StromVG) die Einhaltung von Artikel 8a StromVG und 5a StromVV.**

### 3.3.8 Bundesamt für Cybersicherheit (BACS): Meldepflicht und Unterstützung



(1) Das Bundesamt für Cybersicherheit (BACS) ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es ist verantwortlich für die koordinierte Umsetzung der Nationalen Cyberstrategie (NCS).

#### 3.3.8.1 Meldepflicht für kritische Infrastrukturen

(2) Erfolgreiche Cyberangriffe können weitreichende Folgen für die Verfügbarkeit und Sicherheit der Schweizer Wirtschaft haben. Die Bevölkerung, Behörden und Unternehmen sind täglich dem Risiko eines Cyberangriffs ausgesetzt. Heute fehlt eine Übersicht darüber, welche Angriffe wo stattgefunden haben, da Meldungen an das BACS nur auf freiwilliger Basis erfolgen. Dank einer Meldepflicht erhält das BACS künftig eine bessere Übersicht über die in der Schweiz erfolgten Cyberangriffe und die Vorgehensweisen der Angreifer. Dadurch wird eine bessere Einschätzung der Bedrohungslage möglich und Betreiberinnen und Betreiber kritischer Infrastrukturen können frühzeitig gewarnt werden. Der Bundesrat will durch die Meldepflicht sicherstellen, dass alle Betreiberinnen und Betreiber von kritischen Infrastrukturen am Informationsaustausch teilnehmen und so zur Frühwarnung beitragen.

#### 3.3.8.2 Pflicht des Bundes zur Unterstützung bei Cyberangriffen

(1) Die Gesetzesvorlage verpflichtet zudem nicht nur die Unternehmen zur Mitwirkung beim Schutz vor Cyberangriffen, sondern auch das BACS, den Meldenden subsidiäre Unterstützung bei der Reaktion auf Cyberangriffe anzubieten.





### 3.4 Institutionen, Frameworks, Normen, Standards, Spezifikation und Anleitungen (Guidelines) zur Steigerung der IKT-Resilienz

- (1) In diesem Kapitel werden die Institutionen, Frameworks, Normen, Standards und Spezifikation im Rahmen dieses Leitfadens zur Steigerung der IKT-Resilienz zusammenfassend beschrieben. Diese Beschreibungen geben einen groben Überblick. Um die IKT-Resilienz zu erhöhen, wird empfohlen, sich an aktuelle, etablierte und eingeführte Frameworks, Normen, Standard und Spezifikation, welche von anerkannten Organisationen und Institutionen publiziert werden, zu orientieren. Viele Normen, Standards und Spezifikationen dienen als Hilfe für die Umsetzung. Oft weisen die Publikationen keine Anwendungsbeispiele auf, sie dienen lediglich zur Orientierung, Definition von Massnahmen und helfen bei der Lösungsfindung.

#### 3.4.1 Frameworks, Normen, Standards und Spezifikationen

- (1) Frameworks, Normen, Standards und Spezifikationen spielen eine Schlüsselrolle bei der Steigerung der IKT-Resilienz, indem sie klare Strukturen und Richtlinien für die Sicherheit von Informations- und Kommunikationstechnologien bieten. Diese etablierten Modelle dienen als Referenzpunkte, um bewährte Praktiken zu definieren, Risiken zu identifizieren und Schutzmassnahmen umzusetzen.
- (2) Frameworks wie ISO/IEC 27001 bieten eine ganzheitliche Struktur für das Informationssicherheitsmanagement, während Frameworks wie das NIST Cybersecurity Framework konkrete Schritte und Checkpoints für die Risikominderung liefern. Normen und Spezifikationen setzen allgemein anerkannte Massstäbe für die Sicherheit von IKT-Systemen, wodurch Unternehmen und Organisationseinheiten eine klare Grundlage für ihre Sicherheitsstrategie erhalten.
- (3) Der Nutzen liegt nicht nur in der Festlegung von Mindestanforderungen, sondern auch in der Förderung von Interoperabilität und Vergleichbarkeit. Durch die Anwendung gemeinsamer Standards wird es einfacher, bewährte Praktiken zu teilen, Erfahrungen auszutauschen und die Zusammenarbeit in der Sicherheitsgemeinschaft zu stärken.
- (4) Zusätzlich dienen diese standardisierten Frameworks, Normen und Standards als Grundlage für Zertifizierungen und Assessments, was Unternehmen und Organisationseinheiten ermöglicht, ihre IKT-Resilienz nachweislich zu verbessern. Sie bieten klare Kriterien für die Evaluierung der Sicherheitspraktiken und unterstützen bei der laufenden Verbesserung der Sicherheitsmassnahmen.
- (5) Insgesamt tragen Frameworks, Normen, Standards und Spezifikationen dazu bei, die Sicherheit und Widerstandsfähigkeit von IKT-Systemen auf globaler Ebene zu stärken. Sie bieten einen gemeinsamen Bezugsrahmen, der es Unternehmen und Organisationseinheiten ermöglicht, systematisch auf Bedrohungen zu reagieren und ihre IKT-Infrastruktur nachhaltig widerstandsfähiger zu gestalten.



**Die VSE Cyber Security Task Force Experten empfehlen die gültigen und aktuellen Frameworks, Normen, Standards und Spezifikationen anzuwenden.**



**Im Angang befindet sich eine detaillierte Auflistung der Frameworks Normen, Standards und Spezifikationen.**



**Die Auflistung im Anhang nicht abschliessend. Es wurden nur Element aufgeführt, welche in direktem Zusammenhang zu diesem Leitfaden stehen. Es gibt noch weitere Dokumente, welche zur Steigerung der IKT-Resilienz verwendet werden können.**



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**

#### 3.4.2 Guidelines und spezielle Publikationen

- (1) Guidelines und spezielle Publikationen tragen wesentlich zur Steigerung der IKT-Resilienz bei, indem sie klare Richtlinien, bewährte Praktiken und spezifische Empfehlungen für die Sicherheit und Widerstandsfähigkeit von Informations- und Kommunikationstechnologien bereitstellen. Diese Ressourcen dienen als wertvolle Wegweiser für Unternehmen und Organisationseinheiten, um potenzielle Risiken zu identifizieren, geeignete Schutzmassnahmen zu implementieren und auf aktuelle Bedrohungen angemessen zu reagieren.



- (2) Die Guidelines bieten praktische Anleitungen für die Entwicklung von Sicherheitsrichtlinien, die Implementierung von Schutzmechanismen und die Schulung von Mitarbeitern. Sie unterstützen dabei, ein solides Fundament für eine umfassende IKT-Sicherheitsstrategie zu schaffen. Spezielle Publikationen gehen oft tiefer in bestimmte Sicherheitsaspekte und -technologien ein, was Unternehmen und Organisationseinheiten ermöglicht, sich spezifisch auf relevante Bedrohungen vorzubereiten.
- (3) Darüber hinaus tragen Guidelines und Publikationen dazu bei, den aktuellen Wissensstand in der sich schnell verändernden IKT-Sicherheitslandschaft zu vermitteln. Sie helfen Unternehmen und Organisationseinheiten dabei, auf dem neuesten Stand zu bleiben, indem sie innovative Ansätze, aktuelle Bedrohungen und bewährte Praktiken kommunizieren. Dies fördert eine proaktive Haltung gegenüber neuen Herausforderungen.
- (4) Die klare Kommunikation von Best Practices Ansätzen und Empfehlungen in diesen Ressourcen unterstützt Unternehmen und Organisationseinheiten dabei, eine robuste Sicherheitskultur zu etablieren und sicherzustellen, dass alle Beteiligten, vom Management bis zu den Mitarbeitern, ein gemeinsames Verständnis für die Bedeutung der IKT-Resilienz entwickeln. Insgesamt tragen Guidelines und spezielle Publikationen dazu bei, die Widerstandsfähigkeit von IKT-Systemen zu stärken und die Fähigkeit von Unternehmen und Organisationseinheiten zu verbessern, auf potentielle Bedrohungen angemessen zu reagieren.

Folgende Guidelines und spezielle Publikationen werden in diesem Leitfaden verwendet oder sind auch Sicht VSE hilfreich:



- BDEW-OE-VSE Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
- NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security
- VSE ICT Continuity
- VSE Handbuch Grundschutz für «Operational Technology» in der Stromversorgung
- VSE Physische Sicherheit für Unterwerke (PSU – CH 2019)
- VSE Business Continuity & Disaster Recovery
- VSE Personensicherheitsprüfung
- VSE Datapolicy in der Energie Branche", VSE 2022



Die VSE Cyber Security Task Force Experten empfehlen die gültigen und aktuellen Frameworks, Normen, Standards und Spezifikationen anzuwenden.



Die Auflistung ist in diesem Abschnitt nicht abschliessend. Es wurden nur Element aufgeführt, welche in direktem Zusammenhang zu diesem Leitfaden stehen. Es gibt noch unzählige weitere Dokumente, welche zur Steigerung der IKT-Resilienz verwendet werden können.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.

### 3.5 Zertifizierungen und Weiterbildungen zur Steigerung der IKT-Resilienz

- (1) Zertifizierungen und Weiterbildungen spielen eine entscheidende Rolle bei der Steigerung der IKT-Resilienz in Unternehmen und Organisationseinheiten. Folgend wird erläutert, wieso sie von grosser Bedeutung sind:
  - **Fachwissen und Qualifikation:** Zertifizierte Fachleute und gut ausgebildete Mitarbeiter verfügen über das erforderliche Fachwissen, um effektive Massnahmen zur Cybersicherheit und IKT-Resilienz umzusetzen. Dies trägt dazu bei, die Wahrscheinlichkeit von Sicherheitsvorfällen zu reduzieren und die Reaktionsfähigkeit im Notfall zu verbessern.
  - **Aktualisierte Kenntnisse:** Die Technologie und die Bedrohungslandschaft entwickeln sich ständig weiter. Durch kontinuierliche Weiterbildung und Zertifizierung bleiben Fachleute auf dem neuesten Wissensstand und sind besser in der Lage, sich den ständig ändernden Anforderungen anzupassen.
  - **Umsetzung von Best Practices:** Zertifizierungsprogramme basieren oft auf bewährten Praktiken und Standards, die von Experten entwickelt wurden. Sie bieten klare Leitlinien zur Implementierung von Sicherheitsmassnahmen und zur Gewährleistung der IKT-Resilienz.



- **Vertrauen und Glaubwürdigkeit:** Zertifizierungen sind ein Zeichen für Fachkompetenz und Professionalität. Unternehmen und Organisationseinheiten, die zertifizierte Mitarbeiter beschäftigen, signalisieren ihren Kunden und Partnern, dass sie die Sicherheit und Resilienz ihrer IKT-Systeme ernst nehmen.
  - **Risikominderung:** Durch gut ausgebildete Mitarbeiter und zertifizierte Experten können Unternehmen Schwachstellen identifizieren, Sicherheitslücken schliessen und Massnahmen zur Risikominderung ergreifen, um sich vor Cyberangriffen und anderen IKT-bezogenen Gefahren zu schützen.
  - **Gelebte Sicherheitskultur:** Gut ausgebildete Mitarbeiter im Bereich IKT-Security erhöht das Verständnis gegenüber Cyberbedrohungen und das Wissen auf diese richtig und angemessen zu reagieren. Dies wiederum ermöglicht es einem Unternehmen und einer Organisationseinheit einfacher eine gelebte Sicherheitskultur zu etablieren.
- (2) Insgesamt sind Zertifizierungen und Weiterbildungen wesentliche Instrumente, um die IKT-Resilienz zu stärken und die Fähigkeit von Unternehmen und Organisationseinheiten zu verbessern, auf Cyberbedrohungen und technische Ausfälle angemessen zu reagieren. Sie tragen dazu bei, die Sicherheit, Stabilität und Effizienz von IKT-Systemen zu gewährleisten.

### 3.5.1 Aus- und Weiterbildungen mit Zertifizierungen

#### 3.5.1.1 VSE IT-/OT-Cyber-Security für System-Engineers



(1) Digitalisierung und Cybersecurity sind herausfordernde Themen in allen Unternehmen und Organisationseinheiten. Der modular aufgebaute Kurs für System-Engineers behandelt alle relevanten Aspekte zu IT/OT, Schwachstellen, Netzwerk Schutzfunktionen, Incident Management und Systemsicherheit. Er basiert auf dem VSE-Handbuch «Grundschutz für Operational Technology (OT) in der Stromversorgung».

(2) Das tiefgreifende Verständnis ist Schwerpunkt der Veranstaltung. Es wird eine detaillierte Sicht der Thematik vermittelt. Der Kurs zeigt auf, wie die Cyber-Risiken in der kritischen Infrastruktur der Stromversorgung auf ein akzeptables Mass reduziert werden können.



**Empfehlung der VSE Cyber Security Task Force Experten:**  
Es wird empfohlen den Lehrgang vollumfänglich zu besuchen

#### 3.5.1.2 Ausbildungsangebot des VSE im Rahmen des Leitfadens

- (1) Beim VSE sind Schulungen und Instruktionen im Rahmen dieses Leitfadens in Planung. Der VSE ist bestrebt, dass die EVUs für die Steigerung der IKT-Resilienz und Einhaltung der gesetzlichen Vorgaben im Bereich Cyber Security die nötigen Schulungen und Instruktionen beim Verband absolvieren können.

#### 3.5.1.3 Weitere Aus- und Weiterbildungsmöglichkeiten

- (1) Der VSE ist bestrebt, dass für seine Mitglieder die notwendigen Ausbildungen in angemessener Qualität, Umfang und Inhalt zu Verfügung stehen. Damit erhalten die EVUs das optimale Rüstzeug, um die regulatorischen Anforderungen zu verstehen und die notwendigen Massnahmen gemäss diesem Leitfaden umsetzen zu können. Das heutige Ausbildungsangebot, für Fachkräfte der Energiebranche, die diese Anforderungen erfüllen sind heute nur minimal oder gar nicht vorhanden. Es fehlen spezifische Ausbildungen für OT-Sicherheitsverantwortliche und Fachkräfte, welche den benötigten Schulungsinhalt Zielgruppen gerecht vermitteln können.
- (2) Aus diesem Grund führt der VSE eine Liste von empfohlenen Aus- und Weiterbildungen im Bereich Umsetzung des IKT-Minimalstandards mit Fokus auf die Steigerung der IKT-Resilienz in der Strombranche ein. Anbieter von Kursen, Aus- und Weiterbildungen haben die Möglichkeit, eine Aufnahme in diese Liste zu beantragen. Die VSE Cyber Security Task Force Experten werden die Anfragen entlang definierter Kriterien prüfen und anschließend die Freigabe für die Aufnahme auf die Liste erteilen. Die entsprechenden Kurse, Lehrgänge und Aus-/Weiterbildungen werden beim VSE auf der «Liste empfohlener Cybersecurity Aus- und Weiterbildungen» geführt und können auf der Website eingesehen werden.





Es werden viele Kurse, Aus- und Weiterbildungen für den Bereich Cyber Security angeboten, welche nur bedingt für den Bereich Umsetzung des IKT-Minimalstandards mit Fokus auf die Steigerung der IKT-Resilienz in der Strombranche geeignet sind bzw. das nötige Know-How dafür vermitteln. Bei der Wahl der Kurse, Aus- und Weiterbildungen ist deshalb grosse Vorsicht geboten. Oft werden die Unkenntnisse der Bedarfsträger ausgenutzt.



#### Empfehlung der VSE Cyber Security Task Force Experten:

Es sollen nur Kurse, Lehrgänge, Aus- und Weiterbildungen absolviert werden, welche auf der «VSE Liste empfohlener Cybersecurity Aus-/Weiterbildungen» im Bereich Umsetzung des IKT-Minimalstandards mit Fokus auf die Steigerung der IKT-Resilienz in der Strombranche aufgeführt sind.

### 3.5.2 Sicherheitszertifizierungen für Unternehmen und Organisationseinheiten

#### 3.5.2.1 Zertifizierung des ISMS nach ISO 27001

- (1) Die ISO 27001-Zertifizierung bezieht sich auf ein Information Security Management System (ISMS). Dieser Standard legt Anforderungen für die Einführung, Umsetzung, Aufrechterhaltung und ständige Verbesserung eines dokumentierten ISMS in einer Organisation fest. Der Prozess umfasst die Analyse von Kontext und Risiken, die Festlegung des Anwendungsbereichs, Implementierung von Sicherheitsmassnahmen, Überwachung der Leistung und regelmässige Bewertungen. Die Zertifizierung erfolgt durch eine unabhängige Stelle und bestätigt die Konformität des ISMS mit ISO 27001, was auf einen effektiven Schutz von Informationen und Daten hinweist.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.

#### 3.5.2.2 Zertifizierung der Anwendung des NIST Cyber Security Frameworks

- (1) Die Zertifizierung für die Anwendung des NIST Cyber Security Frameworks erfolgt nicht direkt durch eine standardisierte Zertifizierungsstelle, wie es bei einigen anderen Standards der Fall ist (z. B. ISO 27001). Das NIST Cyber Security Framework (CSF) ist ein Rahmenwerk mit Checkpoints und nicht ein Zertifizierungsstandard mit konkreten Massnahmen. Unternehmen und Organisationseinheiten können jedoch ihre Einhaltung des Frameworks auf verschiedene Weisen nachweisen:
  - **Selbstbewertung:** Unternehmen und Organisationseinheiten können eine Selbstbewertung durchführen, um zu prüfen, mit welcher Maturität ihr Unternehmen und ihre Organisationseinheiten die NIST CSF-Kategorien bzw. Subkategorien erfüllen.
  - **Drittanbieter-Audits:** Unternehmen und Organisationseinheiten können externe Sicherheitsdienstleister oder Auditoren beauftragen, ihre Sicherheitspraktiken anhand des NIST CSF zu überprüfen und entsprechende Empfehlungen abzugeben.
  - **Branchenspezifische Anforderungen:** In einigen Branchen sind spezifische Vorgaben oder Verordnungen in Bezug auf Cybersicherheit vorhanden. Die Erfüllung dieser Vorschriften kann als indirekter Nachweis für die Anwendung des NIST CSF dienen.
  - **Bestätigung durch Lieferanten oder Partner:** Unternehmen und Organisationseinheiten können von ihren Lieferanten oder Partnern Nachweise darüber verlangen, dass sie ihre Sicherheitspraktiken gemäss dem NIST CSF implementiert haben.
- (2) Die NIST selbst ermutigt Unternehmen und Organisationseinheiten, das Framework anzupassen und zu implementieren, um den individuellen Bedürfnissen und Risiken gerecht zu werden. Daher kann die Zertifizierung in diesem Kontext eher auf die Wirksamkeit und Reife der Sicherheitspraktiken eines Unternehmens und der Organisationseinheiten im Einklang mit dem NIST CSF abzielen als auf eine formelle, standardisierte Zertifizierung.



Zusammen mit den offiziellen nationalen Zertifizierungsstellen sind Bestrebungen vom BWL im Gange, dass in Zukunft eine Zertifizierung für die Anwendung des NIST Cyber Security Framework angeboten werden kann.





## 4. Basis die für Effektivität zur Verbesserung der IKT-Resilienz

### 4.1 Das Integrierte Management System IMS

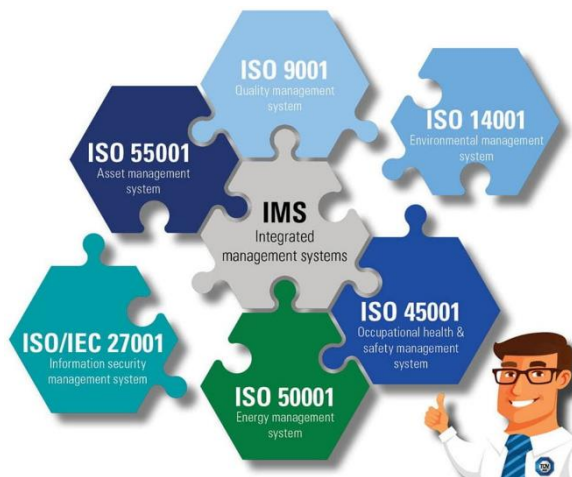


Abbildung 8: Integriertes Management System  
IMS(Quelle TÜV Süd)

(1) Das Integrierte Management System (IMS) dient als umfassender Rahmen für die Steigerung der Resilienz der Informations- und Kommunikationstechnologie (IKT). Die Verwendung eines IMS in diesem Kontext zielt darauf ab, eine ganzheitliche und koordinierte Herangehensweise an das Management von IKT-Ressourcen zu schaffen, um auf Herausforderungen, Bedrohungen und Störungen effektiv reagieren zu können. Hier sind verschiedene Aspekte, die die Verwendung des IMS zur Steigerung der IKT-Resilienz umfassen:

- **Integration von Managementsystemen:** Das IMS integriert verschiedene Managementsysteme, wie zum Beispiel Qualitätsmanagement (ISO 9001), Umweltmanagement (ISO 14001), Informationssicherheitsmanagement (ISO 27001) und Managementsysteme für Sicherheit und Gesundheit bei der Arbeit (ISO 45001). Diese Integration ermöglicht eine kohärente und effiziente Verwaltung von IKT-Ressourcen, indem sie verschiedene Aspekte der Organisation miteinander verknüpft.
  - **Risikomanagement:** Das IMS ermöglicht ein integriertes Risikomanagement für die IKT. Risiken in Bezug auf Sicherheit, Compliance, Umweltauswirkungen und Qualität können analysiert und bewertet werden. Dies ermöglicht eine proaktive Identifikation von Risiken für die IKT und die Implementierung von Massnahmen zur Risikominderung.
  - **Kontinuierliche Verbesserung:** Durch den PDCA-Zyklus (Plan-Do-Check-Act) fördert das IMS eine Kultur der kontinuierlichen Verbesserung. Dies ist entscheidend, um die Resilienz der IKT langfristig zu stärken. Unternehmen und Organisationseinheiten können aufgrund von Erfahrungen und Veränderungen in der Bedrohungslandschaft ihre Prozesse und Massnahmen kontinuierlich optimieren.
  - **Notfall- und Kontinuitätsmanagement:** Das IMS ermöglicht die Integration von Notfall- und Kontinuitätsmanagementprozessen über alle Managementsysteme eines Unternehmens und der Organisationseinheiten. Dies umfasst die Entwicklung von Notfallplänen, die regelmässige Überprüfung der Wirksamkeit dieser Pläne und die Schulung von Mitarbeitern für den Umgang mit IKT-Störungen oder Sicherheitsvorfällen.
  - **Ganzheitlicher Ansatz:** Das IMS fördert einen ganzheitlichen Ansatz für das IKT-Management. Es berücksichtigt nicht nur technologische Aspekte, sondern auch organisatorische und personelle Faktoren. Dies ist entscheidend, um die Widerstandsfähigkeit der IKT in einem umfassenden Kontext zu verbessern.
  - **Compliance-Management:** Die Integration von Compliance-Management in das IMS stellt sicher, dass die IKT-Ressourcen den geltenden Vorschriften entsprechen. Dies ist wichtig, um rechtliche Anforderungen im Bereich der IKT-Sicherheit zu erfüllen und damit die Resilienz zu stärken.
  - **Schulung und Bewusstseinsbildung:** Das IMS unterstützt Schulungs- und Bewusstseinsprogramme für Mitarbeiter im Umgang mit IKT-Ressourcen. Ein gut informiertes und geschultes Personal trägt wesentlich zur Stärkung der IKT-Resilienz bei.
- (2) Zusammengefasst bietet die Verwendung des IMS als Basis für die Steigerung der IKT-Resilienz eine strukturierte und integrierte Herangehensweise, um auf Herausforderungen und Störungen zu reagieren und gleichzeitig eine nachhaltige Leistung der IKT sicherzustellen.



#### Empfehlung der VSE Cyber Security Task Force Experten:

Die Einführung eines Integrierten Management Systems IMS bietet einen strukturierten und ganzheitlichen Ansatz, welcher zur Steigerung der IKT Resilienz eine vollumgängliche Basis bietet. Somit wird empfohlen, dass ein IMS oder eine ähnliche Form angewendet wird.





**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**



**Dieser Leitfaden basiert auf den Grundsätzen eines Integrierten Management System (IMS). Es wird aber primär nur auf die Bereiche der Informationssicherheit eingegangen. Dies mit Hilfe des Aufbaus und Umsetzung eines Information Sicherheit Management Systems (ISMS). Verknüpfungen zu anderen Management Systemen, werden punktuell behandelt und aufgezeigt, wo dies notwendig ist.**

## **4.2 Informationssicherheitsmanagement (ISM) als Basis zur Steigerung der IKT-Resilienz**

- (1) Die Anwendung des Informationssicherheitsmanagements (ISM) als Grundlage zur Steigerung der Resilienz der Informations- und Kommunikationstechnologie (IKT) spielt eine entscheidende Rolle in der modernen Unternehmenslandschaft. Das ISM ist ein ganzheitlicher Ansatz, der darauf abzielt, die Sicherheit, Integrität und Verfügbarkeit von Informationen zu gewährleisten. Im Kontext der IKT-Resilienz trägt das ISM zu verschiedenen Schlüsselaspekten bei:
- (2) Das ISM ermöglicht eine systematische Identifikation und Bewertung von Risiken für die Informationssicherheit. Durch die Analyse von Bedrohungen und Schwachstellen können präventive Massnahmen ergriffen werden, um die potentiellen Auswirkungen auf die IKT zu minimieren.
- (3) Ein integraler Bestandteil des ISM ist die Entwicklung von Notfallplänen und -prozessen. Diese gewährleisten eine strukturierte Reaktion auf Sicherheitsvorfälle und IKT-Störungen. Notfallpläne sorgen dafür, dass die Organisation in der Lage ist, schnell und effektiv auf Krisensituationen zu reagieren.
- (4) Das ISM fördert eine kontinuierliche Überwachung und Verbesserung der Sicherheitsprozesse durch den PDCA-Zyklus (Plan-Do-Check-Act). Durch die Identifizierung von Schwächen können angemessene Massnahmen ergriffen werden, um die IKT-Resilienz kontinuierlich zu stärken.
- (5) Das ISM stellt sicher, dass Sicherheitsziele mit den übergeordneten Geschäftszielen in Einklang stehen. Dies gewährleistet, dass die IKT-Resilienz direkt zur Geschäftskontinuität beiträgt und strategische Unternehmensziele unterstützt.
- (6) Durch das ISM werden Schulungs- und Sensibilisierungsprogramme für Mitarbeiter im Umgang mit Informationssicherheit unterstützt. Gut informierte Mitarbeiter sind entscheidend für die Aufrechterhaltung der IKT-Resilienz.
- (7) Das ISM fördert die Kommunikation und Zusammenarbeit zwischen verschiedenen Abteilungen und Interessengruppen. Eine koordinierte Herangehensweise ist wichtig, um eine effektive Reaktion auf Sicherheitsvorfälle zu gewährleisten und die IKT-Resilienz zu stärken.
- (8) Das ISM erleichtert die Einhaltung von Compliance-Anforderungen und gesetzlichen Vorgaben im Bereich der Informationssicherheit. Dies minimiert rechtliche Risiken und stärkt die IKT-Resilienz gegenüber regulatorischen Herausforderungen.
- (9) Durch die Implementierung von Monitoring- und Frühwarnsystemen kann das ISM potentielle Bedrohungen frühzeitig erkennen. Dies ermöglicht eine proaktive Reaktion, um Schäden zu minimieren und die IKT-Resilienz zu stärken.
- (10) Zusammenfassend bietet das ISM eine strukturierte Methodik, um die IKT-Resilienz zu erhöhen. Es konzentriert sich auf präventive Massnahmen, Notfallplanung, kontinuierliche Verbesserung und die Einhaltung von Standards, um eine robuste und widerstandsfähige IKT-Umgebung zu schaffen.



**Das Informationssicherheitsmanagement (ISM) kann mit der Hilfe eines Information Sicherheit Management Systems (ISMS) operationalisiert und betrieben werden. Dieser Leitfaden beschreibt in 8-Phasen den Aufbau und Betrieb eines ISMS nach ISO27001.**



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Einführung des Informationssicherheitsmanagement ISM bietet einen strukturierten und ganzheitlichen Ansatz, welcher zur Steigerung der IKT Resilienz eine umfassende Basis bietet. Somit wird empfohlen, dass ein ISM eingeführt werden soll.**



#### 4.3 Managementsystem für Sicherheit und Gesundheit bei der Arbeit zur Unterstützung der Steigerung der IKT-Resilienz

- (1) Das Management-System für Sicherheit und Gesundheit bei der Arbeit, bietet eine wichtige Unterstützung zur Steigerung der Resilienz der Informations- und Kommunikationstechnologie (IKT). Dieses Managementsystem legt einen strukturierten Rahmen fest, um die Sicherheit und Gesundheit der Mitarbeiter am Arbeitsplatz zu gewährleisten, was wiederum zur Stärkung der IKT-Resilienz beiträgt.
- (2) Ein zentraler Aspekt des Managementsystems für Sicherheit und Gesundheit bei der Arbeit ist die systematische Identifikation und Bewertung von Risiken im Zusammenhang mit Sicherheit und Gesundheit bei der Arbeit. Dies schliesst nicht nur physische Risiken am Arbeitsplatz ein, sondern auch potentielle Gefahren im Bereich der IKT. Durch die Analyse von Arbeitsprozessen, -umgebungen und -bedingungen können mögliche Schwachstellen identifiziert werden, die die IKT beeinflussen könnten.
- (3) Das Managementsystem fördert ausserdem die Entwicklung von klaren Richtlinien und Verfahren für Notfallsituationen und Notfallmanagement. Dies ist entscheidend, um auf unvorhergesehene Ereignisse oder Sicherheitsvorfälle in der IKT angemessen reagieren zu können. Ein gut ausgearbeiteter Notfallplan ermöglicht es, schnell Massnahmen zu ergreifen und die Auswirkungen von Störungen zu minimieren.
- (4) Das Management-System unterstützt ebenfalls bei der Integration von Sicherheits- und Gesundheitsaspekten in die Planung und Umsetzung von IKT-Strategien. Dies trägt dazu bei, sicherzustellen, dass Sicherheitsüberlegungen von Anfang an in die Entwicklung und Implementierung von IKT-Systemen einfließen. Die Verbindung zwischen Arbeitssicherheit und IKT-Sicherheit wird somit gestärkt.
- (5) Des Weiteren legt das Managementsystem grossen Wert auf die kontinuierliche Verbesserung von Sicherheits- und Gesundheitsmassnahmen. Dieser Ansatz ermöglicht es Unternehmen und Organisationseinheiten, nicht nur auf aktuelle Risiken zu reagieren, sondern auch proaktiv Massnahmen zu ergreifen, um die IKT-Resilienz langfristig zu stärken. Durch regelmässige Überprüfungen und Anpassungen kann auf sich verändernde Bedrohungen in der IKT-Landschaft reagiert werden.
- (6) Schulungen und Sensibilisierungsprogramme für Mitarbeiter, die durch die ISO 45001 gefördert werden, spielen eine wichtige Rolle bei der Stärkung der IKT-Resilienz. Gut informierte und geschulte Mitarbeiter sind besser in der Lage, sicherheitsrelevante Aspekte in Bezug auf die IKT zu verstehen und umzusetzen.
- (7) Zusammenfassend bietet die ISO 45001 als Management-System für Sicherheit und Gesundheit bei der Arbeit eine ganzheitliche Herangehensweise, die nicht nur die physische Gesundheit der Mitarbeiter schützt, sondern auch dazu beiträgt, die Widerstandsfähigkeit und Widerstandskraft der IKT-Infrastruktur zu stärken. Dies erfolgt durch eine systematische Risikobewertung, klare Richtlinien für Notfälle, Integration von Sicherheitsaspekten in IKT-Strategien, kontinuierliche Verbesserung und Schulungen für Mitarbeiter.



In diesem Leitfaden wird nicht vollumfänglich auf das Managementsystem für Sicherheit und Gesundheit bei der Arbeit eingegangen. Es werden nur die Elemente verwendet und beschrieben, welche zur Erhöhung der IKT-Resilienz beitragen.



##### Empfehlung der VSE Cyber Security Task Force Experten:

Die Einführung eines Managementsystem für Sicherheit und Gesundheit bei der Arbeit sollte bei Unternehmen und Organisationseinheiten eingeführt und betrieben werden. Dieses System unterstützt die Unternehmen und Organisationseinheiten bei der Steigerung der IKT-Resilienz.

#### 4.4 Prozess-, Risiko-, Business Continuity- und Notfallmanagement als weitere Grundlagen zur Steigerung der IKT-Resilienz



Prozess-, Risiko-, Business Continuity- und Notfallmanagement bilden weitere wichtige Grundpfeiler für die Steigerung der IKT-Resilienz. Es sind mächtige und umfangreiche Instrumente für ein solides und effektives Management des Unternehmens und der Organisationseinheiten. Sie liefern wichtig Vorgaben und Inputs für die Effektivität zur Steigerung der IKT-Resilienz. Auf die Beschreibung, Einführung und den Betrieb dieser grundlegenden Managementsystemen wird in diesem Leitfaden nur bedingt bzw. beschränkt eingegangen.

##### 4.4.1 Prozessmanagement

- (1) Das Prozessmanagement bezieht sich auf die systematische Planung, Gestaltung, Umsetzung, Überwachung und kontinuierliche Verbesserung von Geschäftsprozessen innerhalb einer Organisation. Geschäftsprozesse sind wiederkehrende, strukturierte Abläufe, die in Unternehmen und



Organisationseinheiten auftreten, um bestimmte Ziele zu erreichen, wie beispielsweise die Bereitstellung von Produkten oder Dienstleistungen, die Optimierung von Arbeitsabläufen oder die Erfüllung von Kundenanforderungen.

- (2) Das Prozessmanagement zielt darauf ab, diese Prozesse effizienter, effektiver und kundenorientierter zu gestalten. Nachfolgend sind einige wichtige Aspekte des Prozessmanagements aufgeführt:
- **Prozessidentifikation:** Zunächst müssen die Prozesse innerhalb einer Organisation identifiziert werden. Dies beinhaltet das Erkennen, welche Abläufe stattfinden, wie sie strukturiert sind und wer für sie verantwortlich ist.
  - **Prozessdesign:** Nach der Identifikation werden die Prozesse analysiert und gegebenenfalls neugestaltet. Ziel ist es, Prozesse so zu optimieren, dass sie die gewünschten Ergebnisse effizient und effektiv liefern.
  - **Prozessimplementierung:** Die überarbeiteten Prozesse werden in den Unternehmen und Organisationseinheiten umgesetzt. Dies kann Schulungen, Veränderungsmanagement, die Einführung von Technologien oder Tools zur Unterstützung der Prozesse umfassen.
  - **Prozessüberwachung:** Die Prozesse werden kontinuierlich überwacht, um sicherzustellen, dass sie ordnungsgemäß ablaufen und die gewünschten Ergebnisse erzielen. Dies beinhaltet die Verwendung von Leistungsindikatoren (KPIs) und Berichterstattungssystemen.
  - **Prozesssteuerung:** Bei Bedarf werden Massnahmen ergriffen, um Prozesse anzupassen oder Probleme zu beheben. Dies kann die Anpassung von Ressourcen, Schulungen oder anderen Massnahmen zur Prozessverbesserung umfassen.
  - **Prozessoptimierung:** Das Prozessmanagement strebt eine kontinuierliche Verbesserung an. Unternehmen und Organisationseinheiten suchen ständig nach Möglichkeiten, Prozesse effizienter und effektiver zu gestalten. Dies kann durch den Einsatz von Lean-Methoden, Six Sigma, Total Quality Management (TQM) und anderen Methoden zur Prozessoptimierung erreicht werden.
  - **Kundenorientierung:** Im Prozessmanagement liegt ein starker Fokus auf den Kundenanforderungen. Die Gestaltung und Verbesserung von Prozessen zielt darauf ab, die Kundenzufriedenheit zu erhöhen und die Bedürfnisse und Erwartungen der Kunden zu erfüllen.
- (3) Prozessmanagement ist von entscheidender Bedeutung, da es zur Steigerung der Effizienz, Senkung der Kosten, Verbesserung der Qualität und Steigerung der Wettbewerbsfähigkeit beitragen kann. Es ist ein kontinuierlicher Prozess, der die Anpassung an sich ändernde Bedingungen und die Berücksichtigung von Kundenfeedback erfordert.

#### 4.4.2 Risikomanagement

- (1) Das Risikomanagement ist ein systematischer Prozess Identifikation, Analyse, Evaluation, Bewältigung sowie Kommunikation und Überwachung von Risiken, die ein Unternehmen und die Organisationseinheiten beeinflussen können. Das Hauptziel des Risikomanagements besteht darin, Risiken zu minimieren oder zu kontrollieren, um die Wahrscheinlichkeit negativer Ereignisse zu reduzieren und gleichzeitig Chancen zu nutzen, um die Unternehmensziele zu erreichen. Hier sind die grundlegenden Schritte und Prinzipien des Risikomanagements:
- **Risikoidentifikation:** In diesem Schritt werden alle potentiellen Risiken, die eine Organisation betreffen können, ermittelt. Dies umfasst interne und externe Risiken, wie beispielsweise finanzielle Risiken, operationelle Risiken, rechtliche Risiken, technologische Risiken oder wettbewerbsbedingte Risiken.
  - **Risikobewertung:** Nach der Identifikation von Risiken werden diese bewertet, um ihre Auswirkungen und Eintrittswahrscheinlichkeit zu bestimmen. Dies ermöglicht es, die Risiken nach ihrer Priorität zu ordnen und zu entscheiden, auf welche Risiken die Organisation ihr Hauptaugenmerk legen soll.
  - **Risikobewältigung:** Nach der Bewertung der Risiken werden Risiko-Behandlungsstrategien entwickelt. Es gibt verschiedene Möglichkeiten, Risiken zu behandeln, darunter:
    - Risikovermeidung: Massnahmen ergreifen, um das Risiko vollständig zu eliminieren.
    - Risikominderung: Massnahmen ergreifen, um die Eintrittswahrscheinlichkeit oder die Auswirkung eines Risikos zu reduzieren.
    - Risikoübertragung: Das Risiko wird auf Dritte, wie Versicherungen oder Vertragspartner, übertragen.





- Risikoakzeptanz: Das Risiko wird bewusst akzeptiert, z.B. wenn die Kosten der Risikobehandlung höher sind als der mögliche Schaden.
  - **Risikokontrolle:** Implementierung von Massnahmen und Kontrollen, um sicherzustellen, dass die festgelegten Risikobewältigungsstrategien effektiv umgesetzt werden. Dies umfasst die Überwachung von Risiken im laufenden Betrieb, die Überprüfung von Prozessen und die Anpassung von Massnahmen, wenn erforderlich.
  - **Risikokommunikation:** Effektive Kommunikation von Risiken und Risikobewältigungsstrategien innerhalb der Organisation sowie an Stakeholder wie Kunden, Investoren und Regulierungsbehörden.
  - **Risikoberichterstattung:** Regelmässige Berichterstattung über den Status der Risikobehandlung und die Fortschritte bei der Implementierung von Massnahmen.
  - **Risikokultur:** Die Schaffung einer Unternehmenskultur, in der Risikomanagement eine wichtige Rolle spielt und in der Mitarbeitende die Bedeutung der Risikominimierung und -kontrolle verstehen.
  - **Überwachung und Bewertung:** Laufende Überwachung der Risikolandschaft und Bewertung der Wirksamkeit der Risikomanagementstrategien.
- (2) Das Risikomanagement ist in Unternehmen und Organisationseinheiten aller Grössen und Branchen von entscheidender Bedeutung, da es dazu beiträgt, finanzielle Verluste zu minimieren, den Geschäftsbetrieb aufrechtzuerhalten und die langfristige Stabilität und Nachhaltigkeit zu gewährleisten. Es ist ein kontinuierlicher Prozess, der sich an die sich ändernden Risiken und Bedingungen anpassen muss, um sicherzustellen, dass die Organisation erfolgreich mit Unsicherheiten umgehen kann.



**Als Betreiber von kritischen Infrastrukturen muss die Risikoidentifikation und -beurteilung nicht nur aus Sicht sicherer Geschäftsführung durchgeführt werden, sondern auch aus Sicht kritischer Infrastruktur und deren Auswirkungen auf die schweizerische Gesellschaft.**



#### Hinweise auf weiterführende und ergänzende Dokumente:

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

### 4.4.3 Business Continuity Management (BCM)

- (1) Das Business Continuity Management (BCM) ist ein umfassender Ansatz zur Planung und Vorbereitung auf Störungen, Krisen und Katastrophen, um die Geschäftskontinuität und die Widerstandsfähigkeit einer Organisation sicherzustellen. Im Zusammenhang mit der Steigerung der IKT-Resilienz spielt das BCM eine entscheidende Rolle, da Informations- und Kommunikationstechnologie (IKT) oft das Rückgrat moderner Geschäftsprozesse darstellt. Das BCM und die IKT-Resilienz sind eng miteinander verknüpft, und die Integration von IKT-Resilienz in das BCM ist von grosser Bedeutung. Hier sind einige wichtige Aspekte des BCM im Zusammenhang mit der IKT-Resilienz:
- **Risikobewertung und Identifikation:** Das BCM beginnt mit der Identifikation und Bewertung von Risiken, die die IKT-Infrastruktur und -Systeme einer Organisation gefährden könnten. Dies umfasst Bedrohungen wie Cyberangriffe, Naturkatastrophen, technische Ausfälle und menschliche Fehler.
  - **Business Impact Analysis (BIA):** Im Rahmen des BCM wird eine Business Impact Analysis durchgeführt, um die Auswirkungen von Störungen auf die Geschäftsprozesse zu verstehen. Dies beinhaltet die Identifizierung kritischer IKT-Systeme und -Anwendungen, deren Ausfall zu erheblichen Geschäftsbeeinträchtigungen führen könnte.
  - **Notfall- und Wiederherstellungsplänen:** Basierend auf der Risikobewertung und der BIA entwickelt die Organisation Notfall- und Wiederherstellungspläne für ihre IKT-Systeme. Diese Pläne enthalten Schritte und Verfahren zur Aufrechterhaltung der Geschäftskontinuität und zur Wiederherstellung der IKT-Systeme im Falle einer Störung.
  - **Testen und Üben:** Das BCM umfasst regelmässige Tests und Übungen, um sicherzustellen, dass die Notfall- und Wiederherstellungspläne effektiv sind. Dies schliesst Testläufe für die Wiederherstellung von IKT-Systemen und Simulationen von Notfall- und Krisenszenarien ein.



- **Schulung und Sensibilisierung:** Mitarbeiter und IT-Personal werden für ihre Rolle im BCM und in der Wiederherstellung von IKT-Systemen geschult, um sicherzustellen, dass sie im Ernstfall angemessen reagieren können.
  - **Incident Response:** Das BCM umfasst klare Verfahren zur Incident Response, die festlegen, wie auf Sicherheitsvorfälle und Störungen der IKT-Systeme reagiert wird.
  - **Überwachung und Anpassung:** Das BCM erfordert eine kontinuierliche Überwachung der IKT-Resilienzmassnahmen und eine Anpassung an neue Bedrohungen, Technologien und Geschäftsanforderungen.
  - **Integration von IKT-Resilienz:** Das BCM und die IKT-Resilienz müssen nahtlos miteinander integriert sein. Dies bedeutet, dass die Sicherheit und Widerstandsfähigkeit der IKT-Systeme in den gesamten BCM-Prozess einbezogen werden.
- (2) Die Integration von IKT-Resilienz in das BCM ist von entscheidender Bedeutung, da IKT in vielen Unternehmen und Organisationseinheiten eine zentrale Rolle spielt. Ein Ausfall oder eine Störung der IKT-Systeme kann erhebliche Auswirkungen auf die Geschäftskontinuität und die Fähigkeit zur Erbringung von Dienstleistungen haben. Durch die Berücksichtigung von IKT-Resilienz im BCM können Unternehmen und Organisationseinheiten sicherstellen, dass sie effektiv auf IKT-bezogene Risiken reagieren können und ihre Widerstandsfähigkeit bei Störungen erhöhen.



#### Hinweise auf weiterführende und ergänzende Dokumente:

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

#### 4.4.3.1 Business Impact Analyse (BIA)

- (1) Die Business Impact Analysis (BIA) ist ein wichtiger Schritt bei der Steigerung der IKT-Resilienz im Rahmen eines umfassenden Risikomanagements. Die BIA ist ein Prozess, bei dem Unternehmen und Organisationseinheiten die potentiellen Auswirkungen von IKT-Störungen und -ausfällen auf ihre Geschäftsprozesse und -funktionen analysieren und bewerten. Sie hilft dabei, die kritischen IKT-Komponenten und -Anwendungen zu identifizieren und festzustellen, wie Störungen in diesen Bereichen die Geschäftskontinuität beeinträchtigen könnten. Im Zusammenhang mit der Steigerung der IKT-Resilienz spielt die BIA eine zentrale Rolle:
- **Identifikation kritischer IKT-Komponenten:** Die BIA unterstützt bei der Identifikation der IKT-Systeme, Anwendungen und Infrastruktur, die für den reibungslosen Betrieb der Geschäftsprozesse und die Erbringung von Dienstleistungen von entscheidender Bedeutung sind. Dies umfasst zum Beispiel die kritischen Datenbanken, Kommunikationssysteme, E-Commerce-Plattformen oder spezielle Softwareanwendungen.
  - **Bewertung der Auswirkungen:** Die BIA bewertet die potentiellen Auswirkungen von IKT-Störungen auf die Geschäftsprozesse und -funktionen. Dies kann finanzielle Auswirkungen, den Verlust von Kunden, rechtliche Konsequenzen, Reputationsschäden und mehr umfassen.
  - **Priorisierung der Wiederherstellung:** Die BIA hilft bei der Priorisierung der IKT-Systeme und Anwendungen, die zuerst wiederhergestellt werden müssen, um die Geschäftskontinuität sicherzustellen. Dies ermöglicht eine gezielte Zuweisung von Ressourcen und Zeitplänen für die Wiederherstellung.
  - **Notfall- und Wiederherstellungsplanung:** Die Ergebnisse der BIA fliessen in die Notfall- und Wiederherstellungspläne ein. Sie bieten klare Anweisungen und Verfahren zur Wiederherstellung der kritischen IKT-Systeme und Anwendungen, um die Auswirkungen von Störungen zu minimieren.
  - **Risikobewertung und Verbesserung:** Die BIA hilft bei der Identifikation von Schwachstellen und Risiken in den IKT-Systemen und ermöglicht die Implementierung von Massnahmen zur Verbesserung der IKT-Resilienz. Dies kann die Implementierung von Sicherheitsmassnahmen, die Aktualisierung von Systemen und die Einführung redundanter Systeme umfassen.
  - **Schulung und Sensibilisierung:** Die Ergebnisse der BIA können dazu beitragen, Schulungs- und Sensibilisierungsprogramme für Mitarbeiter zu entwickeln, um sicherzustellen, dass sie die Bedeutung der IKT-Resilienz verstehen und wissen, wie sie sich im Notfall verhalten sollen.



- (2) Die BIA ist ein entscheidendes Werkzeug, um sicherzustellen, dass IKT-Resilienzmassnahmen gezielt und effektiv sind. Durch die Identifizierung kritischer IKT-Komponenten und die Bewertung ihrer Auswirkungen auf die Geschäftsprozesse können Unternehmen und Organisationseinheiten gezielt in Massnahmen investieren, die die Widerstandsfähigkeit gegenüber IKT-Störungen erhöhen. Dies trägt dazu bei, Geschäftskontinuität sicherzustellen und die Organisation besser auf die Bewältigung von IKT-bezogenen Risiken vorzubereiten.



#### Hinweise auf weiterführende und ergänzende Dokumente:

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

#### 4.4.4 Notfallmanagement

- (1) Das Notfallmanagement spielt eine entscheidende Rolle bei der Steigerung der Resilienz der Informations- und Kommunikationstechnologie (IKT). Es bezeichnet den strukturierten Prozess, mit dem Unternehmen und Organisationseinheiten auf unvorhergesehene Ereignisse oder Störungen reagieren, diese bewältigen und sich anschliessend erholen. Im Kontext der IKT zielt ein effektives Notfallmanagement darauf ab, die Auswirkungen von Störungen zu minimieren und sicherzustellen, dass die IKT-Systeme auch unter widrigen Umständen optimal funktionieren.
- (2) Zu Beginn steht die Entwicklung eines klaren Notfallmanagementplans, der die Struktur, Zuständigkeiten und Handlungsabläufe definiert. Dieser Plan sollte speziell auf die IKT-Infrastruktur zugeschnitten sein und verschiedene Szenarien berücksichtigen, darunter Cyberangriffe, Naturkatastrophen, technische Ausfälle oder andere sicherheitsrelevante Vorfälle.
- (3) Eine umfassende Risikobewertung bildet die Grundlage für den Notfallmanagementplan. Hierbei werden potentielle Bedrohungen für die IKT identifiziert und ihre Auswirkungen auf die Geschäftskontinuität bewertet. Diese Analyse ermöglicht es, gezielte Massnahmen zu entwickeln, um die Resilienz der IKT gegenüber den identifizierten Risiken zu stärken.
- (4) Während einer Krise ist eine klare Kommunikation entscheidend. Der Notfallmanagementplan sollte klare Richtlinien für die interne und externe Kommunikation festlegen, sowohl innerhalb der Organisation als auch mit relevanten Stakeholdern. Dies trägt dazu bei, Unsicherheiten zu minimieren und die Effektivität der Reaktion zu optimieren.
- (5) Ein weiterer wichtiger Aspekt des Notfallmanagements ist die Einrichtung von Notfallreaktions-Teams, die speziell darauf ausgerichtet sind, Störungen in der IKT zu bewältigen. Diese Teams sollten nicht nur über technisches Know-how verfügen, sondern auch in der Lage sein, effektiv zusammenzuarbeiten und unter Druck fundierte Entscheidungen zu treffen.
- (6) Regelmässige Schulungen und Simulationen sind entscheidend, um sicherzustellen, dass das Notfallmanagementteam gut vorbereitet ist. Durch das Durchspielen verschiedener Szenarien können Schwachstellen im Plan identifiziert und Verbesserungen vorgenommen werden.
- (7) Die Nachbereitung eines Notfalles ist genauso wichtig wie die unmittelbare Reaktion. Eine umfassende Analyse der getroffenen Massnahmen, der Wirksamkeit des Notfallmanagements und der erzielten Lerneffekte führt zu kontinuierlichen Verbesserungen für zukünftige Ereignisse.
- (8) Insgesamt trägt ein gut durchdachtes Notfallmanagement erheblich zur Steigerung der IKT-Resilienz bei. Es ermöglicht nicht nur eine effektive Bewältigung von Störungen, sondern fördert auch die Fähigkeit, sich von Notfällen zu erholen und gestärkt aus ihnen hervorzugehen.



#### Hinweise auf weiterführende und ergänzende Dokumente:

- NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems"
- BSI-Standard 100-4 Notfallmanagement

#### 4.5 Cyber-Security-Strategie nach Defense in Depth

- (1) Die Cybersecurity-Strategie "Defense in Depth" (deutsch: Verteidigung in der Tiefe) ist ein Ansatz, der darauf abzielt, ein umfassendes und mehrschichtiges Verteidigungssystem zu schaffen, um IKT-Systeme und -Daten vor Cyberbedrohungen zu schützen. Diese Strategie geht davon aus, dass keine einzelne Sicherheitsmassnahme ausreicht, um alle potenziellen Bedrohungen abzuwehren. Stattdessen werden mehrere Schutzebenen implementiert, um einen umfassenden Schutz zu gewährleisten.



- (2) Hier sind die Hauptkomponenten und Prinzipien der Defense-in-Depth-Cybersecurity-Strategie zur Steigerung der IKT-Resilienz:
- **Prävention:** Die erste Schicht der Verteidigung konzentriert sich auf die Verhinderung von Angriffen. Dies umfasst Sicherheitsmassnahmen wie Firewalls, Intrusion Detection/Prevention Systeme (IDS/IPS), Antivirus-Software und sichere Konfigurationen von Netzwerken und Endgeräten.
  - **Erkennung:** Wenn präventive Massnahmen scheitern, ist die Erkennung von Sicherheitsvorfällen von entscheidender Bedeutung. Dies beinhaltet die Implementierung von Sicherheitsüberwachungssystemen, Protokollierung und Security Information and Event Management (SIEM)-Tools, um verdächtige Aktivitäten zu identifizieren.
  - **Reaktion:** Im Falle einer Sicherheitsverletzung oder eines Vorfalls ist eine schnelle Reaktion entscheidend. Dies schliesst die Einrichtung von Notfallplänen und die Schulung von Incident-Response-Teams ein, um angemessen auf Vorfälle zu reagieren, sie zu isolieren und zu beseitigen.
  - **Authentifizierung und Zugriffskontrolle:** Zugriff auf Systeme und Daten sollte nur autorisierten Benutzern gestattet werden. Dies wird durch die Implementierung von starken Authentifizierungsmethoden wie Zwei-Faktor-Authentifizierung (2FA) und die Verwendung von Berechtigungen und Zugriffssteuerungslisten erreicht.
  - **Netzwerksicherheit:** Schichtenbasierte Sicherheitsansätze wie Netzwerksegmentierung, VLANs und Sicherheitszonen helfen dabei, das Netzwerk vor seitlichen Bewegungen von Angreifern zu schützen.
  - **Endgerätesicherheit:** Das Sichern von Endgeräten wie Computer, Smartphones und IoT-Geräten ist ein wesentlicher Bestandteil der Defense-in-Depth-Strategie. Dies umfasst regelmässige Software-Updates, Sicherheitsrichtlinien und Endpunktschutzlösungen.
  - **Verschlüsselung:** Datenverschlüsselung schützt Informationen sowohl während der Übertragung als auch im Ruhezustand. Dies ist entscheidend, um Daten vor unbefugtem Zugriff zu schützen.
  - **Schulung und Sensibilisierung:** Eine gut informierte Belegschaft ist ein wichtiger Faktor für die Sicherheit. Schulungen und Sensibilisierungskampagnen können Mitarbeiter dazu ermutigen, sicherheitsbewusst zu handeln und Phishing-Angriffe zu erkennen.
  - **Patch-Management:** Die regelmässige Aktualisierung von Software und Betriebssystemen, um bekannte Sicherheitslücken zu schliessen, ist ein wesentlicher Schutzmechanismus.
  - **Überwachung und Prüfung:** Die laufende Überwachung und regelmässige Sicherheitsaudits und Penetrationstests helfen dabei, Sicherheitslücken zu identifizieren und zu beheben.
- (3) Die Defense-in-Depth-Strategie ist flexibel und kann an die spezifischen Anforderungen und Risiken einer Organisation angepasst werden. Sie betont die Wichtigkeit, dass keine Sicherheitsmassnahme allein ausreicht, um die immer komplexer werdenden Cyberbedrohungen wirksam zu bekämpfen. Statt dessen setzt sie auf eine Kombination aus Schutzschichten, um ein höheres Mass an Sicherheit zu gewährleisten.



#### Hinweise auf weiterführende und ergänzende Dokumente:

- VSE Grundsatz OT in der Stromversorgung
- NIST SP 800-82
- BSI ICS-Security-Kompodium



In diesem Leitfaden wird nicht weiter auf die Cyber-Security-Strategie nach Defense in Depth eingegangen. Es finden sich genügend Erklärungen und Hinweise in anderen Dokumenten.

## 5. Grundlagen zur Steigerung der IKT-Resilienz



In diesem Kapitel werden die Grundlagen zur Steigerung der IKT-Resilienz von den VSE Cyber Security Task Force Experten aufgezeigt.

### 5.1 Grundsätzliches Verständnis zur Vorgehensweise

- (1) Oftmals besteht das Missverständnis, dass Vorgaben, Vorschriften, Normen, Standards, Frameworks usw. eine Anleitung bzw. die Lösung zur Umsetzung von Massnahmen für die Steigerung der IKT-





Resilienz beschreiben. Dies ist aber in den meisten Fällen nicht so. Oftmals werden nur Kontrollen und Checkpoints beschrieben, welche in den einzelnen Bereichen und Punkten zur Steigerung der IKT-Resilienz betrachtet bzw. berücksichtigt werden müssen. Die eigentliche Lösungsfindungen bzw. effektive Massnahmen zur Ausführung muss von jedem Unternehmen und jeder Organisationseinheit selbständig analysiert, entwickelt und umgesetzt werden.

- (2) Diese beinhalten oftmals Anleitungen und Anwendungsbeispiele, welche die Unternehmen und Organisationseinheiten bei der Lösungsfindung und Umsetzung unterstützen. Dabei handelt es sich meistens um spezifische Praxisbeispiele, welche u.U. bei den jeweiligen Unternehmen und Organisationseinheiten in der Regel nicht 1:1 umgesetzt werden können.



**Vorgaben, Vorschriften, Normen und Standards, Frameworks usw. sind keine Anleitungen und enthalten keine Anwendungsbeispiele welche 1:1 umgesetzt werden können. Sie enthalten nur Kontrollen, Checkpoints und Beschreibungen von möglichen Massnahmen, welche umgesetzt werden sollen. Jedes Unternehmen und jeder Organisationseinheit ist für die Lösungsfindung zur Umsetzung der Kontrollen und Massnahmen selbst zuständig. Anwendungsbeispiele aus den oben erwähnten Dokumenten, können jedoch bei der Lösungsfindung behilflich sein.**

## 5.2 Komplexität und Umfang der Informationssicherheit zur Steigerung der IKT-Resilienz

- (1) Die Komplexität und der Umfang der Informationssicherheit im Kontext mit der Steigerung der IKT-Resilienz sind äusserst anspruchsvoll und weitreichend. Informationssicherheit erstreckt sich über eine breite Palette von Dimensionen, die sowohl technische als auch organisatorische Aspekte umfassen.
- (2) In technischer Hinsicht beinhaltet die Sicherung der IKT-Infrastruktur den Schutz von Netzwerken, Systemen, Anwendungen und Daten vor unbefugtem Zugriff, Manipulation oder Ausfall. Dies erfordert fortgeschrittene Sicherheitsmassnahmen wie Firewalls, Intrusion Detection Systeme, Verschlüsselung und regelmässige Sicherheitsaktualisierungen, um mit sich ständig weiterentwickelnden Bedrohungen Schritt halten zu können.
- (3) Die Komplexität steigt weiter mit der Diversität der Technologien und Plattformen, die in modernen Unternehmen und Organisationseinheiten eingesetzt werden, weiter an. Cloud Computing, mobile Geräte, Internet of Things (IoT) und vernetzte Systeme erweitern den Angriffsvektor erheblich und erfordern eine umfassende Sicherheitsstrategie.
- (4) Auf der organisatorischen Ebene müssen klare Sicherheitsrichtlinien und -prozeduren entwickelt und implementiert werden. Die Sensibilisierung und Schulung aller Mitarbeiter bezüglich sicherheitsrelevanter Praktiken sind entscheidend, da der menschliche Faktor oft eine reale Schwachstelle darstellt.
- (5) Das Management von Identitäten und Zugriffsberechtigungen ist eine weitere komplexe Herausforderung. Sicherzustellen, dass nur autorisierte Personen auf sensible Informationen zugreifen können, erfordert fortschrittliche Authentifizierungs- und Autorisierungssysteme und Prozesse.
- (6) Ein entscheidender Aspekt ist die Fähigkeit zur Erkennung und Reaktion auf Sicherheitsvorfälle in Echtzeit. Dies erfordert leistungsfähige Security Information and Event Management (SIEM)-Systeme, die Unregelmässigkeiten oder Anomalien frühzeitig erkennen können.
- (7) Die ständige Anpassung an neue Bedrohungen und Technologien macht den Umfang der Informationssicherheit dynamisch. Es erfordert regelmässige Risikobewertungen, Sicherheitsaudits und eine kontinuierliche Verbesserung der Sicherheitsmassnahmen.
- (8) Zusammenfassend ist die Informationssicherheit im Rahmen der Steigerung der IKT-Resilienz ein hochkomplexes Unterfangen, das nicht nur technische Schutzmassnahmen umfasst, sondern auch den Aufbau einer unternehmensweiten Sicherheitskultur, Durchführung von Schulungen sowie die Einführung von organisatorischen Prozessen erfordert. Eine umfassende Sicherheitsstrategie ist unerlässlich, um die Resilienz der Informations- und Kommunikationstechnologie gegenüber vielfältigen Bedrohungen zu gewährleisten.



**Die Komplexität und Umfang der Informationssicherheit zur Steigerung der IKT-Resilienz darf nicht unterschätzt werden.**

## 5.3 Aufwand für die Informationssicherheit zur Steigerung der IKT-Resilienz

- (1) Der Aufwand für die Informationssicherheit im Rahmen der Steigerung der IKT-Resilienz ist beträchtlich und umfasst eine Vielzahl von Aspekten. Beginnend mit technologischen Investitionen erfordert die



Implementierung von robusten Sicherheitsmassnahmen einen erheblichen finanziellen Aufwand. Dies schliesst den Erwerb und die Aktualisierung von Sicherheitssoftware, die Implementierung von Firewalls, Intrusion Detection Systemen, Verschlüsselungstechnologien und anderen Sicherheitsinfrastrukturen ein.

- (2) Die Schulung und Sensibilisierung der Mitarbeiter sind weiterer wesentlicher Bestandteil. Die Entwicklung des Sicherheitsbewusstseins erfordert regelmässige Schulungen, um die Mitarbeiter über aktuelle Bedrohungen, Best Practices und Sicherheitsrichtlinien auf dem aktuellen Wissensstand zu halten. Dieser Prozess erfordert nicht nur finanzielle Mittel, sondern auch Zeit und Ressourcen.
- (3) Die Erstellung und Umsetzung klarer Sicherheitsrichtlinien und -verfahren erfordern eine intensive Beteiligung des Unternehmensmanagements. Die Entwicklung, Aktualisierung und Überwachung dieser Richtlinien bedeuten einen beträchtlichen Verwaltungsaufwand, um sicherzustellen, dass sie den aktuellen Bedrohungen und regulatorischen Anforderungen entsprechen.
- (4) Der technologische Fortschritt und die kontinuierliche Evolution der Bedrohungslandschaft bedeuten, dass ein erheblicher Aufwand für Forschung und Entwicklung erforderlich ist. Unternehmen und Organisationseinheiten müssen sich ständig über neue Sicherheitsbedrohungen und Gegenmassnahmen auf dem Laufenden halten, um ihre Sicherheitsinfrastruktur effektiv zu gestalten.
- (5) Der Einsatz von Security Operation Center (SOC)-Teams, die rund um die Uhr auf Sicherheitsvorfälle reagieren, ist eine weitere Investition, die Unternehmen und Organisationseinheiten tätigen müssen, um die Erkennung und Reaktion auf mögliche Angriffe rund um die Uhr sicherstellen zu können.
- (6) Die kontinuierliche Verbesserung der Informationssicherheit bedeutet einen dauerhaften Aufwand. Dies umfasst regelmässige Sicherheitsaudits, Risikobewertungen und Anpassungen von Sicherheitsmassnahmen entsprechend den sich ändernden Bedrohungen und Geschäftsanforderungen.
- (7) Der Aufwand für die Informationssicherheit zur Steigerung der IKT-Resilienz wird oft unterschätzt, weil die Komplexität und die vielschichtigen Anforderungen dieser Aufgabe nicht immer sofort ersichtlich sind. Ein Grund dafür liegt in der rasanten Entwicklung der Technologie und der sich ständig verändernden Bedrohungslandschaft. Unternehmen und Organisationseinheiten müssen nicht nur mit den neuesten Technologien Schritt halten, sondern auch proaktiv auf neue Bedrohungen reagieren können.
- (8) Die Integration von Informationssicherheit in die Unternehmenskultur erfordert einen kulturellen Wandel, der Zeit und Anstrengungen erfordert. Dieser Aspekt wird oft nicht ausreichend berücksichtigt, wenn der Aufwand für Informationssicherheit betrachtet wird.
- (9) Zusammengefasst wird der Aufwand für Informationssicherheit zur Steigerung der IKT-Resilienz unterschätzt, weil die Herausforderungen in der Breite und Tiefe des Themas liegen. Es erfordert nicht nur finanzielle Investitionen und zusätzliche Ressourcen, sondern auch eine strategische Ausrichtung, kontinuierliche Anpassung und die Integration von Sicherheit in die gesamte Organisation.



**Der Aufwand für die Informationssicherheit zur Steigerung der IKT-Resilienz ist beträchtlich und darf auf keinen Fall unterschätzt werden.**



## 5.4 Grundlagen einer erfolgreichen Steigerung der IKT-Resilienz

### 5.4.1 Notwendige Elemente einer erfolgreichen Steigerung der IKT-Resilienz

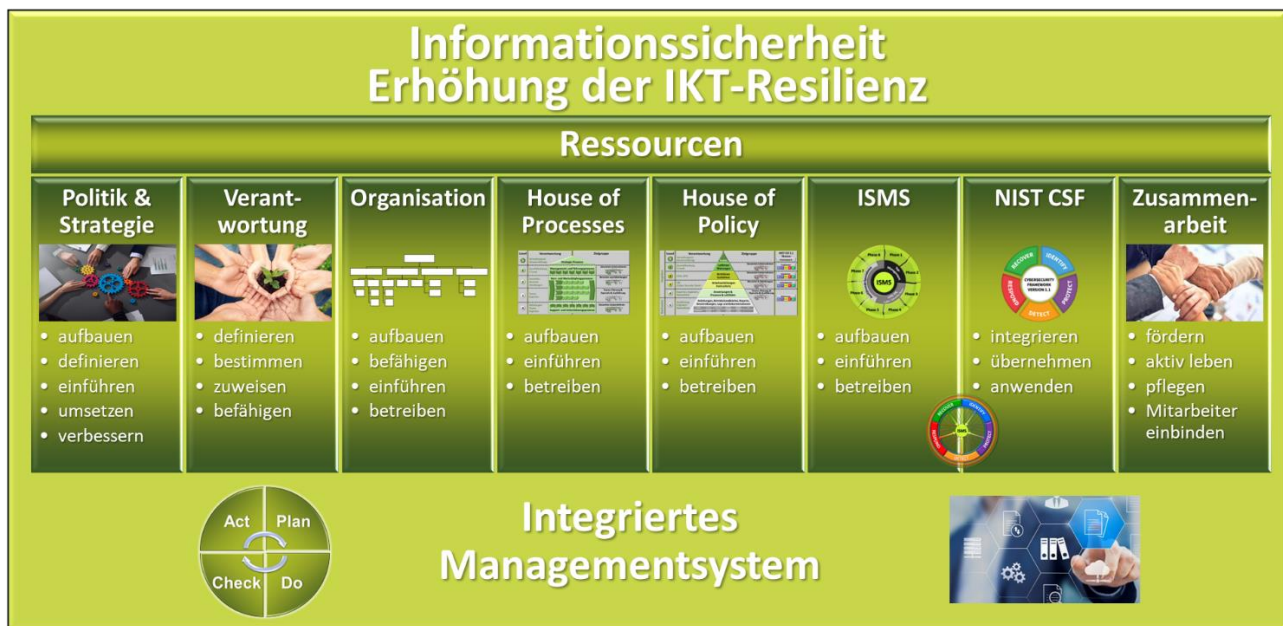


Abbildung 9: Die notwendigen Elemente für eine erfolgreiche Steigerung der IKT-Resilienz (Quelle VSE)

- (1) Die integralen Elemente für eine erfolgreiche Steigerung der IKT-Resilienz müssen ganzheitlich in Angriff genommen werden. Sie spielen in sich zusammen und haben deshalb keine klare Abgrenzung zueinander. Je nach Unternehmen und Organisationseinheiten können spezifische Bereiche auch von externen Dienstleistern ausgeführt werden. Die gesamte, Planung, Einführung, Umsetzung und der anschließende Betrieb des Informationssicherheitsmanagement (ISM) soll nach dem PDCA-Zyklus (Plan, Do, Check, Act) erfolgen.

### 5.4.2 Ausreichende Ressourcen zur Steigerung der IKT-Resilienz

- (1) Ausreichend Ressourcen für Informationssicherheit zur Steigerung der IKT-Resilienz bereitzustellen, ist entscheidend. Es ist eine anspruchsvolle Aufgabe, die häufig unterschätzt wird. Wichtig zu beachten ist, dass die begrenzten Ressourcen nicht nur für technische, sondern auch für organisatorische Massnahmen eingesetzt werden.
- (2) Die Notwendigkeit kontinuierlicher Investitionen wird oft unterschätzt. Die Dynamik der Bedrohungslandschaft erfordert regelmässige Aktualisierungen der Sicherheitsinfrastruktur, um mit neuen Angriffsmethoden Schritt zu halten. Dies erfordert nicht nur finanzielle Ressourcen, sondern auch eine ständige Bereitschaft zur Anpassung.
- (3) Die Implementierung und Überwachung von Sicherheitsrichtlinien erfordern nicht nur finanzielle Mittel, sondern auch zeitliche Ressourcen. Es ist wichtig sicherzustellen, dass die Vorgaben nicht nur existieren, sondern auch effektiv kommuniziert, geschult und eingehalten werden. Dies benötigen einen organisatorischen Aufwand und eine kontinuierliche Überwachung.
- (4) Die Integration von Informationssicherheit in die Unternehmenskultur ist ein langfristiger Prozess, der auch ein Engagement auf Führungsebene erfordert. Dieser kulturelle Wandel ist entscheidend, um sicherzustellen, dass Sicherheit nicht nur als eine isolierte Aufgabe der IT/OT-Abteilungen betrachtet wird, sondern als zentrales Element jeder Organisation wahrgenommen wird.
- (5) Insgesamt wird die Bedeutung ausreichender Ressourcen für Informationssicherheit oft erst dann vollständig erkannt, wenn Sicherheitsvorfälle auftreten. Eine umfassende Strategie erfordert eine angemessene Investition in Technologien, Schulungen, Richtlinien und kulturellen Wandel, um die Resilienz der IKT-Infrastruktur zu stärken und auf die ständig wachsenden Bedrohungen vorbereitet zu sein.



**Der Aufwand für die Informationssicherheit zur Steigerung der IKT-Resilienz ist beträchtlich und darf auf keinen Fall unterschätzt werden.**



### 5.4.3 Integriertes Managementsystem (IMS)



Abbildung 10: IMS (Quelle TÜV NORD)

- (1) Das Integrierte Managementsystem (IMS) spielt eine entscheidende Rolle bei der Steigerung der IKT-Resilienz, indem es eine umfassende und koordinierte Herangehensweise an verschiedene Aspekte des Managements ermöglicht. Die Bedeutung des IMS liegt darin, dass es verschiedene Managementstandards und -systeme in einer einzigen Struktur integriert, darunter Qualitätsmanagement, Umweltmanagement oder Informationssicherheitsmanagement.
- (2) Durch die Integration verschiedener Managementsysteme wird eine effizientere Nutzung von Ressourcen ermöglicht, da gemeinsame Prozesse und Verfahren eingeführt werden können. Dies führt zu einer konsistenten und koordinierten Umsetzung von Massnahmen zur Steigerung der IKT-Resilienz. Das IMS hilft dabei, Redundanzen zu vermeiden und Synergien zwischen den verschiedenen Managementsystemen zu nutzen.
- (3) Der Nutzen des IMS für die Steigerung der IKT-Resilienz liegt in der ganzheitlichen Betrachtung von Risiken und Chancen. Durch die Integration von Qualitäts-, Umwelt- und Informationssicherheitsaspekten können Unternehmen und Organisationseinheiten ihre Prozesse so gestalten, dass sie nicht nur den Schutz der Informationstechnologie gewährleisten, sondern auch effektive Abläufe und hohe Qualitätsstandards aufrechterhalten.
- (4) Ein weiterer Vorteil des IMS liegt in der Optimierung von Audits und Überwachungen. Da verschiedene Standards und Normen miteinander verknüpft sind, können Audits effizienter durchgeführt werden, was zu einer ressourcenschonenden Überwachung führt. Dies ermöglicht eine ganzheitliche Bewertung der Leistung und Einhaltung der verschiedenen Aspekte des Managements.
- (5) Die kohärente Struktur des IMS trägt dazu bei, dass Unternehmen und Organisationseinheiten flexibler auf sich ändernde Bedingungen reagieren können. Dies ist entscheidend um in einer sich ständig weiterentwickelnden IKT-Landschaft, schnell auf neue Herausforderungen und Anforderungen zu reagieren.
- (6) Insgesamt fördert das Integrierte Managementsystem eine systematische und effektive Vorgehensweise zur Steigerung der IKT-Resilienz. Durch die Verknüpfung von Qualitätsmanagement, Umweltmanagement und Informationssicherheitsmanagement werden nicht nur Sicherheitsaspekte gestärkt, sondern auch die Gesamtleistung und Nachhaltigkeit einer Organisation verbessert.



In diesem Leitfaden wird nicht explizit auf ein Integriertes Managementsystem eingegangen. Die Methodiken, Grundsätze und Elemente werden aber als Basis verwendet.



**Empfehlung der VSE Cyber Security Task Force Experten:**  
Integrierte Managementsysteme (IMS) sollten von den Unternehmen und Organisationseinheiten eingeführt und angewendet werden.



#### 5.4.4 Steigerung der IKT-Resilienz nach dem Deming-Zyklus

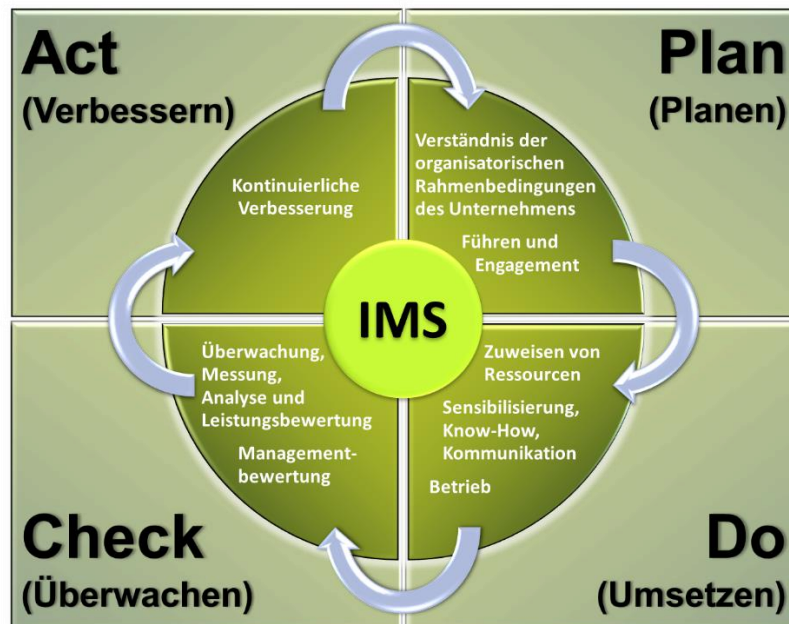


Abbildung 11: PDCA Deming-Zyklus (Quelle VSE)

- (1) Der Deming-Zyklus, auch als PDCA-Zyklus bezeichnet, ist ein bewährtes Qualitätsmanagement- und kontinuierlicher Verbesserungsprozess. Der PDCA-Zyklus besteht aus vier wiederkehrenden Phasen:
  - **1. Planen (Plan):** In dieser Phase werden die Ziele und Prozesse identifiziert und geplant. Dies beinhaltet das Festlegen von klaren Zielen, die Identifizierung von Problemen oder Schwachstellen, die Analyse von Daten und Informationen sowie die Festlegung von Massnahmen und Einplanung von Ressourcen, die benötigt werden, um die Ziele zu erreichen.
  - **2. Umsetzen (Do):** Nachdem die Planungsphase abgeschlossen ist, erfolgt die Umsetzung der geplanten Massnahmen. Dies kann die Einführung neuer Prozesse, Schulungen von Mitarbeitern oder auch Änderungen an bestehenden Arbeitsabläufen umfassen. In dieser Phase wird die Planung in die Praxis umgesetzt.
  - **3. Überprüfen (Check):** In dieser Phase werden die Ergebnisse und Fortschritte überprüft. Es werden Daten gesammelt und analysiert, um sicherzustellen, dass die Massnahmen wie angedacht funktionieren. Die Überprüfung hilft, Probleme oder Abweichungen von den Zielen zu identifizieren und gibt Hinweise darauf, ob weitere Anpassungen notwendig sind.
  - **4. Handeln (Act):** Basierend auf den Ergebnissen der Überprüfung wird in dieser Phase gehandelt. Wenn Probleme oder Abweichungen festgestellt wurden, werden entsprechende Massnahmen ergriffen, um diese zu beheben. Dies kann bedeuten, dass die Planung angepasst, neue Massnahmen ergriffen oder Prozesse weiter optimiert werden, um die Qualität und Effizienz zu steigern.
- (2) Nachdem die "Handeln"-Phase abgeschlossen ist, beginnt der Zyklus von vorne. Dieser Prozess der Planung, Umsetzung, Überprüfung und Handlung trägt dazu bei, kontinuierliche Verbesserungen in einem Unternehmen und in den Organisationseinheiten zu erzielen. Der PDCA-Zyklus ist ein wichtiger Bestandteil des Total Quality Management (TQM) und hat sich als effektive Methode zur Steigerung der Qualität, Effizienz und Wettbewerbsfähigkeit bewährt.



#### Empfehlung der VSE Cyber Security Task Force Experten:

Der PDCA- oder auch Deming-Zyklus ist ein kontinuierlicher Verbesserungsprozess und muss für die Steigerung der IKT-Resilienz in den verschiedenen Bereichen angewendet werden.





## 5.4.5 Informationssicherheit: Politik und Strategie

### 5.4.5.1 Informationssicherheitspolitik (ISP)

- (1) Eine umfassende Informationssicherheitspolitik (ISP) ist ein zentrales Dokument in jeder Organisation, dass die grundlegenden Prinzipien und Verfahren zur Gewährleistung der Sicherheit von Informationen und Daten innerhalb der Organisation festlegt. Eine ISP ist entscheidend, um sicherzustellen, dass vertrauliche und kritische Informationen angemessen geschützt sind. Nachfolgend sind die Schlüsselkomponenten einer umfassenden Informationssicherheitspolitik aufgeführt:
- **Ziel und Zweck:** Die ISP sollte das übergeordnete, strategische Ziel und den Zweck der Informationssicherheit in der Organisation erläutern. Dies kann den Schutz von Informationen, den Datenschutz, die Geschäftskontinuität und die Einhaltung gesetzlicher Vorschriften umfassen.
  - **Geltungsbereich:** Die ISP sollte klar angeben, auf welche Bereiche, Systeme und Daten sie anwendbar ist. Dies schliesst auch externe Partner und Dienstleister ein, die mit den Informationen des Unternehmens und der Organisationseinheiten in Berührung kommen.
  - **Grundsätze und Werte:** Die ISP sollte eine klare Erklärung der Grundsätze und Werte enthalten, die die Organisation in Bezug auf Informationssicherheit fördert. Dies kann Ethik, Integrität, Vertraulichkeit, Verfügbarkeit und Resilienz einschliessen.
  - **Verantwortlichkeiten:** Die ISP sollte die Rollen und Verantwortlichkeiten für die Umsetzung der Informationssicherheitsrichtlinien und -verfahren innerhalb der Organisation definieren. Dies kann die Benennung eines Chief Information Security Officers (CISO) oder eines Informationssicherheitsbeauftragten (ISB) einschliessen.
  - **Risikomanagement:** Die ISP sollte den Ansatz der Organisation für das Risikomanagement im Zusammenhang mit der Informationssicherheit beschreiben. Dies umfasst die Identifizierung, Bewertung und Behandlung von Sicherheitsrisiken.
  - **Schutz von Informationen:** Die ISP sollte klare Anweisungen zur Sicherung von Informationen enthalten. Dies umfasst den Zugriff, die Verschlüsselung, die Sicherung, die Wiederherstellung, die sichere Aufbewahrung und Entsorgung von Dokumenten und Informationen.
  - **Meldung von Sicherheitsvorfällen:** Die Politik sollte die Verfahren und Fristen für die Meldung von Sicherheitsvorfällen und Datenschutzverletzungen festlegen, um eine schnelle Reaktion und Untersuchung zu gewährleisten.
  - **Schulung und Sensibilisierung:** Die ISP sollte Anforderungen an die Schulung und Sensibilisierung der Mitarbeiter in Bezug auf Informationssicherheit definieren, um das Bewusstsein und die Fähigkeiten zu stärken.
  - **Compliance und Gesetze:** Die ISP sollte sicherstellen, dass die Organisation relevante gesetzliche und behördliche Anforderungen im Bereich Informationssicherheit einhält.
  - **Kontinuierliche Verbesserung:** Die ISP sollte die Bedeutung der kontinuierlichen Verbesserung der Informationssicherheitsmassnahmen unterstreichen und Mechanismen für die Überprüfung und Aktualisierung der Politik bereitstellen.
  - **Überprüfung und Genehmigung:** Die ISP sollte festlegen, wie die Politik überprüft, genehmigt und aktualisiert wird, um sicherzustellen, dass sie den sich ändernden Anforderungen und Bedrohungen entspricht.
- (2) Die ISP sollte von allen Mitarbeitern und Stakeholdern in der Organisation verstanden und befolgt werden. Sie ist ein wesentlicher Bestandteil eines umfassenden Informationssicherheitsmanagementsystems (ISMS) und dient als Grundlage für die Entwicklung und Umsetzung konkreter Sicherheitsmassnahmen und -verfahren.



#### Empfehlung der VSE Cyber Security Task Force Experten:

Jedes Unternehmen und jede Organisationseinheit muss eine für sich zutreffende Informationssicherheitspolitik (ISP) erstellen. Diese muss durch die Geschäftsleitung abgenommen, eingeführt, geschult und umgesetzt und bei Bedarf angepasst werden. Sie legt einen entscheidenden Grundstein für die Steigerung der IKT-Resilienz. Wichtig ist, dass die Informationssicherheitspolitik in der Unternehmenskultur verankert ist und gelebt wird.



#### 5.4.5.2 Informationssicherheitsstrategie (ISS)



Abbildung 12: Verantwortung (Quelle weka.ch)

(1) Eine Informationssicherheitsstrategie (ISS) ist ein strategischer Ansatz zur Sicherung von Informationen und Daten in einer Organisation. Sie legt die Grundprinzipien, Ziele und Massnahmen fest, die erforderlich sind, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten und gleichzeitig die Einhaltung gesetzlicher Vorschriften und branchenspezifischer Standards sicherzustellen. Als Basis der Informationssicherheitsstrategie dient eine Ist-Analyse der implementierten Informationssicherheit.

(2) Nachfolgend sind die Schlüsselemente einer Informationssicherheitsstrategie aufgeführt:

- **Ziele und Prioritäten:** Die ISS sollte klare und messbare Ziele für die Informationssicherheit in der Organisation definieren. Dies kann die Reduzierung von Sicherheitsvorfällen, den Schutz sensibler Daten oder die Verbesserung der Incident-Response-Fähigkeiten umfassen.
  - **Risikobewertung:** Eine umfassende Bewertung der Risiken, der das Unternehmen und die Organisationseinheiten im Hinblick auf ihre Informationen und Daten ausgesetzt sind, ist ein wesentlicher erster Schritt. Dies hilft dabei, die wichtigsten Bedrohungen und Schwachstellen zu identifizieren.
  - **Compliance:** Die Einhaltung von Gesetzen und branchenspezifischer Vorgaben müssen in der Strategie berücksichtigt werden.
  - **Informationssicherheitsrichtlinien und -verfahren:** Die Entwicklung und Implementierung von Informationssicherheitsrichtlinien und -verfahren, die Mitarbeiter und Stakeholder einhalten müssen, ist von entscheidender Bedeutung. Dies umfasst beispielsweise Zugriffsrichtlinien, Passwortsrichtlinien oder Verschlüsselungsstandards.
  - **Technische Sicherheitsmassnahmen:** Die Auswahl und Implementierung von Sicherheitstechnologien wie Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), Antivirensoftware, Verschlüsselungslösungen und Authentifizierungsmethoden sollte in die Strategie einfließen.
  - **Schulung und Sensibilisierung:** Die Sensibilisierung der Mitarbeiter für die Bedeutung der Informationssicherheit und die Schulung in Sicherheitsbewusstsein sind unerlässlich, um menschliche Fehler und erfolgreiche Social Engineering Angriffe zu verhindern.
  - **Incident Response-Plan:** Die Strategie sollte die Erstellung eines auf das Unternehmen und die Organisationseinheiten optimierten Incident-Response-Plans einschliessen, um sicherzustellen, dass effektiv auf Sicherheitsvorfälle reagieren werden kann.
  - **Überwachung und Audits:** Die kontinuierliche Überwachung der Sicherheitslage und regelmässige Sicherheitsaudits und Penetrationstests sind notwendig, um sicherzustellen, dass die Sicherheitskontrollen effektiv sind und um mögliche Schwachstellen aufzudecken.
  - **Ressourcenallokation:** Die Zuweisung von Budget, Personal und anderen Ressourcen zur Umsetzung der Informationssicherheitsstrategie ist entscheidend.
  - **Kontinuierliche Verbesserung:** Eine Informationssicherheitsstrategie sollte den Grundsatz der kontinuierlichen Verbesserung beinhalten. Dies bedeutet, dass die Strategie regelmässig überprüft und angepasst wird, um auf neue Bedrohungen und Entwicklungen in der Cybersecurity-Landschaft zu reagieren.
- (3) Eine wirksame Informationssicherheitsstrategie ist wichtig, um Datenverluste, Sicherheitsvorfälle und Reputationsverluste zu verhindern. Sie sollte eng mit den Geschäftszielen der Organisation verknüpft sein und einen ganzheitlichen Ansatz zur Sicherung von Informationen und Daten verfolgen.



#### 5.4.6 Informationssicherheit: Verantwortung



Abbildung 13: Verantwortung (Quelle: meinekrankenkasse.de)

(1) Die Definition von Verantwortlichkeiten ist in Unternehmen und Organisationseinheiten besonders im Zusammenhang mit der Steigerung der IKT-Resilienz von grosser Bedeutung aus einer Vielzahl von Gründen:

- **Klarheit und Transparenz:** Die Festlegung von Verantwortlichkeiten schafft Klarheit darüber, wer für welche Aufgaben und Aktivitäten verantwortlich ist. Dies verhindert Missverständnisse und sorgt für Transparenz in der Organisation.

- **Effizienz und Produktivität:** Durch die klare Zuweisung von Verantwortlichkeiten wird die Effizienz gesteigert, da Mitarbeiter wissen, was

von ihnen erwartet wird. Dies führt zu einer höheren Produktivität, da Zeit und Ressourcen effektiver genutzt werden.

- **Rechenschaftspflicht:** Verantwortlichkeiten sorgen für Rechenschaftspflicht. Wenn bestimmte Aufgaben und Ziele einer bestimmten Person oder Gruppe zugeordnet sind, können sie für die Erfüllung dieser Aufgaben verantwortlich gemacht werden.
  - **Qualitätskontrolle:** Die klare Zuweisung von Verantwortlichkeiten ermöglicht die Überwachung und Kontrolle von Prozessen und Aktivitäten. Dies trägt zur Sicherstellung hoher Qualitätsstandards bei.
  - **Risikomanagement:** In Bereichen wie Informationssicherheit und Compliance ist die Definition von Verantwortlichkeiten entscheidend, um Risiken zu identifizieren und zu minimieren. Sie trägt dazu bei, Sicherheitslücken zu schliessen und rechtliche Anforderungen zu erfüllen.
  - **Konfliktlösung:** Wenn es Meinungsverschiedenheiten oder Konflikte gibt, können klare Verantwortlichkeiten helfen, diese zu lösen. Es ist klar ersichtlich, wer die letzte Entscheidungsbefugnis hat.
  - **Delegation und Entwicklung:** Die Definition von Verantwortlichkeiten ermöglicht es Führungskräften, Aufgaben und Verantwortlichkeiten gezielt zu delegieren. Dies trägt zur beruflichen Entwicklung der Mitarbeiter bei und fördert ihr Lernen und Wachstum.
  - **Vertrauen und Mitarbeiterengagement:** Mitarbeiter, die wissen, dass ihre Verantwortlichkeiten klar definiert sind, haben in der Regel mehr Vertrauen in die Organisation und sind stärker engagiert, da sie sich ihrer Rolle und Bedeutung bewusst sind.
  - **Kontinuität:** Klare Verantwortlichkeiten gewährleisten die Kontinuität in Unternehmen und Organisationseinheiten. Wenn eine Person ausscheidet oder vorübergehend abwesend ist, kann eine andere Person ihre Aufgaben nahtlos übernehmen.
  - **Einhaltung von Standards und Vorschriften:** In regulierten Branchen oder in Bereichen, in denen hohe Standards eingehalten werden müssen, sind klar definierte Verantwortlichkeiten entscheidend, um sicherzustellen, dass alle Anforderungen erfüllt werden.
- (2) Insgesamt ist die Definition von Verantwortlichkeiten ein wichtiger Bestandteil des effektiven Organisationsmanagements. Sie hilft, Unklarheiten und Ineffizienzen zu beseitigen, fördert die Rechenschaftspflicht und trägt zur Verbesserung der Gesamtleistung und des Erfolgs einer Organisation bei. Die klare Kommunikation von Verantwortlichkeiten ist ein Zeichen für eine gut geführte Organisation.
- (3) Die Steigerung der IKT-Resilienz erfordert klare Verantwortlichkeiten und Rollen in einer Organisation. Dies gewährleistet, dass Massnahmen zur Verteidigung gegen Cyberbedrohungen und zur Aufrechterhaltung der Geschäftskontinuität effektiv geplant, umgesetzt und überwacht werden.
- (4) Die klare Festlegung dieser Verantwortlichkeiten sorgt dafür, dass alle Aspekte der IKT-Cyber-Resilienz abgedeckt sind, von der Strategieentwicklung über die technische Umsetzung bis zur täglichen Überwachung und Reaktion auf Sicherheitsvorfälle. Es ermöglicht auch eine effektive Koordination zwischen den verschiedenen Teams und Abteilungen, um sicherzustellen, dass Cybersicherheit als gemeinsame Verantwortung wahrgenommen wird.



Die oberste Führungsebene jedes Unternehmens muss sich seiner Verantwortung bewusst sein (OR 754 Organhaftung).

Bei der Zuteilung von Verantwortlichkeiten ist darauf zu achten, dass für sämtliche zugeteilten Personen eine Stellvertretung benannt wird. Und diese befähigt wird, jederzeit lückenlos die ihr zugeteilte Verantwortlichkeit zu übernehmen.



#### 5.4.6.1 Verantwortlichkeiten nach dem RASCI-Modell

- (1) Das RASCI-Modell (auch als RACI-Modell bezeichnet) ist ein Framework zur Definition von Verantwortlichkeiten und Rollen innerhalb von Projekten, Prozessen oder Unternehmen und Organisationseinheiten. Es hilft dabei, Klarheit über die Aufgaben und Verantwortlichkeiten verschiedener Beteiligten herzustellen, um eine effektive Zusammenarbeit sicherzustellen und die Erfolgswahrscheinlichkeit zu erhöhen. Das Akronym "RASCI" steht für die fünf Hauptrollen im Modell.

Index	Bezeichnung	Beschreibung / Grundsätze
<b>R</b>	<b>Responsible</b> (Verantwortlich)	Die Person oder Gruppe, die für die tatsächliche Ausführung einer Aufgabe oder Aktivität verantwortlich ist. Diese Person führt die notwendigen Schritte aus, um die Aufgabe zu erledigen und das gewünschte Ergebnis zu erzielen. Es kann mehrere "Verantwortliche" für eine Aufgabe geben, abhängig von deren Umfang und Komplexität.
<b>A</b>	<b>Accountable</b> (Zuständig / Rechenschaftspflichtig)	Die Person, die die ultimative Verantwortung für eine Aufgabe oder einen Prozess trägt. Die "Zuständige" ist dafür verantwortlich, dass die Aufgabe erfolgreich abgeschlossen wird. Es kann nur eine einzige "Zuständige" für eine Aufgabe geben. Diese Person ist für die Endabnahme, die Sicherstellung der Qualität und die Einhaltung von Terminen zuständig.
<b>S</b>	<b>Supportive</b> (Ausführend / Unterstützend)	Personen oder Gruppen, die den "Verantwortlichen" dabei unterstützen, die Aufgabe erfolgreich auszuführen. Sie können Ressourcen, Fachwissen, Werkzeuge oder Informationen bereitstellen und ermöglichen damit, dass die Aufgabe reibungslos abläuft. Die "Unterstützenden" arbeiten eng mit den "Verantwortlichen" zusammen.
<b>C</b>	<b>Consulted</b> (Konsultierend)	Personen oder Gruppen, die konsultiert werden müssen, bevor Entscheidungen getroffen oder Massnahmen ergriffen werden. Sie haben spezifisches Wissen oder Fachkenntnisse, die für die Aufgabe oder den Prozess relevant sind, und bieten Beratung oder Feedback an. Die endgültige Entscheidungskompetenz liegt jedoch nicht bei ihnen, sondern beim «Zuständigen».
<b>I</b>	<b>Informed</b> (Informieren)	Personen oder Gruppen, die über den Fortschritt, das Ergebnis oder die Entscheidungen im Zusammenhang mit der Aufgabe oder dem Prozess informiert werden müssen. Diese Personen müssen auf dem Laufenden gehalten werden, sind jedoch in der Regel nicht direkt in die Aufgabe involviert.

**Tabelle 3:** Verantwortlichkeiten nach RASCI (Quelle VSE)

- (2) Das RASCI-Modell wird oft in einer Matrixform dargestellt, in der Aufgaben oder Prozesse auf der horizontalen Achse und die fünf Rollen auf der vertikalen Achse aufgeführt sind. Jede Aufgabe oder Aktivität wird dann mit den entsprechenden Buchstaben abgekürzt, um die Rollen zuzuweisen. Das RASCI-Modell fördert die Klarheit und Transparenz bei der Zuweisung von Verantwortlichkeiten und Rollen. Es hilft dabei, Missverständnisse und Doppelspurigkeit zu vermeiden, die Effizienz zu steigern, die Kommunikation zu verbessern und die Koordination innerhalb eines Projekts, Prozesses oder einer Organisation zu erleichtern. Es ist ein wertvolles Instrument für das Management von Aufgaben und die Sicherstellung einer effektiven Zusammenarbeit.



#### Empfehlung der VSE Cyber Security Task Force Experten:

Die Verwendung des RASCI-Modells für die Zuweisung der Verantwortlichen hilft den Unternehmen und Organisationseinheiten für ein gemeinsames Verständnis und sollte somit allumfassend eingeführt werden.



### 5.4.7 Informationssicherheit: Organisation und Organigramm

- (1) Die Sicherung von Informationen und Systemen ist entscheidend für die Widerstandsfähigkeit gegen Bedrohungen. Eine gut strukturierte Sicherheitsorganisation mit klaren Verantwortlichkeiten und Hierarchien ist unerlässlich. Das Organigramm für die Informationssicherheit sollte eine dedizierte Sicherheitsabteilung mit direkter Unterstellung unter die Unternehmensführung umfassen. Innerhalb dieser Abteilung werden spezialisierte Teams für Netzwerksicherheit, Datenschutz, Incident Response und Compliance gebildet, die eng zusammenarbeiten. Eine strukturierte Organisation fördert eine Sicherheitskultur, in der alle Mitarbeiter ihre Verantwortung für den Schutz von Informationen verstehen.
- (2) Die Zusammenarbeit mit externen Partnern ist ebenfalls wichtig, um Informationen über Bedrohungen zu erhalten. Das Organigramm sollte klare Schnittstellen zu anderen Sicherheitsorganisationen aufweisen, um die IKT-Resilienz zu stärken. Die Sicherheitsorganisation plant, implementiert und überwacht Sicherheitsmassnahmen, um Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und IT-Systemen sicherzustellen. Sie koordiniert verschiedene Sicherheitsfunktionen und entwickelt auf die Bedürfnisse des Unternehmens und die Organisationseinheiten zugeschnittene Strategien, Richtlinien und Prozeduren.
- (3) Das Sicherheitsorganigramm visualisiert diese Struktur und zeigt Hierarchien, Verantwortlichkeiten und Interaktionen. Es legt Schnittstellen fest und verdeutlicht den Informationsfluss innerhalb der Organisation. Die Funktionen können vielfältig sein, von Netzwerksicherheit bis zu Risikomanagement. Die klaren Zuständigkeiten gewährleisten eine effektive Kommunikation. Schnittstellen zwischen Teams ermöglichen eine nahtlose Zusammenarbeit, insbesondere zwischen Netzwerksicherheit und physischer Sicherheit.
- (4) Die Sicherheitsorganisation ist eng mit anderen Abteilungen wie IT, Rechtsabteilung und Risikomanagement verbunden, was eine ganzheitliche Betrachtung von Sicherheitsrisiken ermöglicht. Insgesamt spielt die Sicherheitsorganisation eine zentrale Rolle bei der Schaffung einer umfassenden und koordinierten Sicherheitsinfrastruktur. Die klare Definition von Verantwortlichkeiten, die effektive Zusammenarbeit und die Integration in die Gesamtstruktur des Unternehmens stärken die Informationssicherheit und erhöhen die Resilienz gegenüber Bedrohungen.

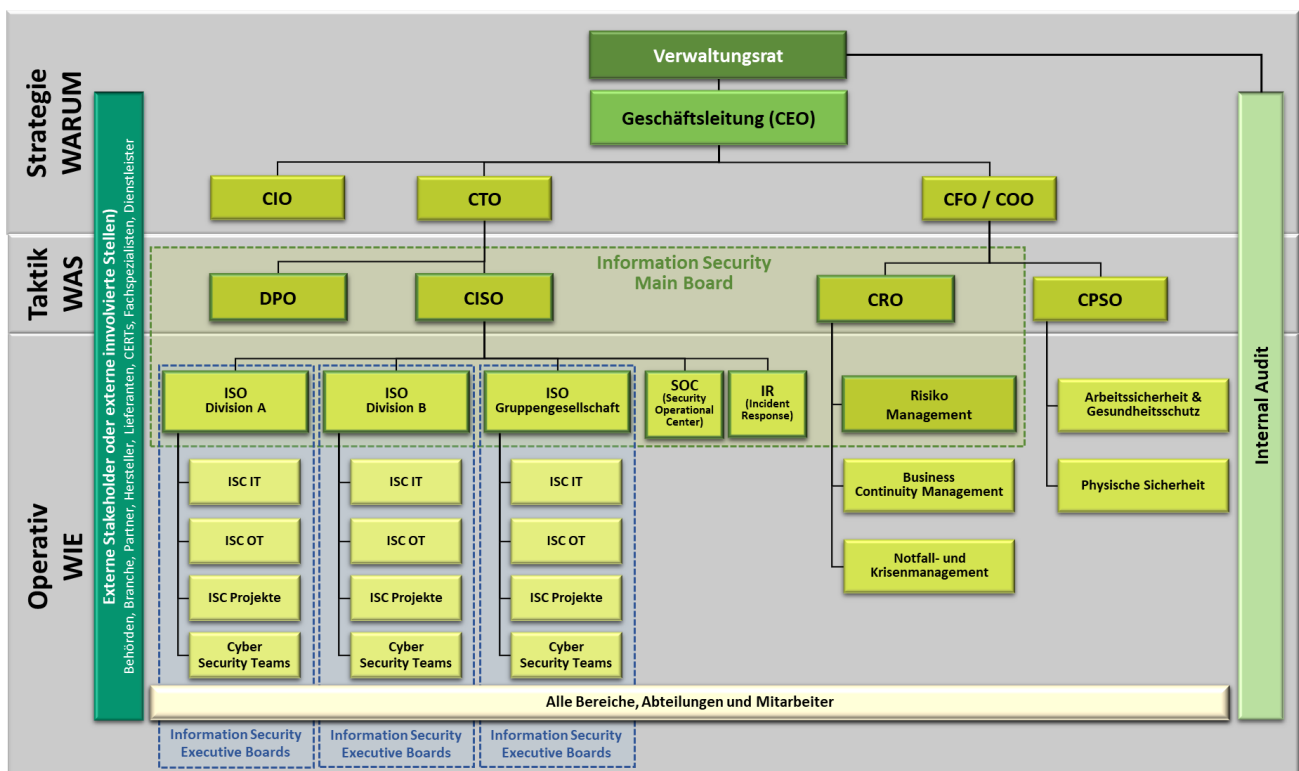


Abbildung 14: Prinzipielle Struktur eines möglichen Sicherheitsorganigramms (Quelle VSE)

- (5) Das Sicherheitsorganigramm für die unternehmensweite Informationssicherheit variiert je nach Grösse, Komplexität und Bedürfnissen der Unternehmung. Wichtig ist dabei sicherzustellen, dass eine Trennung zwischen strategischer, taktischer und operativer Ebene gewährleistet ist. Weiter soll eine klare Trennung zwischen den Verantwortlichkeiten betreffend Vorgaben und Ausführung mit anschliessenden Nachweisen gemacht werden (wer etwas vorgibt, kann es nicht auch ausführen -> Segregation of Duties). Die genaue Struktur und die Verantwortlichkeiten können je nach den spezifischen Anforderungen und





Ressourcen der Organisation variieren. Das Ziel besteht darin, eine umfassende Sicherheitsstruktur zu schaffen, damit ein effizientes und angemessenes Informationssicherheits-Management umgesetzt und betrieben werden kann.



Die Struktur einer Sicherheitsorganisation für die Informationssicherheit variiert je nach Grösse, Komplexität und Bedürfnissen eines Unternehmens und der Organisationseinheiten. Wichtig ist, dass eine Trennung zwischen strategischer, taktischer und operativer Ebene gemacht wird. Weiter soll eine klare Trennung zwischen den Verantwortlichkeiten betreffend Vorgaben und Ausführung mit anschliessenden Nachweisen eingehalten werden (wer vorgibt, kann nicht in Personalunion ausführen).



**Empfehlung der VSE Cyber Security Task Force Experten:**

Der Aufbau einer Sicherheitsorganisation ist für die Steigerung der IKT-Resilienz zwingend erforderlich. Diese muss schriftlich festgehalten und durch das oberste Management getragen und kommuniziert werden. Alle involvierten Stellen und Personen müssen sich ihren Funktionen, Rechten und Pflichten bewusst sein.

- (6) Im Bild oben ist ein Beispiel für eine mögliche Struktur eines Sicherheitsorganigramms aufgezeigt, welches folgende Elemente umfasst:

#### 5.4.7.1 Funktionen des Sicherheitsorganigramms auf strategischer Ebene:

- **Verwaltungsrat:** Der Verwaltungsrat definiert die Informationssicherheit auf höchster Ebene und trägt somit auch die Gesamtverantwortung.
- **Geschäftsleitung (C-Level):** Die Geschäftsleitung ist ein elementarer Bestandteil der Sicherheitsorganisation. Sie muss die Sicherheitsstrategie festlegen und ist gesamthaft verantwortlich für die Umsetzung der Informationssicherheit, somit auch für die Steigerung der IKT-Resilienz.

#### 5.4.7.2 Funktionen des Sicherheitsorganigramms auf taktischer Ebene:

- **DPO (Data Protection Officer oder Compliance- und Datenschutzbeauftragte):** Diese Positionen sind verantwortlich für die Gewährleistung der Einhaltung gesetzlicher Vorschriften und Branchenstandards im Bereich Datenschutz und Sicherheit. Sie helfen bei der Einhaltung von Vorschriften wie des Schweizer Datenschutzgesetzes und deren Verordnung sowie weiteren relevanten gesetzlichen Vorgaben im Bereich Datenschutz und Compliance.
- **CISO (Chief Information Security Officer):** Der CISO ist verantwortlich für das Informationssicherheit Management und ist die Führungsperson für die Cybersicherheitsstrategie der Organisation. Er berichtet direkt an die Geschäftsleitung. Er leitet das Information Security Main Board, in welchem alle Vorgaben (Richtlinien und Arbeitsanleitungen) erstellt und überwacht werden. Oft wird bei mittleren und kleinen Unternehmen und Organisationseinheiten der CISO durch eine externe Stelle besetzt.
- **Information Security Main Board:** Das Information Security Main Board spielt eine entscheidende Rolle bei der Gewährleistung der Informationssicherheit in einem Unternehmen und in den Organisationseinheiten. Dieses Board ist operationell verantwortlich für die Entwicklung, Umsetzung und Überwachung der Informationssicherheitsstrategie sowie sämtlicher Vorgaben und Massnahmen, die darauf abzielen, die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und IT-Ressourcen sicherzustellen.

Zu den Hauptaufgaben des Information Security Main Boards gehört die Formulierung von umfassenden Sicherheitsvorgaben und -strategien, die den Geschäftszielen des Unternehmens und den Organisationseinheiten entsprechen. Dies beinhaltet unter anderem die Gestaltung einer robusten Sicherheitsarchitektur für IKT-Systeme und -Infrastrukturen, um potenzielle Risiken zu minimieren.

Ein weiterer zentraler Bereich ist die Zusammenarbeit mit dem Risikomanagement, das die Identifikation, Bewertung und Priorisierung von Sicherheitsrisiken umfasst. Hierbei entwickelt das Information Security Main Board Strategien zur Risikominderung und -kontrolle, um die Widerstandsfähigkeit des Unternehmens und der Organisationseinheiten gegenüber Bedrohungen zu stärken.

Das Board ist es auch massgeblich an der Einrichtung von Prozessen und Plänen zur effektiven Reaktion auf Sicherheitsvorfälle beteiligt. Dies umfasst Incident Response und die Schnittstelle zum Notfall- und Krisenmanagement, um eine schnelle und koordinierte Reaktion auf Sicherheitsvorfälle zu gewährleisten.



Zusätzlich spielt das Information Security Main Board eine entscheidende Rolle bei der Überwachung und Analyse von Sicherheitsereignissen in Echtzeit. Es initiiert den Aufbau von Sicherheitsüberwachungssysteme und analysiert Bedrohungen, um proaktiv auf potenzielle Sicherheitsrisiken reagieren zu können.

Das Board ist auch für Schulungs- und Sensibilisierungsprogramme verantwortlich, um das Sicherheitsbewusstsein der Mitarbeiter zu stärken. Dies schliesst die Bereitstellung von Schulungen zu Sicherheitspraktiken und die Sensibilisierung für aktuelle Bedrohungen ein.

Das Information Security Main Board stellt sicher, dass das Unternehmen und die Organisationseinheiten gesetzliche Anforderungen und branchenspezifische Vorschriften hinsichtlich Informationssicherheit erfüllt.

Der Datenschutz ist ein Teilbereich der Informationssicherheit. Er wird jedoch vom DPO verantwortet. Die Massnahmen werden durch das Main Board nach Vorgaben des DPO in Auftrag gegeben und überprüft.

Die technologische Evaluierung von neuen Lösungen und die Empfehlung von Sicherheitstechnologien sind ebenfalls wichtige Aufgaben. Hierbei bewertet das Information Security Main Board kontinuierlich neue Technologien, um sicherzustellen, dass sie den Sicherheitsstandards entsprechen.

Die enge Zusammenarbeit mit anderen Bereichen, Abteilungen, Führungskräften und externen Partnern ist ein wesentlicher Bestandteil der Arbeit des Information Security Main Board. Durch Kommunikation auf C-Level-Ebene wird das Bewusstsein für Sicherheitsrisiken geschärft und die Zusammenarbeit zur Erreichung gemeinsamer Sicherheitsziele gefördert.

Schliesslich legt das Information Security Main Board grossen Wert auf kontinuierliche Verbesserung, indem es Sicherheitsvorgaben und -prozesse überprüft, aktualisiert und Massnahmen zur ständigen Optimierung der Informationssicherheit implementiert.

- **CRO (Chief Risk Officer):** Der Chief Risk Officer (CRO) ist verantwortlich für das unternehmensweite Risikomanagement und rapportiert direkt an die Geschäftsleitung. Seine Aufgaben umfassen nebst dem unternehmensweiten Risikomanagement auch die Unterstützung des Information Security Main Boards und weiteren Funktionen bei der Identifikation, Bewertung und Kontrolle von Risiken in den jeweiligen Teilbereichen. Der CRO entwickelt Strategien zur Risikominderung und -kontrolle, gewährleistet die Einhaltung von Gesetzen und Vorschriften, und spielt eine Schlüsselrolle im Business Continuity -, Notfall- und Krisenmanagement. Durch kontinuierliche Überwachung und Bewertung sorgt der CRO dafür, dass das Unternehmen und die Organisationseinheiten angemessen auf Sicherheitsrisiken reagiert und somit eine resilientere Informationssicherheitsermöglich.
- **CPSO (Chief Physical Safety Officer):** Der Chief Physical Safety Officer (CPSO) ist zuständig für die Arbeitssicherheit und Gesundheitsschutz sowie physische Sicherheit. Im Bereich Arbeitssicherheit und Gesundheitsschutz entwickelt der CPSO Strategien und Massnahmen, um sicherzustellen, dass Mitarbeiter in einer sicheren und gesunden Umgebung arbeiten können. Dies beinhaltet die Implementierung von Schulungsprogrammen und Richtlinien, um Unfälle zu vermeiden und die Gesundheit der Mitarbeiter zu schützen.

Im Bereich physische Sicherheit ist der CPSO für den Schutz von Unternehmenseinrichtungen und -ressourcen verantwortlich. Dies umfasst die Implementierung von Zugangskontrollen, Überwachungssystemen und anderen Sicherheitsmassnahmen, um unbefugten Zugriff zu verhindern und physische Bedrohungen zu minimieren. Der CPSO spielt eine zentrale Rolle bei der Entwicklung von Sicherheitsplänen, um die physische Sicherheit des Unternehmens und der Organisationseinheiten zu gewährleisten.



**Empfehlung der VSE Cyber Security Task Force Experten:**

Mittlere und kleinere Unternehmen und Organisationseinheiten sollen prüfen, ob die Funktion des CISO's wie auch die Bereiche des Information Security Main Boards von einem Dienstleister 'As a Service', bezogen werden sollen. Da der Aufbau von internen Ressourcen mit den benötigten Fähigkeiten längere Zeit in Anspruch nehmen wird.

#### 5.4.7.3 Funktionen des Sicherheitsorganigramms auf operativer Ebene:

- **ISO (Information Security Officer):** Diese Funktion ist Mitglied des Information Security Main Board und verantwortet die Informationssicherheit für eine oder mehrere Divisionen im Unternehmen. Er ist die Schnittstelle zwischen dem CISO und den zuständigen Divisionen. Der ISO erstellt und überwacht



die Arbeitsanleitungen und publiziert diese in den verschiedenen Bereichen. Weiter stellt er zusammen mit dem Information Security Coordinator (ISC) sicher, dass die Sicherheitsvorgaben umgesetzt werden.

- **ISC (Information Security Coordinator):** Er ist das Bindeglied zwischen den einzelnen organisatorischen Bereichen in den Divisionen und dem Information Security Main Board bzw. dem ISO. Abhängig vom Unternehmen und den Organisationseinheiten koordiniert der ISC in der IT, der OT und den Projekten die Belange der Informationssicherheit.
- **SOC (Security Operation Center):** Das Security Operation Center (SOC) ist ein essenzieller Bestandteil und unter der Koordination des Information Security Main Board. Es spielt eine zentrale Rolle im Bereich des Incident Response eines Unternehmens und der Organisationseinheiten. Die Hauptaufgaben des SOC liegen in der proaktiven Überwachung, Erkennung und Reaktion auf Sicherheitsvorfälle. Eine der zentralen Funktionen des SOC besteht in der kontinuierlichen Überwachung der IT-OT-Infrastruktur auf potenzielle Sicherheitsbedrohungen. Hierbei kommen fortschrittliche Überwachungssysteme und Technologien zum Einsatz, um Anomalien und verdächtige Aktivitäten frühzeitig zu erkennen.

Das SOC meldet die erkannten Sicherheitsvorfälle dem CSIRT für weitere Untersuchungen und Behandlung. Die Integration von Threat Intelligence ist eine weitere Aufgabe des SOC. Hierbei werden aktuelle Informationen über Bedrohungen aus verschiedenen Quellen genutzt, um die Verteidigung des Unternehmens und der Organisationseinheiten gegenüber neuen und sich entwickelnden Gefahren zu stärken.

Insgesamt fungiert das SOC als Nervenzentrum für die Überwachung und Reaktion auf Sicherheitsvorfälle. Durch eine effektive Zusammenarbeit mit anderen Sicherheitsabteilungen und dem CISO trägt das SOC dazu bei, die Gesamtsicherheit der Informationssysteme zu gewährleisten und die Organisation widerstandsfähiger gegenüber Cyberbedrohungen zu machen.



Für die Unternehmen und Organisationseinheiten macht es Sinn, dass das SOC (Security Operation Center) 'As a Service' bei einem Drittanbieter bezogen wird.

- **IR (Incident Response):** Das Incident Response (IR) spielt eine wichtige Rolle im Bereich der Informationssicherheit, indem es auf die Erkennung und Bewältigung von komplexen Sicherheitsvorfällen fokussiert ist, welches durch das interne CSIRT nicht selbständig bewältigt werden können. Die Hauptaufgabe des Incident Response besteht darin, effektiv auf komplexe Sicherheitsvorfälle zu reagieren, um potenzielle Schäden zu minimieren und die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und Ressourcen zu schützen.



In mittleren und kleinen Unternehmen und Organisationseinheiten macht es oft Sinn, dass das IR (Incident Response) 'As a Service' bei einem Drittanbieter bezogen wird.



Bei Abschluss einer Cyber Assurance ist bei einigen Anbietern ein Incident Response Service inkludiert.

- **Die Cybersecurity Teams:** Unter dem ISO gibt es in der Regel ein Team von Spezialisten, das sich auf verschiedene Aspekte der Cybersicherheit konzentriert. Dieses Team kann folgende Rollen umfassen:
  - **CSIRT:** Die Sicherheitsanalysten im CSIRT spielen eine entscheidende Rolle bei der Bewertung von Warnmeldungen und der Unterscheidung zwischen normalen Betriebsereignissen und potenziellen Angriffen. Hierbei kommt auch die enge Zusammenarbeit mit dem Information Security Main Board und anderen Cyber Security Teams im Unternehmen und in den Organisationseinheiten ins Spiel.  
Wenn ein Sicherheitsvorfall auftritt, ist das CSIRT dafür verantwortlich, schnell zu handeln. Das beginnt mit der umgehenden Identifikation und Verifizierung des Vorfalls. Hierbei werden unterschiedliche Tools und Technologien eingesetzt, um die Art und den Umfang des Vorfalls zu verstehen. Sobald potenzielle Bedrohungen identifiziert sind, ist das Cyber Security Team inkl. CSIRT für die Untersuchung und Analyse dieser Vorfälle verantwortlich. Dies umfasst die Bestimmung der Art und des Ausmasses der Bedrohung sowie die Einschätzung ihrer



potenziellen Auswirkungen auf die einzelnen Bereiche eines Unternehmens und der Organisationseinheiten. Ein weiterer wichtiger Aspekt liegt in der effektiven Reaktion auf Sicherheitsvorfälle.

Das CSIRT entwickelt und implementiert klare Verfahren und Pläne für den Umgang mit Sicherheitszwischenfällen, einschliesslich der Koordination mit anderen relevanten Teams und Abteilungen.

Die effektive Eindämmung des Vorfalls steht im Zentrum des CSIRT. Das Team arbeitet daran, die Ausbreitung des Angriffs zu stoppen und weitere Schäden zu verhindern. Dies kann die Isolierung von Systemen, die Deaktivierung von Benutzerkonten oder andere Massnahmen umfassen, um den Vorfall einzudämmen.

Parallel dazu kann zusammen mit dem Incident Response Team eine forensische Analyse erfolgen, um die Ursachen des Vorfalls zu verstehen und Beweismaterial für weitere Massnahmen zu sammeln. Hierbei werden auch Schwachstellen identifiziert, die zu dem Vorfall geführt haben könnten, um präventive Massnahmen zur Stärkung der Sicherheit zu ergreifen.

Die Kommunikation spielt eine entscheidende Rolle im CSIRT. Das Team ist dafür verantwortlich, relevante Stakeholder, darunter Führungskräfte, Mitarbeiter und gegebenenfalls externe Parteien, zu informieren. Dies fördert eine transparente Kommunikation und ermöglicht eine koordinierte Reaktion auf den Vorfall.

Schliesslich erfolgt die Dokumentation des gesamten Vorfalls und der getroffenen Massnahmen. Diese Dokumentation ist nicht nur wichtig für die interne Analyse und Verbesserung, sondern auch für rechtliche oder regulatorische Anforderungen sowie für die Zusammenarbeit mit externen Behörden.

Zusammengefasst ist das CSIRT unverzichtbar, um die Reaktionsfähigkeit eines Unternehmens und der Organisationseinheiten auf Sicherheitsvorfälle sicherzustellen. Durch eine schnelle, koordinierte und gut dokumentierte Reaktion trägt das Team dazu bei, die Auswirkungen von Sicherheitsvorfällen zu minimieren und die Widerstandsfähigkeit der Organisation zu stärken.

Bei komplexen Sicherheitsvorfällen kann das CSIRT auf das (externe) Incident Response Team zur Unterstützung und weiteren Behandlung bzw. Analyse zurückgreifen.

Das CSIRT ist ebenfalls massgeblich an der kontinuierlichen Verbesserung der Sicherheitslage beteiligt. Durch die Analyse von Sicherheitsvorfällen und die Identifizierung von Schwachstellen trägt das CSIRT dazu bei, präventive Massnahmen zu entwickeln, um zukünftige Angriffe zu verhindern.

- **Security Awareness and Training Team:** Diese Gruppe kümmert sich um die Schulung der Mitarbeiter und erhöht das Bewusstsein für Sicherheitsrisiken und bewährte Verfahren.
- **Security Architects:** Diese Experten sind für die Planung und Gestaltung sicherer IKT-Architekturen und -lösungen verantwortlich.
- **Security Analysts:** Diese Analytiker überwachen die Sicherheitsereignisse, untersuchen Vorfälle, führen Sicherheitsaudits durch und unterstützen bei der Identifizierung von Schwachstellen.
- **Network Security Team:** Diese Gruppe konzentriert sich auf die Sicherheit von Netzwerken und Kommunikationssystemen. Dazu gehören Firewall-Administratoren, Netzwerksicherheitssingenieure und Experten für die Netzwerksegmentierung.
- **Server and Client Security Team:** Dieses Team konzentriert sich auf die Sicherheit von Server und Client. Es umfasst Sicherheitsprüfer, Entwickler für sichere Anwendungen und Experten für Sicherheitstests.
- **Application Security Team:** Dieses Team konzentriert sich auf die Sicherheit von Anwendungen und Software-Entwicklungen. Es umfasst interne Sicherheitsprüfer, Spezialisten und Experten für Sicherheitstests.
- **Physical Security Team:** Neben der digitalen Sicherheit ist auch die physische Sicherheit der IKT-Infrastruktur wichtig. Dieses Team ist für den Schutz von Rechenzentren, Serverräumen und anderen physischen Ressourcen verantwortlich.
- **Third-Party Risk und Supply Chain Management:** Dieses Team ist dafür verantwortlich, die Sicherheit von Dienstleistern, Drittanbietern und Lieferanten zu überwachen und sicherzustellen, dass sie die Sicherheitsstandards der Organisation einhalten.



- **Alle Mitarbeiter:** Jeder Nutzer von IKT-Mitteln muss sich möglicher Cyberbedrohungen bewusst sein und im eigenen Handlungsbereich darauf adäquat agieren können. Er muss vermeintliche Sicherheitsvorfälle zeitnah den entsprechenden Sicherheitsstellen melden und somit als Sensor für die Informationssicherheit agieren können. Damit leistet jeder Mitarbeiter massgebend und kontinuierlich einen grossen Beitrag zur Steigerung der IKT-Resilienz und ist somit auch in seiner täglichen Tätigkeit mitverantwortlich für den Schutz des Unternehmens und der Organisationseinheiten.

Die Sicherheit der Informationen betrifft alle Mitarbeiter gleichermassen. Jeder Einzelne kann durch verantwortungsbewusstes und qualitätsorientiertes Handeln dazu beitragen, Schäden zu vermeiden und zum Erfolg beizutragen. Eine Sensibilisierung für Informationssicherheit sowie Schulungen für Mitarbeiter und Führungskräfte sind daher grundlegend für die Sicherheit der Informationen. Um Sicherheitsmassnahmen effektiv umzusetzen, müssen Mitarbeiter nicht nur die erforderlichen Kenntnisse über die Bedienung von Sicherheitsmechanismen besitzen, sondern auch das Verständnis für den Sinn und Zweck dieser Massnahmen. Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeiter beeinflussen die Informationssicherheit massgeblich.

Bei Neueinstellungen oder Veränderungen von Aufgaben ist eine umfassende Einarbeitung und gegebenenfalls Schulung notwendig. Sicherheitsrelevante Aspekte des jeweiligen Arbeitsplatzes sollten dabei berücksichtigt werden. Bei Ausscheiden oder Veränderungen der Zuständigkeiten von Mitarbeitern muss dieser Prozess durch geeignete Sicherheitsmassnahmen begleitet werden, wie etwa dem Entzug von Berechtigungen und der Rückgabe von Schlüsseln und Ausweisen.

Es ist wichtig, dass Mitarbeiter sich zur Einhaltung aller relevanten Gesetze, Vorschriften und Regelungen verpflichten. Hierbei ist es erforderlich, sie mit den bestehenden Regelungen zur Informationssicherheit vertraut zu machen und sie gleichzeitig zur Einhaltung zu motivieren. Darüber hinaus sollten die Mitarbeiter darüber informiert sein, dass jeder erkannte oder vermutete Sicherheitsvorfall unverzüglich dem Sicherheitsmanagement gemeldet werden muss, und sie sollten wissen, wie und an wen diese Meldung erfolgen sollte.

- **Information Security Executive Boards:** Die Information Security Executive Boards spielen eine zentrale Rolle im Rahmen der Informationssicherheit auf der operationellen Ebene, welche verschiedene Schlüsselakteure und Funktionen innerhalb eines Unternehmens und der Organisationseinheiten einbezieht. Dieses Gremium besteht aus Führungskräften, darunter der Information Security Officer (ISO), der Information Security Coordinator (ISC) für IT, OT und Projekte, sowie Vertretern der Cyber Security Teams. Es agiert als Bindeglied zu den vielfältigen Bereichen, Abteilungen und Mitarbeitern, die alle an der Sicherung der Informationen und IT-Systeme beteiligt sind.

Der Information Security Officer (ISO) übernimmt die Rolle des höchsten Verantwortlichen im Information Security Executive Board. Der ISO trägt die Verantwortung für die Umsetzung umfassender Sicherheitsstrategien sowie die Gewährleistung der Einhaltung gesetzlicher Bestimmungen und interner Richtlinien.

Der Information Security Coordinator (ISC) spielt eine entscheidende Rolle bei der Koordinierung der Sicherheitsbemühungen in verschiedenen Schlüsselbereichen, einschliesslich IT, OT und Projekten. Der ISC ist verantwortlich für die Integration von Sicherheitspraktiken in diese verschiedenen Kontexte und stellt sicher, dass Sicherheitsaspekte in alle Unternehmens- und der Organisationseinheitenaktivitäten integriert werden.

Die Cyber Security Teams, die spezialisierte Gruppen von Fachleuten umfassen, sind unmittelbar an der Umsetzung von Sicherheitsmassnahmen und der Bewältigung von Sicherheitsvorfällen beteiligt. Sie arbeiten eng mit dem Information Security Executive Board zusammen, um aktuelle Bedrohungen zu bewerten, geeignete Gegenmassnahmen zu entwickeln und sicherzustellen, dass die gesamte Organisation gegenüber Cyberbedrohungen widerstandsfähig ist.

Das Information Security Executive Board schafft eine koordinierte und kohärente Herangehensweise an Informationssicherheit, indem es die verschiedenen Akteure in die Entwicklung und Umsetzung von Sicherheitsstrategien einbezieht. Es fördert eine Kultur der Sicherheit, die alle Bereiche, Abteilungen und Mitarbeiter eines Unternehmens und der Organisationseinheiten einschliesst. Durch regelmässige Kommunikation, Schulungen und klare Sicherheitsrichtlinien trägt das Board dazu bei, das Bewusstsein für Sicherheitsfragen zu schärfen und sicherzustellen, dass Informationssicherheit eine Priorität auf allen Ebenen der Organisation bleibt.





- (7) Die genaue Struktur und die Verantwortlichkeiten können je nach den spezifischen Anforderungen und Ressourcen der Organisation variieren. Das Ziel besteht darin, eine umfassende Sicherheitsstruktur zu schaffen, die die Organisation vor Cyber-Bedrohungen schützt und sicherstellt, dass die IKT-Systeme sicher und konform betrieben werden.



**Empfehlung der VSE Cyber Security Task Force Experten:**

Da das Aufgabengebiet eines Security Operation Center (SOC) und Incident Respond sehr umfangreich ist und spezielles Know-How erfordert, müssen Unternehmen und Organisationseinheiten genau prüfen, ob sie diesen Bereich nicht von einem Dienstleister 'As a Service' beziehen wollen.



Es ist sehr wichtig, dass alle Mitarbeiter in die Sicherheit eines Unternehmens und der Organisationseinheiten einbezogen werden. Sie leisten massgebend und kontinuierlich einen grossen Beitrag zur Steigerung der IKT-Resilienz und ist somit auch in seiner täglichen Tätigkeit mitverantwortlich.

#### 5.4.7.4 Übergreifende Elemente der Sicherheitsorganigramm über alle Ebenen:

- **Internal Audit (interne Revision):** Die interne Revision des Verwaltungsrates spielt eine entscheidende Rolle im Rahmen der Informationssicherheit, insbesondere wenn es darum geht, die IKT-Resilienz zu erhöhen. Das Hauptaugenmerk der internen Revision liegt darauf, sicherzustellen, dass die Sicherheitsmassnahmen und -kontrollen angemessen und effektiv sind, um die Informationen und IKT-Systeme der Organisation zu schützen. Die interne Revision überprüft und bewertet die Umsetzung von Informationssicherheitsrichtlinien, -verfahren und -standards. Dabei werden sowohl die technologischen Aspekte als auch die Prozesse und die Einhaltung von Vorschriften berücksichtigt. Die Revision zielt darauf ab, mögliche Schwachstellen und Risiken in der Sicherheitsinfrastruktur zu identifizieren.

Darüber hinaus prüft die interne Revision die Wirksamkeit von Sicherheitsmassnahmen, um sicherzustellen, dass sie den aktuellen Bedrohungen und Anforderungen standhalten. Dies beinhaltet eine Bewertung der Zugangskontrollen, Verschlüsselungsverfahren, Sicherheitsüberwachungssysteme und anderer technologischer Lösungen. Die Überprüfung erstreckt sich auch auf die Einhaltung von Sicherheitsstandards und Vorschriften. Die interne Revision stellt sicher, dass die Organisation die gesetzlichen Anforderungen erfüllt und branchenspezifische Best Practices befolgt, um die Informationssicherheit zu gewährleisten.

Ein weiterer wichtiger Aspekt ist die Bewertung der Resilienz der IKT gegenüber potenziellen Bedrohungen und Störungen. Die interne Revision prüft die Pläne und Massnahmen zur Wiederherstellung nach Sicherheitsvorfällen oder Katastrophen, um sicherzustellen, dass die Organisation schnell und effektiv auf solche Ereignisse reagieren kann.

Die Ergebnisse der internen Revision werden in Berichten festgehalten, die an den Verwaltungsrat und das Management der Organisation weitergeleitet werden. Diese Berichte bieten Einsichten in den aktuellen Stand der Informationssicherheit, identifizieren potenzielle Verbesserungsbereiche und unterstützen bei der Festlegung von Massnahmen zur Steigerung der IKT-Resilienz.

Insgesamt spielt die interne Revision eine Schlüsselrolle dabei, sicherzustellen, dass die Informationssicherheit im Unternehmen und in den Organisationseinheiten angemessen verwaltet wird. Durch ihre Überprüfungen und Empfehlungen trägt sie dazu bei, die Widerstandsfähigkeit der IKT gegenüber Bedrohungen zu erhöhen und somit die Kontinuität der Geschäftsprozesse sicherzustellen.

- **Externe Stakeholder oder externe involvierte Stellen:** Behörden, Branche z.B. VSE, Partner z.B. andere EVU, Hersteller, Lieferanten, Fachspezialisten und Dienstleister zählen zu den externen Stakeholdern oder externen involvierten Stellen. Externe Stakeholder und involvierte Stellen spielen eine entscheidende Rolle im umfassenden Rahmen der Informationssicherheit, der darauf abzielt, die Widerstandsfähigkeit der IKT zu erhöhen.

Behörden stellen als externe Stakeholder eine wichtige Quelle für rechtliche Rahmenbedingungen und Regulierungen dar, die die Informationssicherheit beeinflussen. Die enge Zusammenarbeit mit Behörden ist von grosser Bedeutung, um sicherzustellen, dass Unternehmen und Organisationseinheiten die gesetzlichen Anforderungen erfüllen und dabei Unterstützung und Richtlinien für bewährte Praktiken erhalten.

Branchenorganisationen spielen eine Schlüsselrolle bei der Schaffung von Branchenstandards und bewährten Methoden in Bezug auf Informationssicherheit. Die Zusammenarbeit mit diesen Organisationen ermöglicht es Unternehmen und Organisationseinheiten, von branchenspezifischem Wissen zu



profitieren und sicherzustellen, dass ihre Sicherheitspraktiken den aktuellen Branchenstandards entsprechen.

Die Partnerschaft mit externen Partnern, Herstellern und Lieferanten ist von essentieller Bedeutung, da deren Produkte und Dienstleistungen oft in die IKT-Infrastruktur integriert sind. Eine enge Abstimmung gewährleistet nicht nur die Sicherheit dieser Produkte und Dienstleistungen, sondern fördert auch einen transparenten Austausch von Sicherheitsinformationen und bewirkt eine verbesserte Gesamtsicherheit.

Externe Fachexperten können zusätzliche Perspektiven und spezialisiertes Wissen einbringen, um Unternehmen und Organisationseinheiten bei der Entwicklung und Umsetzung wirksamer Sicherheitsstrategien zu unterstützen.

Dienstleister, die auf Sicherheitsdienste spezialisiert sind, bieten zusätzliche Ressourcen und Fachkenntnisse an. Von Penetrationstests über Sicherheitsschulungen bis hin zu Incident Response-Dienstleistungen tragen sie dazu bei, die Sicherheitskapazitäten einer Organisation zu erweitern und sicherzustellen, dass sie auf eine breite Palette von Sicherheitsanforderungen vorbereitet ist.

Die Schnittstellen zwischen diesen externen Stakeholdern sind entscheidend, um einen nahtlosen Informationsaustausch zu gewährleisten und gemeinsam an der Stärkung der IKT-Resilienz zu arbeiten. Durch eine koordinierte Zusammenarbeit mit diesen externen Akteuren können Unternehmen und Organisationseinheiten eine umfassende, proaktive und widerstandsfähige Strategie entwickeln, um den Herausforderungen der sich ständig weiterentwickelnden Bedrohungslandschaft zu begegnen.



**Die konstruktive Zusammenarbeit mit externen Stakeholdern und externen Stellen ist von essentieller Bedeutung für die Steigerung der IKT-Resilienz. Die Schnittstellen müssen klar definiert und zugewiesen werden. Es ist sicherzustellen, dass alle notwendigen Stellen involviert und diese Schnittstellen aktiv bewirtschaftet werden.**

#### 5.4.8 Informationssicherheit: House of Processes

- (1) Ein Prozesshaus dient als organisatorische Struktur, um die Prozesse eines Unternehmens und der Organisationseinheiten hierarchisch zu ordnen und zu visualisieren. Der Sinn eines Prozesshauses liegt in mehreren wichtigen Aspekten:
  - **Strukturierung und Übersicht:** Ein Prozesshaus bietet eine klare Hierarchie, die es ermöglicht, die Vielzahl von Prozessen in einem Unternehmen und Organisationseinheiten zu strukturieren. Dies fördert die Übersichtlichkeit und Verständlichkeit der Prozesslandschaft.
  - **Transparente Prozessdarstellung:** Es ermöglicht eine transparente und leicht verständliche Darstellung der Prozesse, angefangen von strategischen und Managementprozessen bis hin zu den Kern- und Supportprozessen. Dies fördert das Verständnis der Mitarbeiter und Stakeholder für die Funktionsweise des Unternehmens und der Organisationseinheit.
  - **Identifikation von Wechselwirkungen:** Durch die Anordnung der Prozesse in einem Prozesshaus werden die Wechselwirkungen zwischen verschiedenen Prozessen verdeutlicht. Dies unterstützt eine ganzheitliche Betrachtung und ermöglicht eine bessere Koordination zwischen den Organisationseinheiten.
  - **Optimierung und Verbesserung:** Das Prozesshaus dient als Grundlage für die Identifikation von Optimierungspotentialen und Verbesserungsmöglichkeiten. Es erleichtert die gezielte Analyse und Anpassung von Prozessen, um Effizienz und Effektivität zu steigern.
  - **Integration von Informationstechnologien:** Ein Prozesshaus dient als Leitfaden für die Integration von Informationstechnologien, um die Prozesse effektiv zu unterstützen und zu automatisieren. Dies fördert die Digitalisierung und verbessert die Arbeitsabläufe.
  - **Kommunikation und Zusammenarbeit:** Es erleichtert die interne und externe Kommunikation, indem es eine klare Struktur für die Informationsvermittlung und Zusammenarbeit zwischen verschiedenen Organisationseinheiten und Interessengruppen bietet.
- (2) Zusammengefasst unterstützt ein Prozesshaus das Unternehmen und die Organisationseinheiten dabei, ihre Prozesse besser zu organisieren, zu verstehen, zu optimieren und effektiv zu gestalten. Es ist ein Werkzeug, um die Komplexität von Unternehmens- und Organisationseinheitsprozessen zu bewältigen und die Gesamtleistung eines Unternehmens und der Organisationseinheiten zu steigern.



#### 5.4.8.1 Aufbau des House of Processes

- (1) Das Konzept des Prozesshauses im Kontext des Informationsmanagements kann spezifisch auf die Anforderungen eines Stromversorgungsunternehmens und Stromorganisationseinheiten zugeschnitten sein. In den Unternehmen und Organisationseinheiten sind die verschiedenen Prozesse in einem Prozesshaus organisiert, um eine effiziente und transparente Verwaltung aller Aktivitäten zu gewährleisten. Folgender grundsätzlicher Aufbau gilt für ein House of Processes:

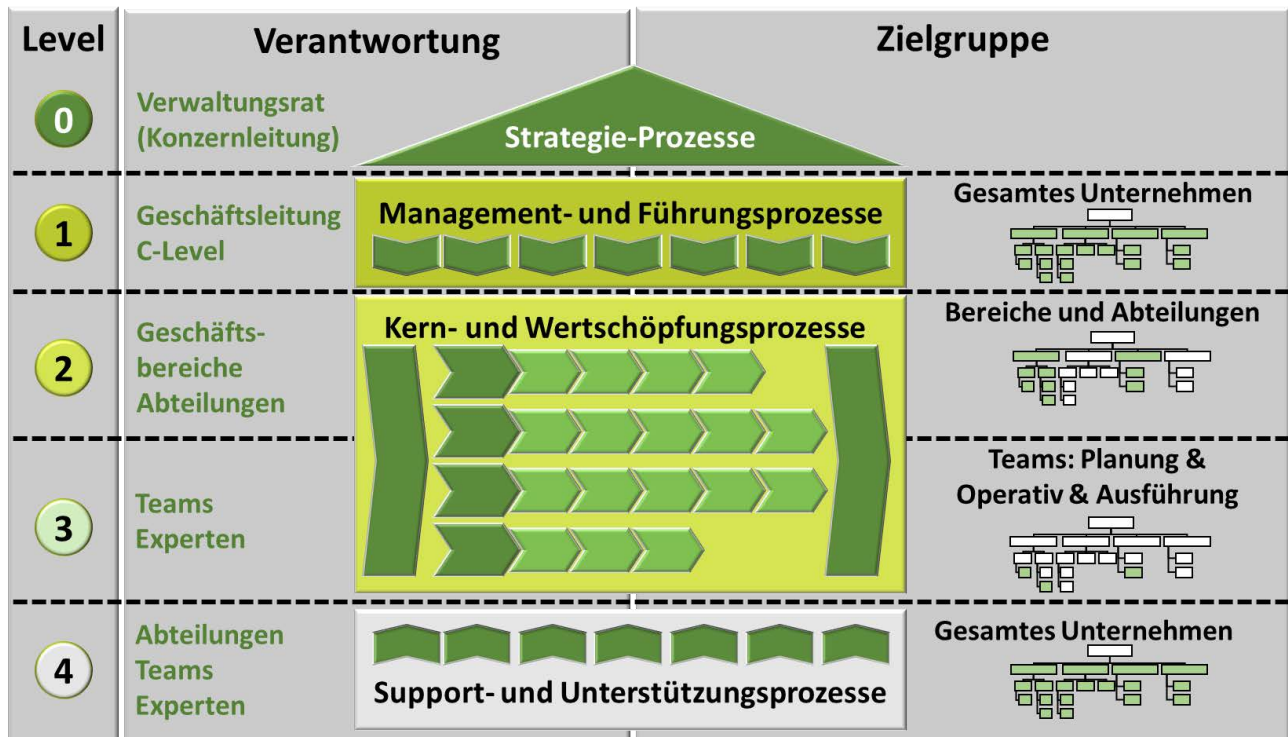


Abbildung 15: Struktur im House of Prozess (Quelle VSE)

- (2) Folgende Zusammenstellung beschreibt die wichtigsten Prozesse im Zusammenhang mit der Informationssicherheit:

- **Level 0 (Dach):** Strategische Prozesse:
  - **Energiepolitik und Strategieentwicklung:** Entwicklung von langfristigen Zielen und Strategien unter Berücksichtigung von Umweltaspekten, politischen Vorgaben und Marktanforderungen.
- **Level 1 (Dachgeschoss):** Management- und Führungsprozesse
 

Management- und Führungsprozesse sind entscheidende Elemente in der Organisation und Führung von Unternehmen. Hier ist eine Auflistung der wichtigsten Management- und Führungsprozesse:

  - **Planung:** Formulierung von konkreten Plänen und Handlungsanweisungen. Ressourcenplanung, einschliesslich Personal, Finanzen und Technologie. Erstellung von Budgets und Finanzprognosen.
  - **Organisation:** Festlegung von Organisationsstrukturen und Hierarchien. Zuweisung von Aufgaben und Verantwortlichkeiten. Etablierung von Kommunikations- und Koordinationsmechanismen.
  - **Entscheidungsfindung:** Analyse von Informationen und Daten. Identifikation von Handlungsoptionen. Auswahl der besten Alternativen unter Berücksichtigung von Risiken und Chancen.
  - **Führung und Motivation:** Entwicklung von Führungsprinzipien und -stilen. Motivation von Mitarbeitern zur Zielerreichung. Förderung einer positiven Unternehmenskultur.
  - **Kommunikation:** Festlegung von Kommunikationsrichtlinien und -plänen.- Verbreitung von relevanten Informationen an die Mitarbeiter. Förderung offener und effektiver Kommunikation in der Organisation.
  - **Implementierung:** Umsetzung von Plänen und Strategien in konkrete Handlungen. Einsatz von Ressourcen gemäss den festgelegten Prioritäten. Überwachung des Fortschritts und Anpassung bei Bedarf.

- **Überwachung und Kontrolle:** Festlegung von Leistungskennzahlen (KPIs) zur Überwachung. Kontinuierliche Bewertung von Prozessen und Ergebnissen. Implementierung von Korrekturmaßnahmen bei Abweichungen.
- **Risikomanagement:** Identifikation und Bewertung von Risiken. Entwicklung von Strategien zur Risikominimierung. Integration von Risikomanagement in Entscheidungs- und Planungsprozesse.
- **Innovationsmanagement:** Förderung einer Innovationskultur. Identifikation von Chancen für Produkt- und Prozessinnovationen. Implementierung von Innovationsstrategien.

Die Management- und Führungsprozesse sind oft miteinander verknüpft und interagieren, um sicherzustellen, dass Unternehmen effektiv geführt und gesteuert werden. Der Erfolg eines Unternehmens hängt massgeblich von der Fähigkeit ab, diese Prozesse sinnvoll zu integrieren und anzupassen.

■ **Level 2 (Obergeschoss):** Kernprozesse der Wertschöpfungskette

- **Stromerzeugung:** Umfasst die verschiedenen Methoden der Stromerzeugung, sei es durch konventionelle Kraftwerke, erneuerbare Energien oder andere Quellen.
- **Netzmanagement:** Planung, Ausbau und Wartung des Stromnetzes, um eine zuverlässige Energieversorgung zu gewährleisten.
- **Netzbetrieb:** Verantwortlich für den reibungslosen Betrieb des Stromnetzes, die Steuerung der Energieströme und die Gewährleistung der Netzstabilität.
- **Lastmanagement:** Überwachung und Anpassung der Energieproduktion an die aktuelle Nachfrage, um Engpässe oder Überkapazitäten zu vermeiden.

■ **Level 3 (Erdgeschoss):** Subprozesse der Wertschöpfungskette

- **Subprozesse der Stromerzeugung:** Umfasst die verschiedenen Methoden der Stromerzeugung, sei es durch konventionelle Kraftwerke, erneuerbare Energien oder andere Quellen.
- **Subprozesse für den Netzbetrieb:** Verantwortlich für den reibungslosen Betrieb des Stromnetzes, die Steuerung der Energieströme und die Gewährleistung der Netzstabilität.
- **Subprozesse für das Lastmanagement:** Überwachung und Anpassung der Energieproduktion an die aktuelle Nachfrage, um Engpässe oder Überkapazitäten zu vermeiden.

■ **Level 4 (Untergeschoss):** Supportprozesse

- **Finanzmanagement:** Verwaltung der finanziellen Aspekte des Unternehmens und der Organisationseinheiten, einschliesslich Budgetierung, Buchführung und Abrechnung.
- **Personalmanagement:** Rekrutierung, Schulung und Verwaltung von Mitarbeitern, einschliesslich Sicherheits- und Gesundheitsrichtlinien.
- **IT-Management:** Verwaltung von Informationstechnologien, die für den Betrieb und die Steuerung des Energieversorgungssystems erforderlich sind.
- **Kundenkommunikation:** Kommunikation mit Endkunden über Stromtarife, Verbrauchsinformationen und kundenspezifische Anfragen.
- **Partnerschaften und Lieferantenkommunikation:** Kommunikation mit anderen Unternehmen und Organisationseinheiten, Regulierungsbehörden und Lieferanten für eine effiziente Zusammenarbeit und Einhaltung von Vorschriften.

- (3) Das Prozesshaus eines Stromversorgungsunternehmens und Stromversorgungsorganisationseinheiten bietet eine hierarchische Darstellung der wichtigsten Prozesse und ermöglicht es, die Wechselwirkungen zwischen den verschiedenen Ebenen zu verstehen. Es dient auch als Grundlage für die Integration von Informationstechnologien, um diese Prozesse effektiv zu unterstützen und zu steuern. Es ist wichtig zu beachten, dass die spezifische Struktur eines Prozesshauses je nach den individuellen Anforderungen und Gegebenheiten des jeweiligen Stromversorgungsunternehmens und Stromversorgungsorganisationseinheiten variieren kann.
- (4) Beispiel für das House of Processes für ein Unternehmen und Organisationseinheiten im Bereich Stromversorgung:



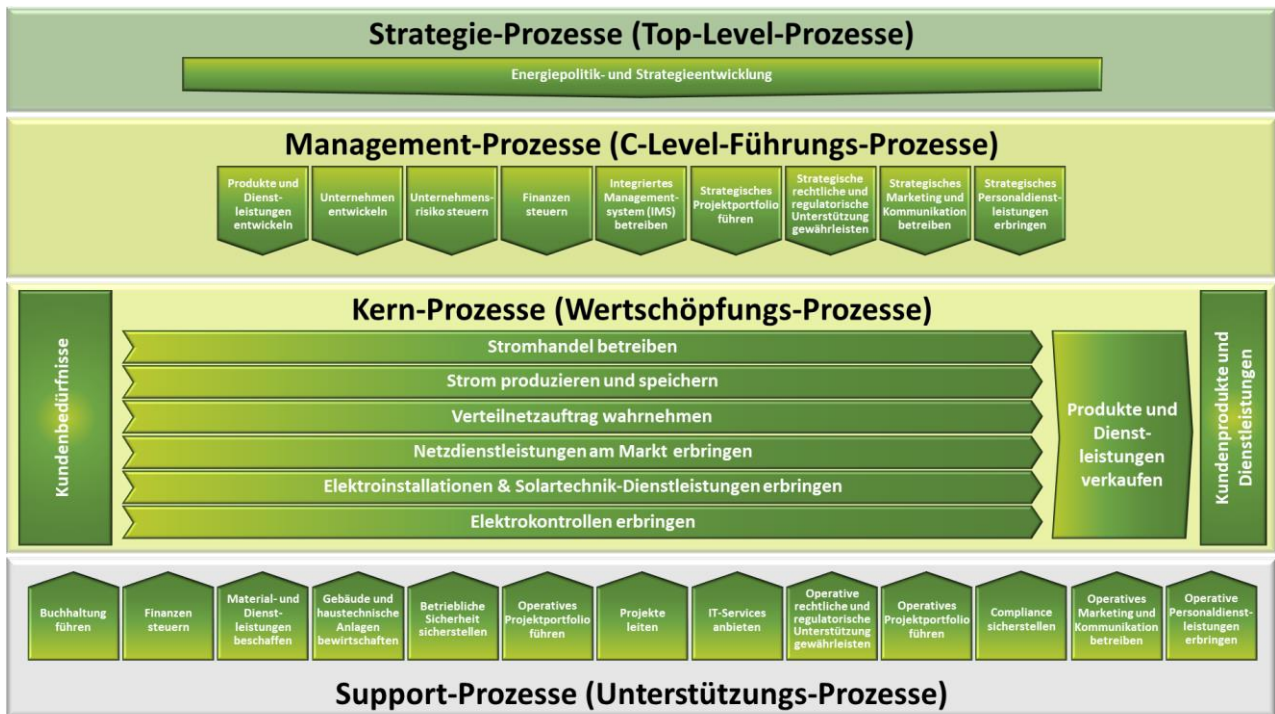


Abbildung 16: Prozesse im House of Processes (Quelle VSE)



**Empfehlung der VSE Cyber Security Task Force Experten:**

Der Miteinbezug des House of Policy des eigenen Unternehmens und Organisationseinheit hilft in verschiedenen Prozessen der Informationssicherheit um angemessene Abläufe, Bewertungen und ein Verständnis der Anforderungen an die IKT-Resilienz zu erhalten. Zum Beispiel bei der Bewertung von Risiken oder dem Aufbau eines Asset-Registers.





#### 5.4.8.2 Verantwortlichkeiten und Zuständigkeiten im House of Processes

- (1) Die Verantwortlichkeiten im House of Processes sind genau geregelt. Es ist definiert wer oder welche Rolle im Unternehmen und in den Organisationseinheiten für die Erstellung und Genehmigung der einzelnen Prozesse zuständig bzw. verantwortlich ist.

Level	Verantwortlich	Prozesstyp	Zielgruppe	Genehmigung durch
0	Verwaltungsrat (Konzernleitung)	Strategie-Prozesse	Konzern Gesamtes Unternehmen	
1	Geschäftsleitung, C-Level	Management- und Führung-prozesse	Gesamte Organisation / Unternehmen	Verwaltungsrat und/oder Konzernleitung
2	Geschäftsbereich- und Abteilungsleiter	Kern-Hauptprozesse in der Wertschöpfungskette	Geschäftsbereiche und Abteilungen	Geschäftsleitung, C-Level
3	Teams und Experten	Subprozesse in der Wertschöpfungskette	Operativ ausführende Teams inkl. Planung, Experten Engineers und Spezialisten	Geschäftsbereich- und Abteilungsleiter
4	Abteilungen, Teams und Experten	Support- und Unterstützungsprozesse	Spezifisch	Geschäftsleitung, C-Level, Geschäftsbereich- und Abteilungsleiter

**Tabelle 4:** Verantwortlichkeiten und Zuständigkeiten im House of Processes (Quelle VSE)

#### 5.4.9 Informationssicherheit: House of Policies

##### 5.4.9.1 Aufbau des House of Policies

- (1) Das "House of Policy" im Kontext eines Information Security Management Systems (ISMS) beschreibt die Struktur und Prozesse der Vorgaben zur Informationssicherheit. Ein ISMS ist ein ganzheitlicher Ansatz zur Verwaltung der Informationssicherheit in einer Organisation. Das "House of Policy" bildet dabei das Fundament dieses Ansatzes und besteht aus mehreren Leveln:
- **Level 0 (Dach):** Das höchste Level des "House of Policy" repräsentiert den Verwaltungsrat und die Konzernleitung (wenn vorhanden). Hier muss ein klares Statement zur Informationssicherheit abgegeben werden. Dadurch wird der Geschäftsleitung eine klare Vorgabe betreffend Steigerung der IKT-Resilienz gemacht. Auf diesem Level werden die strategischen Vorgaben definiert und es geht um das "Warum".
  - **Level 1 (Dachgeschoss):** Das Level 1 des "House of Policy" repräsentiert die Unternehmensleitung bzw. das Top-Management (C-Level) des Unternehmens. Hier werden die grundlegenden Prinzipien und strategischen Ziele für die Informationssicherheit festgelegt. Dies kann beinhalten, wie wichtig die Sicherheit von Informationen für das Unternehmen ist, wieviel Budget dafür bereitgestellt wird und welche Verantwortlichkeiten und Kompetenzen vorliegen. Auf diesem Level werden die strategischen Vorgaben auf das Unternehmen konkretisiert und festgehalten. Es geht um das "Warum". Dabei sollen alle Funktionen der Informationssicherheit abgebildet werden.
  - **Level 2 (Maisonette):** Dieser Level ist für die Entwicklung von konkreten Sicherheitsrichtlinien und -verfahren auf taktischer Ebene verantwortlich. Hier werden die allgemeinen taktische Vorgaben mittels Richtlinien und Guidelines betreffend Informationssicherheit und folglich Steigerung der IKT-Resilienz erstellt, die auf der strategischen Ausrichtung des Dachgeschosses basieren. Grundsätzlich wird auf dieser Ebene der Rahmen und der Geltungsbereich festgelegt. Es geht um "WAS" soll grundsätzlich gemacht werden. Dabei werden den Kategorien für die Informationssicherheit gebildet und definiert.
  - **Level 3 (Dachgeschoss):** Auf diesem Level werden operationelle Arbeitsanleitungen und Instructions erarbeitet. Es wird spezifisch auf alle spezifischen Gebiete und Themen der Informationssicherheit eingegangen. Sie umfassen Themen wie Schutz der Daten, Zugriffskontrolle, Passwörter, Datensicherung usw. anderen grundlegenden Sicherheitsaspekten. Als Grundsatz gilt: "Wie" soll etwas gemacht



werden. Dabei werden die nötigen Subkategorien mit den Checkpoints für die Informationssicherheit definiert.

- **Level 4 (Erdgeschoss):** Auf diesem Level werden die konkreten Anweisungen, Prozesse und Leitfäden entwickelt, die die Umsetzung der Arbeitsanleitungen und Instructions ermöglichen. Hier werden spezifische Massnahmen aus den Checkpoints festgelegt, wie beispielsweise die Implementierung von Firewalls, Intrusion Detection Systems, Verschlüsselung, die Erstellung und Umsetzung von Notfallplänen, Schulungen für Mitarbeiter, die Sicherung physischer Ressourcen und die Überwachung von Sicherheitsereignissen usw. Grundsätzlich wird auf diesem Level definiert, "Wie" etwas konkret gemacht werden soll.
  - **Level 5 (Fundament):** Das Fundament oder Level 5 des "House of Policy" repräsentiert die technischen Massnahmen und Sicherheitslösungen, die benötigt werden, um die Sicherheitsziele umzusetzen und den Nachweis dafür zu erbringen. Dies umfasst zum Beispiel Implantierung von Firewalls, Intrusion Detection Systems, Verschlüsselung und andere technische Sicherheitsmassnahmen.
- (2) Dabei werden im Level 0 bis 4 grundsätzlich Vorgaben erstellt und beschrieben. Diese Vorgaben können aber auch Nachweise enthalten, welche belegen, dass die Vorgaben vom höherliegenden Level verstanden und umgesetzt werden. Auf dem Level 5 sind die Nachweise für die Durchführung wie auch technische Dokumentationen für die Umsetzung.
- (3) Das "House of Policy" stellt eine hierarchische Struktur dar, die sicherstellt, dass die Informationssicherheitsziele der Organisation von der obersten Führungsebene bis zur technischen Umsetzung in der IT/OT-Infrastruktur durchgängig verfolgt und implementiert werden. Die verschiedenen Level sind eng miteinander verbunden und bauen aufeinander auf, um eine konsistente und effektive Informationssicherheitsstrategie sicherzustellen.



Abbildung 17: Prinzipieller Aufbau des House of Policy mit dem Mapping zum NIST CSF 1.1 (Quelle VSE)



#### Empfehlung der VSE Cyber Security Task Force Experten:

Für die Steigerung der IKT-Resilienz ist ein Aufbau, die Einführung und der Betrieb eines House of Policy zwingend erforderlich.



#### 5.4.9.2 Verantwortlichkeiten und Zuständigkeiten im House of Policies

- (1) Die Verantwortlichkeiten im House of Policy sind genau geregelt. Es ist definiert wer oder welche Rolle oder Funktion im Unternehmen und in den Organisationseinheiten für die Erstellung und Genehmigung der einzelnen Dokumente zuständig bzw. verantwortlich ist.

		Level	Verantwortlich	Policytyp	Zielgruppe	Genehmigung durch
Vorgaben     Nachweise	strategisch	0	Verwaltungsrat (Konzernleitung)	Politik	Konzern Gesamtes Unternehmen	
		1	Geschäftsleitung, C-Level	Weisungen, Direktiven	Gesamte Organisation / Unternehmen	Verwaltungsrat und/oder Konzernleitung
	taktisch	2	Chief Information Security Officer (CISO), Chief Risk Officer (CRO), Data Protection Officer (DPO)	Richtlinien, Guidelines	Gesamte Organisation / Unternehmen	Geschäftsleitung, C-Level
	operationell	3	Information Security Officer (ISO), Information Security Coordinator (ISC), Cyber Security Team	Arbeitsanleitungen, Instructions	Bereiche und Abteilungen	CISO, CRO, DPO
		4	Experten, Engineers, Spezialisten	Anweisungen, Prozesse und Leitfäden	Operativ ausführende Teams inkl. Planung, Experten Engineers und Spezialisten	ISO, ISC, Cyber Security-Team
		5	Anwender, Engineers, Spezialisten	Anleitungen, Beschreibungen und Dokumentationen usw.	Spezifisch	Review durch Experten, Engineers oder Spezialisten

**Tabelle 5:** Verantwortlichkeiten und Zuständigkeiten im House of Policy (Quelle VSE)

#### 5.4.9.3 Vorgaben und Nachweise



**Abbildung 18:** Vorgaben und Nachweise mit fließendem Übergang (Quelle VSE)

- (1) Bei den Vorgaben und Nachweisen ist keine klare Grenze zu ziehen. Da sich im gesamten House of Policy eine Vorgabe von einem Level durch untergestellten Level bestätigt bzw. der Nachweis erbracht wird, dass die Vorgabe verstanden und deren Umsetzung beschrieben ist. Dabei ist ein granularer Detaillierungsgrad anzuwenden. Grundsätzlich gilt immer wieder, dass im unterliegenden Dokument die Vorgaben detaillierter ausgearbeitet sind und somit auch der Nachweis erbracht wird, dass diese verstanden und umgesetzt werden.

#### 5.4.9.4 Dokumentenlenkung im House of Policy

- (1) Die Dokumentenlenkung ist ein wichtiger Bestandteil des Qualitätsmanagementsystems (QMS) in Unternehmen und Organisationseinheiten. Sie bezieht sich auf den Prozess der Erstellung, Aktualisierung, Genehmigung, Verteilung und Verwaltung von Dokumenten, um sicherzustellen, dass sie korrekt, aktuell und zugänglich sind. Hier ist eine Schritt-für-Schritt-Beschreibung der Dokumentenlenkung:
- **Dokumenterstellung und -änderung:** Zunächst werden Dokumente erstellt oder aktualisiert, um sicherzustellen, dass sie den aktuellen Anforderungen und Standards entsprechen. Dies kann Politiken, Weisungen, Direktiven, Richtlinien, Guidelines, Anweisungen, Prozess, Leitfäden, Verfahrensanweisungen, Arbeitsanweisungen, Qualitätsrichtlinien, Formulare, Berichte und andere Arten von Dokumenten umfassen.
  - **Kennzeichnung und Identifikation:** Jedes Dokument sollte eindeutig gekennzeichnet und identifiziert werden, um Verwechslungen zu vermeiden. Dies beinhaltet die Vergabe von Dokumentennamen, Versionsnummern und Erstellungs- oder Änderungsdaten.



- **Genehmigung und Autorisierung:** Dokumente, insbesondere solche, die kritisch für die Organisation sind, sollten genehmigt werden. Dies erfolgt in der Regel durch festgelegte Rollen oder Funktionen, die die Verantwortung für den Inhalt des Dokuments tragen.
- **Vertrieb und Zugriffskontrolle:** Genehmigte Dokumente sollten an die relevanten Mitarbeiter kommuniziert und wenn notwendig geschult werden. Zugriffsrechte und -kontrollen werden festgelegt, um sicherzustellen, dass nur autorisierte Personen auf die Dokumente zugreifen können.
- **Speicherung und Aufbewahrung:** Dokumente werden sicher gespeichert, um ihre Integrität und Vertraulichkeit zu gewährleisten. Dies kann physische Aufbewahrung (z. B. in Aktenordnern) oder elektronische Speicherung in einem Dokumentenmanagementsystem (DMS) umfassen.
- **Änderungsverfolgung:** Änderungen an Dokumenten werden nachverfolgt, um die Historie und den Verlauf der Dokumentenentwicklung zu dokumentieren. Dies umfasst die Angabe von Gründen für Änderungen und die Versionierung.
- **Rücknahmeprozess:** Wenn Dokumente nicht mehr benötigt werden oder obsolet sind, sollten sie zurückgezogen und archiviert oder ordnungsgemäss entsorgt werden.
- **Überprüfung und Überwachung:** Regelmässige Überprüfungen der Dokumente sind erforderlich, um sicherzustellen, dass sie aktuell und relevant bleiben. Dies kann im Rahmen von internen Audits oder Qualitätsprüfungen erfolgen.
- **Schulung und Bewusstsein:** Mitarbeiter sollten über die Dokumentenlenkungsverfahren informiert und geschult werden, um sicherzustellen, dass sie die Prozesse verstehen und befolgen.
- **Kommunikation:** Änderungen an Dokumenten und Aktualisierungen sollten kommuniziert werden, damit alle relevanten Parteien informiert sind.

- (2) Die Dokumentenlenkung trägt zur Sicherung der Qualität, Compliance und Effizienz in einer Organisation bei. Ein effektives Dokumentenlenkungssystem sorgt dafür, dass die richtigen Informationen zur richtigen Zeit den richtigen Personen zur Verfügung stehen und dass diese Informationen aktuell und genau sind.

#### 5.4.9.5 Übersicht der Dokumente im House of Policy zur Steigerung der IKT Resilienz auf Level 0 - 3

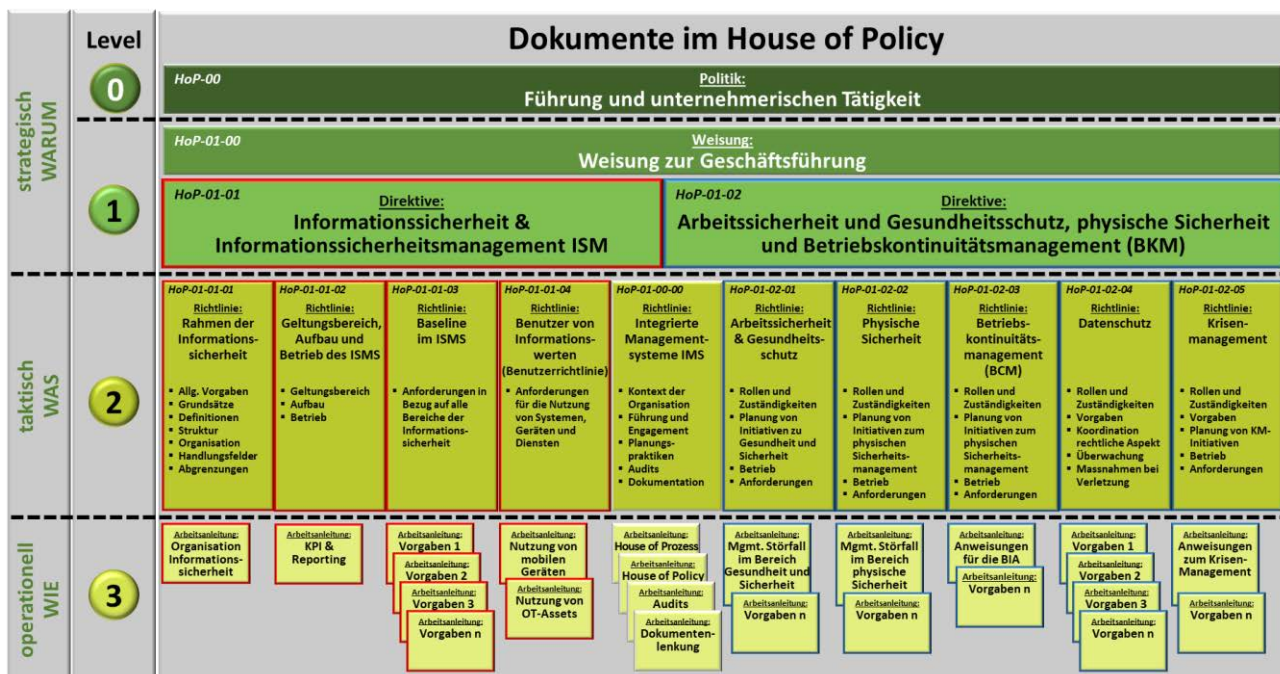


Abbildung 19: Dokumente im House of Policy auf Level 0 bis 3 (Quelle VSE)



In diesem Leitfaden wird im House of Policy der Level 0 bis 3 beschrieben. Im Anhang befindet sich eine Beschreibung der aus Sicht VSE notwendigen Vorgaben. In den Beilagen finden sich Beispiele für die Firma STROM AG, welche als Vorlagen oder Hilfe zur Erstellung der Dokumente verwendet werden können.



In den Beilagen gibt es Musterbeispiele, welche angewendet werden können.





#### 5.4.9.6 Mapping des House of Policies mit dem NIST CSF 1.1

- (1) Das NIST Cyber-Security-Framework weist vier Ebenen auf, in welchen systematisch die Steigerung der IKT-Resilienz in verschiedenen Detaillierungsgraden darstellt wird. Je tiefer die Ebenen sind, desto detaillierter und konkreter wird auf die einzelnen Massnahmen zur Steigerung der IKT-Resilienz eingegangen.

		Level	Verantwortlich	Policytyp	NIST CSF 1.1 Ebenen	
Vorgaben	Strategisch "WARUM"	0	Verwaltungsrat (Konzernleitung)	Politik	Framework	Grundsätzlich soll in der Informationssicherheitspolitik verankert sein, dass ein Rahmenwerk wie das NIST CSF 1.1 zur Steigerung der IKT-Resilienz verwendet werden soll.
		1	Geschäftsleitung, C-Level	Leitlinien, Weisungen	Funktionen ID. PR. DE. RS. RE.	In der Informationssicherheitsstrategie und den spezifischen Weisungen muss auf die einzelnen Funktionen des NIST CSF 1.1 (ID=Identify, PR=Protect, DE=Detect, RS = Response und RE=Recover) Bezug genommen werden. Es ist sicherzustellen, dass alle Funktionen entsprechen behandelt und die entsprechenden Vorgaben einfließen.
	Taktisch "WAS"	2	Chief Information Security Officer (CISO), Chief Risk Officer (CRO), Data Protection Officer (DPO)	Richtlinien, Guidelines	Kategorien ID. PR. DE. RS. RE.	In den Richtlinien und Guidelines müssen alle Punkte auf der Ebene Kategorie im NIST CST behandelt werden. Es kann Bezug auf die Ebene Funktion gemacht werden. Dabei ist es zwingend erforderlich, dass alle Punkte auf der Ebene Kategorie umschrieben und definiert sind.
		3	Information Security Officer (ISO), Information Security Coordinator (ISC), Cyber Security Team	Arbeitsanleitungen, Instructions	Checkpoints (Subkategorie) ID. PR. DE. RS. RE.	In Arbeitsanleitungen und Instructions sind im Detaillierungsgrad mindestens bis NIST CSF 1.1 Ebene Subkategorie einzugehen. Es kann Bezug oder Referenz auf die oberen oder unteren Ebenen gemacht werden, wenn dies zur Verständlichkeit hilft.
	Operationell "WIE"	4	Experten, Engineers, Spezialisten	Anweisungen, Prozesse und Leitfäden	Massnahmen aus Referenzen ID. PR. DE. RS. RE.	Für die Nachweise sollen die Referenzen im NIST CSF 1.1 beigezogen werden. Es kann auch auf die oberen Ebenen im NIST CSF 1.1 verwiesen werden. Weiter sind auch hilfreiche Dokumente in unzähliger Form vorhanden. In diesem Leitfaden sind einige Beispiele aufgelistet.
		5	Anwender, Engineers, Spezialisten	Anleitungen, Beschreibungen und Dokumentationen usw.		

**Tabelle 6:** Mapping House of Policy mit den Ebenen im NIST CSF 1.1

- (2) Grundsätzlich muss jeder Punkt im NIST Cyber Security Framework CSF 1.1 in den Vorgabedokumenten im House of Policy auf den Layern 0 bis 3 abgebildet werden. Mindestens hat dies bis auf Stufe Checkpoint (Subkategorie) zu erfolgen. Zusätzlich können auch Referenzen oder Punkte aus den aufgeführten Referenzen einfließen.



Im "VSE-NIST-CSF-1.1\_HoP-Mapping-Tool" können im Vorfeld zur Erstellung der Dokumente die einzelnen Elemente des NIST CSF 1.1 zu den Dokumenten im House of Policy zugewiesen werden.



**Empfehlung der VSE Cyber Security Task Force Experten:**  
Durch das Mapping der NIST CSF 1.1 Elementen zu den Dokumenten im House of Policy wird sichergestellt, dass alle Punkte zugeordnet und behandelt werden.





#### 5.4.9.7 Mapping der ISO 27001:2022 Annex A mit den Dokumenten im House of Policy

- (1) Grundsätzlich soll jeder gemäss ISO 27001:2022 Annex A in den Vorgabedokumenten im House of Policy auf den Leveln 0 bis 3 abgebildet werden. Dies hat mindestens bis auf Stufe Subkategorie zu erfolgen. Zusätzlich können auch Referenzen oder Punkte aus den aufgeführten Massnahmen nach ISO 27002:2022 einfließen.



Im "VSE-ISO27002-Annex-A\_HoP-Mapping-Tool" können im Vorfeld zur Erstellung der Dokumente die einzelnen Elemente der ISO27001:2022 Annex A zu den Dokumenten im House of Policies zugewiesen werden.



**Empfehlung der VSE Cyber Security Task Force Experten:**  
Durch das Mapping der ISO 27001 Annex A zu den Dokumenten im House of Policy wird sichergestellt, dass alle Punkte zugeordnet und behandelt werden.



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**

#### 5.4.9.8 Aufgelistete Vorgaben und Nachweise im House of Policy



In diesem Leitfaden sind nur die Vorgaben und Nachweise aufgelistet, welche im direkten Zusammenhang mit dem House of Policy für die Informationssicherheit stehen. Die Auflistung ist dabei nicht abschliessend und kann jederzeit durch zusätzliche Dokumente erweitert werden. Die Namensdefinition bzw. Bezeichnung für die einzelnen Dokumentenarten wurden an die aktuellen Vorgaben in verschiedenen Frameworks und Standards angelehnt, sie können aber je nach Unternehmen oder Organisationseinheiten und deren Definitionen variieren. Wichtig ist jedoch, dass die Bezeichnung und Funktion der Dokumentenarten im gesamten Unternehmen und Organisationseinheiten angewendet wird.

#### 5.4.10 Information Security Management System (ISMS)

- (1) Ein Information Security Management System (ISMS) ist ein strukturiertes und ganzheitliches Rahmenwerk, das dazu dient, die Informationssicherheit in einem Unternehmen und in den Organisationseinheiten zu managen. Es umfasst Richtlinien, Prozesse, Technologien und Massnahmen, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten. Das ISMS berücksichtigt dabei sowohl technologische als auch organisatorische Aspekte, und es orientiert sich an internationalen Standards wie ISO/IEC 27001. Ziel ist es, Risiken zu identifizieren, zu bewerten und zu behandeln, um die IKT-Infrastruktur widerstandsfähiger gegenüber Bedrohungen zu machen. Durch kontinuierliche Überwachung, Schulungen und Anpassungen trägt das ISMS dazu bei, die Informationssicherheit auf einem angemessenen Niveau zu gewährleisten und den Schutz sensibler Daten sicherzustellen.

##### 5.4.10.1 Gründe für den Aufbau eines ISMS:

- (1) Ein Information Security Management System (ISMS) ist von entscheidender Bedeutung für Unternehmen und Organisationseinheiten, da es dazu dient, die Informationssicherheit zu gewährleisten und zu verbessern. Nachfolgend sind einige Gründe aufgeführt, warum ein ISMS wichtig ist:
  - **Schutz sensibler Informationen:** Ein ISMS hilft dabei, vertrauliche und sensible Informationen vor unbefugtem Zugriff, Diebstahl oder Datenverlust zu schützen. Dies ist besonders wichtig, da Daten heute zu den wertvollsten Vermögenswerten vieler Unternehmen und Organisationseinheiten gehören.
  - **Einhaltung gesetzlicher Vorschriften:** In vielen Ländern und Branchen gibt es gesetzliche Vorschriften und Datenschutzbestimmungen, die Unternehmen und Organisationseinheiten einhalten müssen. Ein ISMS ermöglicht es, diese Anforderungen zu erfüllen und rechtliche Konsequenzen zu vermeiden.
  - **Vertrauen der Kunden:** Eine robuste Informationssicherheit vermittelt Kunden und Partnern Vertrauen. Unternehmen und Organisationseinheiten, die nachweislich sicher mit Daten umgehen, können Kunden gewinnen und halten.
  - **Risikomanagement:** Ein ISMS hilft bei der Identifizierung, Bewertung und Minderung von Sicherheitsrisiken. Dies ermöglicht es der Organisation, potenzielle Bedrohungen proaktiv zu bewältigen.



- **Kontinuität und Widerstandsfähigkeit:** Das ISMS unterstützt die Entwicklung von Notfall- und Wiederherstellungsplänen, um sicherzustellen, dass die Organisation auch nach Sicherheitsvorfällen oder Katastrophen ihren Betrieb aufrechterhalten kann.
  - **Effizienz und Produktivität:** Die Implementierung von Sicherheitsrichtlinien und -verfahren kann die Effizienz in der Organisation steigern, da Mitarbeiter wissen, wie sie sicher mit Informationen umgehen sollen.
  - **Kosteneinsparungen:** Durch die Vorbeugung von Sicherheitsvorfällen und Datenverlusten können Unternehmen und Organisationseinheiten erhebliche Kosten für die Bewältigung von Vorfällen und den Wiederaufbau von Ruf und Vertrauen einsparen.
  - **Bewährte Praktiken und Standards:** Ein ISMS kann auf internationalen Standards wie ISO 27001 basieren, was bewährte Praktiken und Rahmenbedingungen für die Informationssicherheit bietet.
  - **Kontinuierliche Verbesserung:** Das ISMS fördert die kontinuierliche Verbesserung der Informationssicherheit. Unternehmen und Organisationseinheiten können ihre Sicherheitsmassnahmen basierend auf den gesammelten Daten und Erfahrungen ständig weiterentwickeln.
  - **Reputations- und Wettbewerbsvorteil:** Unternehmen und Organisationseinheiten, die nachweislich robuste Sicherheitspraktiken implementieren, können ihre Reputation und ihre Wettbewerbsfähigkeit steigern, da sie als zuverlässige Partner angesehen werden.
- (2) In einer Zeit, in der Cyberangriffe und Datenschutzverletzungen alltäglich sind, ist ein ISMS ein wichtiger Bestandteil der Geschäftsstrategie. Es hilft, das Risiko zu minimieren, den Betrieb aufrechtzuerhalten und das Vertrauen der Stakeholder zu gewinnen.

#### 5.4.10.2 Der Aufbau eines ISMS

- (1) Ein Information Security Management System (ISMS) ist eine systematische und strukturierte Herangehensweise zur Verwaltung und Sicherung von Informationen in einer Organisation. Der Aufbau eines ISMS erfolgt in mehreren Schritten, ein bewährter Rahmen dafür ist der in der ISO 27001 Standard beschriebene Plan-Do-Check-Act (PDCA)-Zyklus. Nachfolgend ist eine Übersicht über den Aufbau eines ISMS:
- **Festlegung des Rahmens:** Begonnen wird mit der Festlegung des Anwendungsbereichs und der Ziele des ISMS. Bestimmen Sie, welche Informationen geschützt werden müssen, und identifizieren Sie die relevanten rechtlichen und regulatorischen Anforderungen.
  - **Führung und Unterstützung:** Das Top-Management muss das ISMS unterstützen und Verantwortlichkeiten für die Informationssicherheit festlegen.
  - **Risikobewertung:** Identifizieren und bewerten Sie die Risiken für die Informationssicherheit. Dies beinhaltet die Analyse von Bedrohungen, Schwachstellen und potenziellen Auswirkungen auf die Organisation.
  - **Planung:** Entwickeln Sie Sicherheitsrichtlinien, -ziele und -verfahren, um die identifizierten Risiken zu behandeln. Erstellen Sie auch einen Plan zur Umsetzung des ISMS.
  - **Umsetzung und Betrieb:** Implementieren Sie die Sicherheitsrichtlinien und -verfahren in der gesamten Organisation. Dies umfasst Schulungen, Sicherheitsmassnahmen und die Festlegung von Verantwortlichkeiten.
  - **Überwachung und Bewertung:** Überwachen Sie kontinuierlich die Wirksamkeit des ISMS. Erfassen Sie Sicherheitsvorfälle, führen Sie interne und externe Audits durch und bewerten Sie die umgesetzten Massnahmen.
  - **Kontinuierliche Verbesserung:** Basierend auf den Ergebnissen der Überwachung und Messung ergreifen Sie Massnahmen zur kontinuierlichen Verbesserung des ISMS. Dies kann die Anpassung von Richtlinien, Verfahren und Schulungen beinhalten.
  - **Bewertung durch die Geschäftsleitung:** Das Top-Management sollte das ISMS regelmässig überprüfen, um sicherzustellen, dass es effektiv ist und den geschäftlichen Anforderungen entspricht.
  - **Dokumentation und Aufzeichnungen:** Erstellen Sie Dokumentation und Aufzeichnungen, die die Einhaltung der Sicherheitsrichtlinien und -verfahren belegen.
  - **Schulung und Sensibilisierung:** Schulen Sie Mitarbeiter und erhöhen Sie das Bewusstsein für Informationssicherheit in der gesamten Organisation.



- **Kommunikation und Berichterstattung:** Kommunizieren Sie die Fortschritte und Ergebnisse des ISMS an das Top-Management und alle relevanten Stakeholder.
- (2) Die Implementierung eines ISMS nach internationalen Standards wie ISO 27001 kann hilfreich sein, um bewährte Praktiken zu implementieren und die Wirksamkeit des ISMS zu bewerten. Der ISMS-Aufbau ist ein iterativer Prozess, bei dem die Organisation ständig lernt und sich verbessert, um mit verändernden Bedrohungen und Anforderungen Schritt halten zu können.



Es wird mit Nachdruck von den VSE Cyber Security Task Force Experten empfohlen, ein ISMS zur Steigerung der IKT-Resilienz einzuführen.

#### 5.4.10.3 ISMS nach ISO 27001

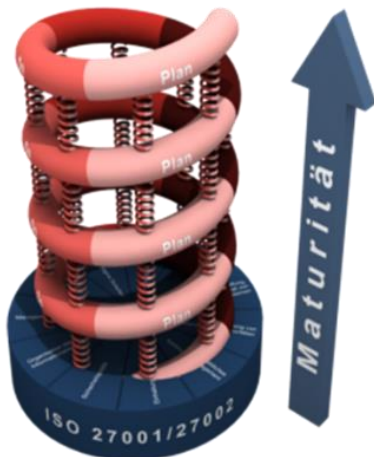


Abbildung 20: Maturitätsspirale des ISMS

(1) Ein Information Security Management System (ISMS) nach ISO 27001 ist ein Rahmenwerk, das entwickelt wurde, um die Informationssicherheit in einer Organisation zu gewährleisten, zu überwachen, zu verwalten und kontinuierlich zu verbessern. Die ISO 27001 ist eine international anerkannte Norm für Informationssicherheit und legt die Anforderungen für den Aufbau, die Umsetzung und den Betrieb eines ISMS fest. Hier sind die Schlüsselkomponenten eines ISMS nach ISO 27001:

- **Politik für die Informationssicherheit:** Die Organisation entwickelt eine formale Informationssicherheitspolitik, die die Verpflichtung der Geschäftsleitung zur Informationssicherheit zum Ausdruck bringt.
- **Festlegung des Anwendungsbereichs:** Die Organisation bestimmt den Anwendungsbereich des ISMS, einschliesslich der relevanten Assets und Prozesse, die abgedeckt werden sollen.

- **Risikobewertung und Risikobehandlung:** Eine umfassende Risikobewertung wird durchgeführt, um Bedrohungen, Schwachstellen und Risiken für die Informationssicherheit zu identifizieren. Auf Grundlage dieser

Bewertung werden angemessene Kontrollen und Massnahmen zur Risikominderung ausgewählt und umgesetzt.

- **Sicherheitsrichtlinien und -verfahren:** Die Organisation entwickelt und dokumentiert Sicherheitsrichtlinien und -verfahren, die die Einhaltung der Sicherheitsanforderungen sicherstellen.
- **Management-Unterstützung:** Das Top-Management engagiert sich für das ISMS und stellt die erforderlichen Ressourcen bereit.
- **Kontrolle der Dokumentation:** Die Dokumentation, einschliesslich Sicherheitsrichtlinien, -verfahren und Aufzeichnungen, wird erstellt, verwaltet und kontrolliert.
- **Kommunikation und Bewusstsein:** Die Organisation kommuniziert die Sicherheitsrichtlinien und -verfahren an die Mitarbeiter und sorgt für Schulungen und Sensibilisierung zur Informationssicherheit.
- **Überwachung und Überprüfung:** Die Leistung des ISMS wird regelmässig überwacht, und interne Audits werden durchgeführt, um die Wirksamkeit der Sicherheitsmassnahmen zu überprüfen.
- **Ständige Verbesserung:** Basierend auf den Überwachungs- und Überprüfungsergebnissen werden kontinuierliche Verbesserungen vorgenommen, um die Informationssicherheit zu optimieren.
- **Notfall- und Wiederherstellungsplanung:** Die Organisation entwickelt Pläne zur Wiederherstellung von Systemen und Daten im Falle von Sicherheitsvorfällen oder Katastrophen.
- **Externe Prüfung und Zertifizierung:** In einigen Fällen kann die Organisation sich einer unabhängigen Prüfung und Zertifizierung unterziehen, um die Einhaltung der ISO 27001-Norm nachzuweisen.

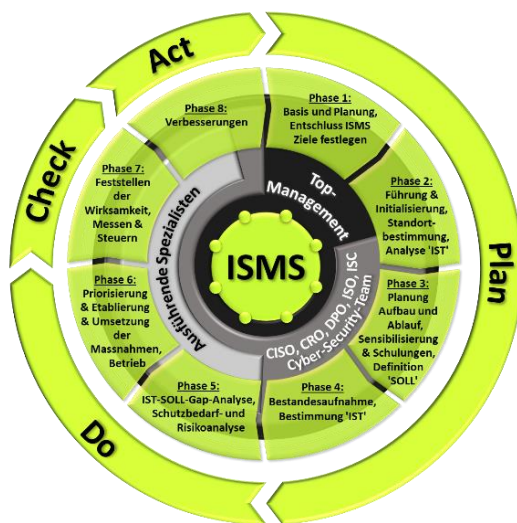
- (2) Ein ISMS nach ISO 27001 bietet einen systematischen Ansatz zur Informationssicherheit und ermöglicht es Unternehmen und Organisationseinheiten, Risiken zu minimieren, die Sicherheit zu erhöhen und das Vertrauen der Stakeholder zu gewinnen. Die Umsetzung und Aufrechterhaltung eines ISMS erfordert die Zusammenarbeit verschiedener Unternehmens- und Organisationseinheitenbereiche und die kontinuierliche Überwachung und Aktualisierung, um mit ändernden Bedrohungen und Anforderungen Schritt halten zu können.





**Empfehlung der VSE Cyber Security Task Force Experten:**  
Es wird empfohlen ein ISMS nach ISO 27001 mit anschliessender Zertifizierung einzuführen.

#### 5.4.10.4 Die VSE Phasen für die Einführung eines ISMS



**Abbildung 21:** VSE-Phasen für die Einführung des ISMS (Quelle VSE)

(1) Die Einführung eines Information Security Management Systems (ISMS) ist ein strategischer Prozess, der darauf abzielt, die Sicherheit von Informationen in einer Organisation zu gewährleisten und kontinuierlich zu verbessern. Diese Einführung erfolgt in mehreren aufeinanderfolgenden Phasen:

(2) Die Initiierung bildet den Ausgangspunkt. Hier wird die Notwendigkeit eines ISMS erkannt und akzeptiert. Dies kann durch externe gesetzliche Anforderungen, Kundenbedürfnisse oder interne Risikobewertungen motiviert sein. Die oberste Führungsebene verpflichtet sich, das ISMS zu unterstützen.

(3) Anschliessend erfolgt die Kontextanalyse, bei der interne und externe Faktoren, die die Informationssicherheit beeinflussen könnten, identifiziert werden. Dies beinhaltet die Bestimmung von Stakeholdern, relevanten Gesetzen und Vorschriften sowie anderen Rahmenbedingungen.

- (4) Die Unternehmensführung setzt klare Rollen, Verantwortlichkeiten und Befugnisse im Zusammenhang mit der Informationssicherheit fest. Das Top Management verpflichtet sich formell, das ISMS zu unterstützen, um die Integration von Informationssicherheit in die Unternehmenskultur zu fördern.
- (5) In der Planungsphase wird ein detaillierter Plan für das ISMS erstellt. Dies umfasst eine umfassende Risikobewertung zur Identifikation von Bedrohungen und Schwachstellen. Sicherheitsziele und -Massnahmen werden entwickelt, um das Risiko auf ein für das Unternehmen und die Organisationseinheiten akzeptables Niveau zu reduzieren.
- (6) Die Umsetzungsphase beinhaltet die konkrete Implementierung der in der Planung entwickelten Massnahmen. Dies umfasst die Einführung von Sicherheitsrichtlinien, Schulungen für Mitarbeiter, die Implementierung von Sicherheitskontrollen und die Einrichtung von Überwachungssystemen.
- (7) Die Überwachung und Messung sind entscheidend, um sicherzustellen, dass die definierten Sicherheitsziele erreicht werden. Interne und externe Audits sowie regelmässige Überprüfungen gewährleisten, dass die festgelegten Prozesse effektiv sind und kontinuierlich verbessert werden können.
- (8) Die Bewertung der Leistung analysiert die gesammelten Daten, um die Wirksamkeit des ISMS zu bewerten. Diese Phase identifiziert auch Verbesserungsmöglichkeiten, die darauf abzielen, die Sicherheitspraktiken und -prozesse zu optimieren.
- (9) Die kontinuierliche Verbesserung wird umgesetzt, basierend auf den Ergebnissen der Bewertung. Dies kann die Anpassung von Prozessen, die Einführung neuer Technologien oder Schulungen der Mitarbeiter umfassen.
- (10) Die Managementbewertung durch die oberste Führungsebene erfolgt regelmässig. Sie überprüft die Effektivität des ISMS im Hinblick auf die geschäftlichen Ziele und strategischen Ausrichtungen der Organisation. Anpassungen werden vorgenommen, um sicherzustellen, dass das ISMS weiterhin den Anforderungen entspricht.
- (11) Die Einführung eines ISMS ist somit ein zyklischer Prozess, der darauf abzielt, Informationssicherheit als integralen Bestandteil der Unternehmenskultur zu etablieren und kontinuierlich zu verbessern.
- (12) Das Vorgehen für die Einführung des ISMS wird in den folgenden Kapiteln umfassend beschrieben.





#### 5.4.11 Informationssicherheit: NIST CSF Version 1.1



Abbildung 22 NIST Cybersecurity Framework

(1) Das NIST Cybersecurity Framework (CSF) ist ein Rahmenwerk der National Institute of Standards and Technology (NIST) der USA, das Unternehmen und Organisationseinheiten bei der Entwicklung und Verbesserung ihrer Cybersecurity unterstützt. Das Framework wurde entwickelt, um als freiwilliges Instrument für Unternehmen und Organisationseinheiten jeder Grösse und Branche zu dienen. Es besteht aus fünf zentralen Funktionen: "Identify," "Protect," "Detect," "Respond," und "Recover."

(2) Die "Identify"-Funktion zielt darauf ab, die grundlegenden Bestandteile der Cybersecurity-Risiken zu verstehen. Dies umfasst die Identifikation von Assets, Bedrohungen und Schwachstellen sowie die Festlegung von Schutzzielen und Prioritäten.

(3) In der "Protect"-Funktion werden Massnahmen ergriffen, um die erkannten Risiken zu begrenzen oder zu kontrollieren. Dies beinhaltet den Schutz von Systemen, Daten und Prozessen durch Sicherheitskontrollen, Schulungen und Sicherheitsbewusstsein der

Mitarbeiter.

- (4) Die "Detect"-Funktion konzentriert sich darauf, Anomalien und Sicherheitsvorfälle frühzeitig zu identifizieren. Hierzu werden Überwachungsmechanismen, Intrusion Detection Systems (IDS) und andere Technologien eingesetzt, um ungewöhnliche Aktivitäten zu erkennen.
- (5) Bei der "Respond"-Funktion steht die rasche Reaktion auf Sicherheitsvorfälle im Vordergrund. Unternehmen und Organisationseinheiten entwickeln klare Reaktionspläne, um auf Cyberangriffe oder andere Sicherheitsvorfälle effektiv reagieren zu können. Dies beinhaltet auch die Zusammenarbeit mit externen Partnern und Behörden.
- (6) Die "Recover"-Funktion adressiert die Fähigkeit einer Organisation, nach einem Sicherheitsvorfall wieder rasch möglichst in den Normalbetrieb überzugehen. Das beinhaltet die Implementierung von Wiederherstellungsplänen, die Evaluierung der Wirksamkeit von Massnahmen und die Anpassung der Recoverystrategien auf Grund von Erkenntnissen bei Vorfällen.
- (7) Das NIST CSF bietet einen flexiblen Rahmen, der es Unternehmen und Organisationseinheiten ermöglicht, ihre eigene Cybersecurity-Strategie zu entwickeln und anzupassen. Es wird weltweit als bewährte Methode anerkannt, um die IKT-Resilienz von Unternehmen und Organisationseinheiten zu stärken und die steigenden Herausforderungen im Bereich der Cybersecurity effektiv anzugehen.



**Im Strom VV wurde der IKT-Minimalstandard verpflichtet. Somit muss das NIST-Framework angewendet werden.**

#### 5.4.12 Informationssicherheit: Vernetzung des ISMS mit dem NIST CSF 1.1

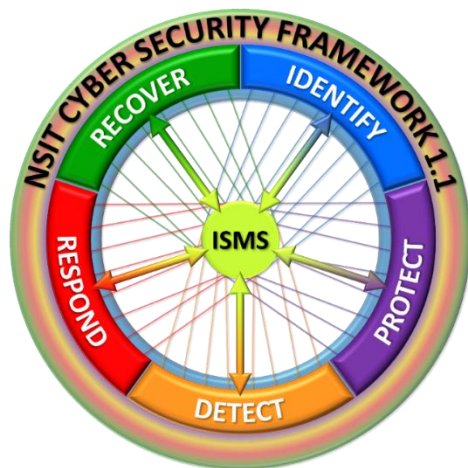


Abbildung 23: Vernetzung ISMS mit NIST CSF

(1) Die Vernetzung Information Security Management Systems (ISMS) mit dem NIST Cybersecurity Framework (CSF) macht Sinn, da sie eine umfassende und ausgewogene Sicherheitsstrategie ermöglicht. Während das ISMS eine breite Palette von Sicherheitsaspekten abdeckt, bietet das NIST CSF einen spezifischen Fokus auf die Herausforderungen der Cybersecurity. Die Integration ermöglicht es Unternehmen und Organisationseinheiten, sowohl eine robuste allgemeine Sicherheitspraxis zu entwickeln als auch gezielte Massnahmen zur Absicherung gegen Cyberbedrohungen zu implementieren.

(2) Das ISMS bietet einen Rahmen für das Risikomanagement und die Umsetzung bewährter Praktiken, während das NIST CSF konkrete Leitlinien für die Cybersecurity bereitstellt. Die Kombination verbessert die Flexibilität und Anpassungsfähigkeit, da Unternehmen und Organisationseinheiten die spezifischen Anforderungen des NIST CSF in ihr ISMS integrieren können.





- (3) Durch diese Vernetzung können Unternehmen und Organisationseinheiten nicht nur ihre Informationssicherheit stärken, sondern auch effektiv auf die dynamischen und sich ständig verändernden Bedrohungen im digitalen Umfeld reagieren.
- (4) Hier sind einige Möglichkeiten, wie ein ISMS mit dem NIST CSF vernetzt werden kann:
- **Risikobewertung und -management:** Das ISMS bietet eine umfassende Methode zur Identifikation, Bewertung und Kontrolle von Risiken. Diese Prozesse können nahtlos in die Risikobewertungskomponente des NIST CSF integriert werden, um eine konsistente und ganzheitliche Sicht auf Risiken zu gewährleisten.
  - **Schutz und Verteidigung:** Das ISMS enthält bereits bewährte Praktiken und Kontrollen zur Sicherung von Systemen und Daten. Diese Kontrollen können mit den Schutz- und Verteidigungspraktiken des NIST CSF abgeglichen werden, um sicherzustellen, dass die Schutzebenen umfassend und effektiv sind.
  - **Ereigniserkennung und Reaktion:** Das ISMS enthält keine Prozesse zur Erkennung von Sicherheitsvorfällen und zur Reaktion auf diese. Diese können mit den Komponenten des NIST CSF zur Erkennung und Reaktion auf Sicherheitsvorfälle integriert werden, um sicherzustellen, dass Bedrohungen zeitnah erkannt und angemessen behandelt werden.
  - **Kommunikation und Koordination:** Das ISMS kann die interne Kommunikation und Koordination von Sicherheitsaktivitäten unterstützen. Diese Aktivitäten können in die Kommunikations- und Koordinationskomponenten des NIST CSF integriert werden, um sicherzustellen, dass Informationen über Sicherheitsvorfälle effektiv geteilt werden.
  - **Überwachung und Verbesserung:** Beide Frameworks betonen die Bedeutung von Überwachung und kontinuierlicher Verbesserung. Die Überwachung von ISMS-Metriken kann in die Überwachungs- und Verbesserungskomponenten des NIST CSF integriert werden, um sicherzustellen, dass die Sicherheitsleistung kontinuierlich bewertet und optimiert wird.
  - **Risikokommunikation:** Die Kommunikation von Cyber-Risiken und -Massnahmen an Geschäftsleitung und Stakeholder ist entscheidend. Ein ISMS kann die Grundlage für die Kommunikation von Risiken bilden und sich nahtlos in die Kommunikations- und Koordinationskomponente des NIST CSF integrieren.
- (5) Die Integration eines ISMS mit dem NIST CSF ermöglicht eine umfassende Herangehensweise an die Informationssicherheit, bei der bewährte Praktiken und Methoden beider Frameworks kombiniert werden. Es stellt sicher, dass die Organisation die umfassenden Anforderungen der Informationssicherheit und der Cybersecurity erfüllt und dabei die Flexibilität und Anpassungsfähigkeit behält, um auf sich ändernde Bedrohungen und Risiken reagieren zu können.



Abbildung 24 Zusammenarbeit (Quelle allegria Blog)

#### 5.4.13 Informationssicherheit: Zusammenarbeit

(1) Die Zusammenarbeit zur Steigerung der IKT-Resilienz ist entscheidend, um sicherzustellen, dass IKT-Systeme und -Infrastrukturen widerstandsfähig gegen Störungen und Bedrohungen sind. Die IKT-Resilienz bezieht sich auf die Fähigkeit von IKT-Systemen, sich von Störungen zu erholen, schnell wiederhergestellt zu werden und den Geschäftsbetrieb aufrechtzuerhalten zu können. Hier sind einige wichtige Aspekte der Zusammenarbeit zur Steigerung der IKT-Resilienz:

- **Zusammenarbeit mit Gesetzgebern, Behörden und Regulatoren:** Die Zusammenarbeit mit den gesetzlichen Vertretern und Behörden ist interdisziplinäre zwingend erforderlich. So kann auf aktuelle Bedrohungen eingegangen und reagiert werden. Vorgaben, Ergänzungen und Anpassungen zur Steigerung der IKT-Resilienz können so zusammen realistisch und zeitnah aufgearbeitet, übernommen und umgesetzt werden.
- **Zusammenarbeit in der Branche:** Eine nationale und internationale branchenweite Zusammenarbeit ist für die Steigerung der IKT-Resilienz essenziell und muss zwingend gefördert und gepflegt werden. Nur so können Branchenstandards entstehen, überarbeitet werden und finden eine breite Abstützung.



- **Zusammenarbeit mit Lieferanten, Hersteller und Dienstleister:** Die Zusammenarbeit mit den Lieferanten, Herstellern und Dienstleister ist zwingend erforderlich. So kann die IKT-Resilienz in den einzelnen Systemen erhöht und auf aktuelle Bedrohungen in den Systemen zeitnah reagiert werden.
  - **Interdisziplinäre Teams:** IKT-Resilienz erfordert die Zusammenarbeit von Experten aus verschiedenen Bereichen. Dies umfasst IT-Experten, Sicherheitsfachleute, Notfallmanagement-Teams und Vertreter aus anderen relevanten Abteilungen wie Personalwesen, Rechtsabteilung und Risikomanagement.
  - **Risikobewertung und -management:** Ein gemeinsames Verständnis der Risiken und Bedrohungen für die IKT-Systeme ist entscheidend. Interdisziplinäre Teams sollten Risikobewertungen durchführen, um die spezifischen Schwachstellen und Bedrohungen zu identifizieren und Massnahmen zur Risikominimierung zu entwickeln.
  - **Notfallvorsorge und -reaktion:** Teams sollten Notfallvorsorgepläne entwickeln, um auf unerwartete Störungen vorbereitet zu sein. Dies umfasst die Identifizierung kritischer IKT-Systeme, die Entwicklung von Notfallplänen und die Schulung von Mitarbeitern, wie sie im Falle eines Ausfalls reagieren sollen.
  - **Kontinuitätsplanung:** Kontinuitätspläne können nur interdisziplinär erstellt werden. Diese Pläne beschreiben, wie der Geschäftsbetrieb aufrechterhalten wird, selbst wenn IKT-Systeme beeinträchtigt sind. Dies kann die Nutzung von Backup-Systemen, Cloud-Services und anderen Wiederherstellungsmechanismen umfassen.
  - **Sicherheitsmassnahmen:** IKT-Resilienz beinhaltet auch die Umsetzung von Sicherheitsmassnahmen, um die Systeme vor Bedrohungen zu schützen. Sicherheitsteams sollten eng mit IKT-Resilienz Teams zusammenarbeiten, um sicherzustellen, dass Schutzmassnahmen in den Resilienz Plänen integriert sind.
  - **Technologie und Infrastruktur:** IKT-Teams müssen die IKT-Infrastruktur überwachen und sicherstellen, dass sie widerstandsfähig gegenüber Ausfällen ist. Dies kann Hochverfügbarkeitslösungen, Redundanz und regelmässige Wartung umfassen.
  - **Schulung und Bewusstseinsbildung:** Mitarbeiter aus verschiedenen Abteilungen und Bereichen sollten geschult und sensibilisiert werden, um die Bedeutung der IKT-Resilienz zu verstehen und wie sie dazu beitragen können.
  - **Übung und Testläufe:** Regelmässige Übungen und Tests von Notfall- und Wiederherstellungsplänen sind entscheidend, um sicherzustellen, dass die IKT-Resilienz Pläne effektiv sind. Diese Übungen sollten realistische Szenarien simulieren und die Zusammenarbeit zwischen den Organisationseinheiten fördern.
  - **Kommunikation und Informationsaustausch:** Offene und effektive Kommunikation zwischen den Teams ist von entscheidender Bedeutung, insbesondere während eines Störfalls. Die Teams sollten wissen, wie sie Informationen austauschen und Entscheidungen treffen können.
  - **Kontinuierliche Verbesserung:** Die Zusammenarbeit zur Steigerung der IKT-Resilienz sollte ein kontinuierlicher Prozess sein. Teams sollten regelmässig Feedback sammeln, Störungen analysieren und Pläne aktualisieren, um die Resilienz kontinuierlich zu verbessern.
- (2) Die Zusammenarbeit für eine gesteigerte IKT-Resilienz ist eine umfassende Anstrengung, die das Zusammenspiel verschiedener Organisationseinheiten und Experten erfordert. Es ist wichtig, dass die Organisation die IKT-Resilienz als entscheidenden Teil ihres Geschäftsverfahrens betrachtet und die notwendigen Ressourcen und Unterstützung bereitstellt.



#### Empfehlung der VSE Cyber Security Task Force Experten:

Eine intensive und konstruktive Zusammenarbeit stellt eine essenzielle Grundlage für die Steigerung der IKT-Resilienz dar. Sie muss aufgebaut, gefördert, aktiv gelebt und gepflegt werden. Sowie durch das Management vorgelebt und getragen werden.

## 5.5 Tools zur Steigerung der IKT-Resilienz

- (1) Die Verwendung von Tools spielt eine entscheidende Rolle bei der Steigerung der IKT-Resilienz von Unternehmen und Organisationseinheiten. Diese Tools umfassen Softwarelösungen, Überwachungsinstrumente, Sicherheitsplattformen und automatisierte Prozesse, die dazu dienen, Schwachstellen zu identifizieren, Angriffe zu erkennen und schnelle Reaktionen auf Sicherheitsvorfälle zu ermöglichen. Sie unterstützen bei der Implementierung von Sicherheitsrichtlinien, der Durchführung von Risikoanalysen und



der Überwachung der IKT-Infrastruktur in Echtzeit. Die Nutzung solcher Tools ermöglicht eine proaktive Herangehensweise an die IKT-Sicherheit, indem sie dazu beitragen, potenzielle Bedrohungen frühzeitig zu erkennen und Gegenmassnahmen schnell einzuleiten. Durch die Integration fortschrittlicher Technologien und Tools können Unternehmen und Organisationseinheiten ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen stärken und den Schutz ihrer Informations- und Kommunikationstechnologien optimieren.

### 5.5.1 VSE-Tools zur Steigerung der IKT-Resilienz



**Folgende Tools sind durch den VSE entwickelt und erstellt worden und stehen den VSE Mitgliedern zur Steigerung der IKT-Resilienz zur Verfügung:**

- 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



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die vom VSE zur Verfügung gestellten Tools sollen angewendet werden. Sie helfen dem Anwender effektiv die IKT-Resilienz systematisch zu erhöhen**



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**



**Im Anhang befindet sich eine ausführliche Beschreibung der VSE-Tools.**



## 5.5.2 Weitere erhältliche Tools als Hilfe zur Steigerung der IKT-Resilienz



**Folgende erhältliche Tools als Hilfe zur Steigerung der IKT-Resilienz Hilfe stehen zur Verfügung:**

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



**Die Liste ist nicht abschliessend. Es gibt noch weitere Tools, welche zur Steigerung der IKT-Resilienz beitragen.**



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**

## 6. Vorgehen zur Steigerung der IKT-Resilienz: Einführung des ISMS mit der Vernetzung des NIST CSF 1.1

- (1) Die Einführung eines Information Security Management Systems (ISMS) mit der systematischen Vernetzung mit dem NIST CSF 1.1 in Schritten macht Sinn, weil es eine strukturierte und umfassende Herangehensweise an die Sicherheit von Informationen in einer Organisation bietet. Dies aus folgenden Gründen:
  - **Systematische Planung:** Die schrittweise Einführung ermöglicht eine gründliche Planung des ISMS. Dies beinhaltet die Identifikation von Zielen, Ressourcen und Verantwortlichkeiten.
  - **Top-Management-Engagement:** Durch die schrittweise Einführung wird das Top-Management von Anfang an in den Prozess einbezogen. Das Engagement der Führungsebene ist entscheidend für den Erfolg eines ISMS, da es Ressourcen und Unterstützung bereitstellt.
  - **Kontinuierlicher Verbesserungsprozess:** Die schrittweise Einführung fördert die Idee der kontinuierlichen Verbesserung. Unternehmen und Organisationseinheiten können regelmässig ihre Sicherheitspraktiken überprüfen und anpassen, um mit sich ändernden Bedrohungen und Anforderungen Schritt zu halten.
  - **Risikobewertung:** Die schrittweise Einführung ermöglicht eine gründliche Risikobewertung. Die Identifizierung von Risiken ist entscheidend, um angemessene Sicherheitsmassnahmen zu implementieren.
  - **Angemessene Ressourcenallokation:** Durch die schrittweise Einführung können Unternehmen und Organisationseinheiten sicherstellen, dass ausreichende Ressourcen für die Umsetzung und Aufrechterhaltung des ISMS zur Verfügung stehen.
  - **Integration in bestehende Prozesse:** Die schrittweise Einführung erlaubt die Integration des ISMS in bereits bestehende Geschäftsprozesse. Dies erleichtert die Akzeptanz und Umsetzung durch die Mitarbeiter.
  - **Schulung und Bewusstseinsbildung:** Die schrittweise Einführung ermöglicht die gezielte Schulung der Mitarbeiter und die Schaffung eines Bewusstseins für Informationssicherheit in der gesamten Organisation.
  - **Zertifizierung und Anerkennung:** Die schrittweise Einführung legt den Grundstein für eine Zertifizierung nach internationalen Standards wie ISO 27001. Eine solche Zertifizierung kann das Vertrauen von Kunden und Partnern stärken.
- (2) Insgesamt ermöglicht die schrittweise Einführung eines ISMS mit der Vernetzung des NIST CFS 1.1 eine methodische und gut koordinierte Umsetzung von Informationssicherheitspraktiken. Dies ist besonders wichtig in einer zunehmend vernetzten und digitalisierten Welt, in der die Sicherheit von Informationen eine kritische Rolle für den Geschäftserfolg spielt.





(3) Die Einführung eines ISMS mit der Vernetzung des NIST CSF 1.1 ist in folgende acht Phasen gegliedert:

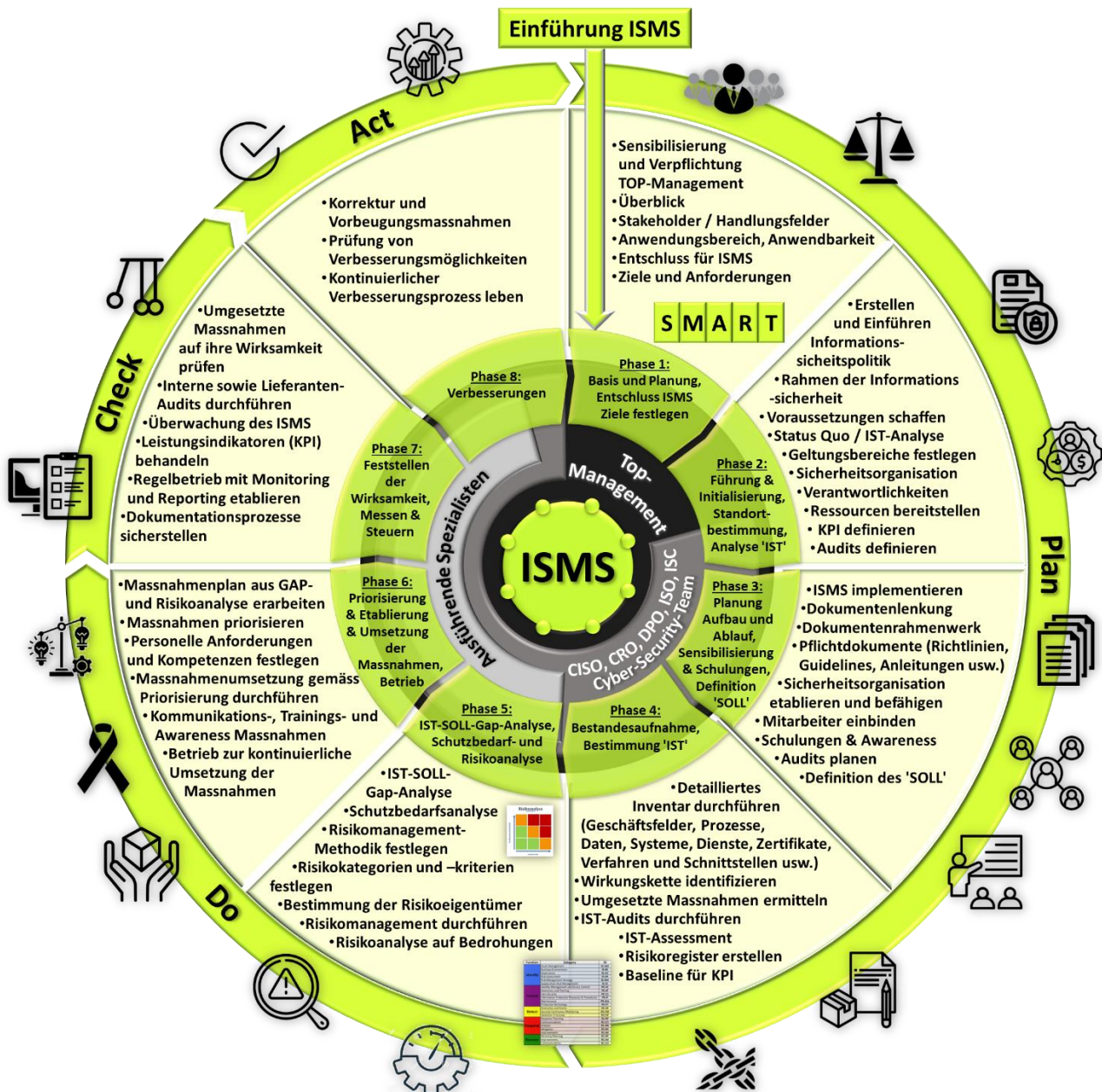


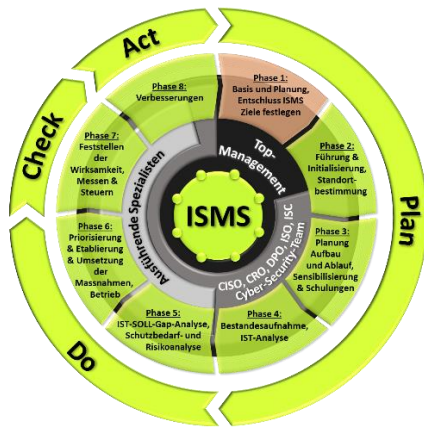
Abbildung 25: Detaillierter Regelkreis der acht VSE-Phasen zur Einführung und Betrieb des ISMS (Quelle VSE)

(4) Die Einführung eines Information Security Management Systems (ISMS) in acht Phasen folgt einem strukturierten Ansatz, um sicherzustellen, dass die Informationssicherheitspraktiken in einer Organisation effektiv entwickelt und implementiert werden.



## 6.1 Phase 1: Basis und Planung; Entschluss ISMS; Ziele festlegen

- (1) Die Basis und Planung zur Einführung eines ISMS bilden eine entscheidende Grundlage für den Erfolg des gesamten Projekts.



Verantwortlich:	Top-Management, C-Level
Zuständig:	Top-Management, C-Level
Involvierte Stellen:	Spezifische Mitarbeiter der Informationssicherheit, externe Experten und Berater
Zu behandelnde Punkte	<ul style="list-style-type: none"> <li>■ Sensibilisierung und Verpflichtung der obersten Führungsebene für die Informationssicherheit</li> <li>■ Identifikation von Interessengruppen (Stakeholder)</li> <li>■ Rechtliche und regulatorische Anforderungen aufzeigen</li> <li>■ (insbesondere Vorgaben nach Strom VV)</li> <li>■ Anwendbarkeit definieren (Assessment-Tools)</li> <li>■ Geschäftsprozesse ableiten</li> <li>■ Handlungsfelder aufzeigen</li> <li>■ Fokus für die Informationssicherheit definieren / anpassen</li> <li>■ Grundsatzentscheid für Einführung eines ISMS auf Stufe Verwaltungsrat, Konzern- oder Geschäftsleitung (C-Level)</li> <li>■ Ziele des ISMS definieren und initiieren</li> </ul>

Tabelle 7: ISMS Phase 1: Basis und Planung; Entschluss ISMS; Ziele festlegen

### 6.1.1 Sensibilisierung und Verpflichtung der obersten Führungsebene für die Informationssicherheit

- (1) Die Sensibilisierung und Verpflichtung der obersten Führungsebene für die Informationssicherheit ist wichtig, um sicherzustellen, dass das ISMS in der gesamten Organisation erfolgreich implementiert wird. Dieser Prozess beinhaltet:
- **Sensibilisierung:** Die Sensibilisierung beginnt mit der Schaffung eines klaren Bewusstseins für die Bedeutung von Informationssicherheit. Dies kann durch Schulungen, Workshops, Präsentationen oder andere Kommunikationsmittel erfolgen. Es ist wichtig, dass das TOP-Management die aktuellen Bedrohungen und Risiken für die Informationssicherheit versteht und sich darüber im Klaren ist, welche Auswirkungen Sicherheitsvorfälle auf die Organisation haben können.
  - **Verpflichtung:** Die oberste Führungsebene muss sich aktiv dazu verpflichten, die Umsetzung des ISMS zu unterstützen. Diese Verpflichtung manifestiert sich in der Bereitstellung von Ressourcen, Unterstützung bei der Festlegung von Sicherheitszielen und -richtlinien sowie der Integration von Informationssicherheit in die gesamte Unternehmenskultur. Die Führungsebene sollte klarstellen, dass Informationssicherheit nicht nur eine technische Angelegenheit ist, sondern ein grundlegender Bestandteil der Unternehmensführung.
- (2) Die Sensibilisierung und Verpflichtung der obersten Führungsebene bildet die Basis für den gesamten Informationssicherheitsansatz des Unternehmens und der Organisationseinheiten. Wenn die Führungsebene die Bedeutung von Informationssicherheit versteht und sich verpflichtet, entsprechende Massnahmen zu unterstützen, steigt die Wahrscheinlichkeit erheblich, dass das ISMS erfolgreich eingeführt und aufrechterhalten wird. Diese Unterstützung ist auch entscheidend, um Mitarbeiter auf allen Ebenen der Organisation für Informationssicherheit zu sensibilisieren und zu motivieren.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-00: Politik zur Führung und unternehmerischen Tätigkeit
- HoP-01-00: Weisung zur Geschäftsführung



Es wird von den VSE Cyber Security Task Force Experten empfohlen, dass für die Sensibilisierung und Verpflichtung der obersten Führungsebene für die Informationssicherheit ein externer Fachexperte beigezogen wird. Durch managementgerechte Ausführung kann so die Affinität und Pflicht besser erläutert werden. Es ist sehr wichtig, dass die Informationssicherheit vom der obersten Führungsstufe ganzheitlich getragen und gefördert wird.



### 6.1.2 Identifikation von Interessengruppen (Stakeholder)

- (1) Die Identifikation von Interessengruppen, auch Stakeholder genannt, ist ein wesentlicher Schritt im Rahmen der Einführung eines ISMS. Diese Interessengruppen spielen eine entscheidende Rolle bei der Definition, Umsetzung und Aufrechterhaltung des ISMS. Hier sind die Schritte zur Identifikation von Stakeholdern:
  - **Analyse der Organisationsstruktur:** Die Organisationsstruktur sollte analysiert werden, um Schlüsselakteure und Abteilungen zu identifizieren, die einen direkten Einfluss auf die Informationssicherheit haben. Dies umfasst typischerweise die oberste Führungsebene, IT/OT-Abteilungen, Sicherheitsbeauftragte, Compliance-Abteilungen und andere relevante Bereiche.
  - **Gesetzliche und regulatorische Anforderungen:** Identifikation von Stakeholdern erfolgt auch durch die Analyse gesetzlicher und regulatorischer Anforderungen. Diese können Vorschriften zur Datensicherheit, Datenschutzbestimmungen oder branchenspezifische Regularien umfassen. Die entsprechenden Behörden oder Aufsichtsorgane werden als wichtige Stakeholder betrachtet.
  - **Interne und externe Partner:** Externe Partner wie Kunden, Lieferanten und Dienstleister können ebenfalls als Stakeholder betrachtet werden, insbesondere wenn sie Zugang zu sensiblen Informationen haben. Auch interne Partner, die in Geschäftsprozesse eingebunden sind, sollten berücksichtigt werden.
  - **Mitarbeiter:** Mitarbeiter auf allen Ebenen der Organisation sind wesentliche Stakeholder. Dies umfasst nicht nur IT-Mitarbeiter, sondern auch Mitarbeiter in anderen Organisationseinheiten, da sie alle einen Beitrag zur Sicherheit von Informationen leisten können oder davon betroffen sind.
  - **Management und Eigentümer:** Die oberste Führungsebene und die Eigentümer der Organisation sind von zentraler Bedeutung. Ihr Engagement und ihre Unterstützung sind entscheidend für den Erfolg des ISMS. Die Identifikation von Schlüsselentscheidungsträgern und deren Einbindung ist daher entscheidend.
  - **Externe Interessengruppen:** Externe Interessengruppen wie Kunden, Investoren, Aktionäre und die Öffentlichkeit können ein Interesse an der Informationssicherheit der Organisation haben. Ihre Erwartungen und Anforderungen sollten berücksichtigt werden.
  - **Risikobewertung:** Eine Risikobewertung kann auch dazu beitragen, potentielle Stakeholder zu identifizieren, indem analysiert wird, welche Parteien am meisten von Sicherheitsrisiken betroffen sein könnten.
- (2) Die Identifikation von Stakeholdern ist ein iterativer Prozess und erfordert eine sorgfältige Analyse der Organisation und ihrer Umgebung. Die Bedürfnisse und Erwartungen dieser Stakeholder werden in den verschiedenen Phasen des ISMS-Projekts berücksichtigt, um sicherzustellen, dass ihre Interessen angemessen adressiert werden.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



**Empfehlung der VSE Cyber Security Task Force Experten:**

Mit Awareness-Trainings durch einen externen Experten kann das Verständnis, die Akzeptanz und die Unterstützung bei den Stakeholdern erlangt werden. Die Stakeholder müssen sich über die Tragweite einer konsequenten Informationssicherheitspolitik bewusst sein. Sie tragen eine grosse Verantwortung und es muss ein Mitwirken bzw. eine konstruktive Zusammenarbeit eingefordert und gefördert werden. Alle Stakeholder müssen sich ihre Rolle bezüglich Informationssicherheit bewusst sein!

### 6.1.3 Rechtliche und regulatorische Anforderungen aufzeigen und anwenden

- (1) Alle rechtlichen und regulatorischen Anforderungen für die Informationssicherheit, welche für ein Unternehmen und Organisationseinheiten zutreffen, müssen identifiziert, aufgezeigt und eingehalten werden. In diesen Leitfaden sind im Anhang alle rechtlichen und regulatorischen Anforderungen aufgelistet. Diese müssen durch die Unternehmen und Organisationseinheiten in einer entsprechenden Vorgabe verankert werden. Durch die Schulung und Sensibilisierung werden alle involvierten Stellen über diese Vorgaben informiert.





In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



**Empfehlung der VSE Cyber Security Task Force Experten:**

Das Aufzeigen und die Anwendung rechtlicher und regulatorischer Anforderungen im Rahmen der Informationssicherheit ist wichtig, um sicherzustellen, dass das Unternehmen gesetzliche Vorschriften einhält, Datenschutz gewährleistet und potenzielle rechtliche Risiken minimiert werden.

#### 6.1.4 Anwendbarkeit definieren (Assessment-Tools)

- (1) Die Anwendbarkeit legt den grundsätzlichen Anwendungsbereich für die Informationssicherheit fest. Dabei soll durch die Unternehmen und Organisationseinheiten analysiert und festgelegt werden, wie die einzelnen Kontrollen anzuwenden bzw. zu behandeln sind.

##### Anwendbarkeit der Kontrollen im NIST Cybersecurity Frameworks (CSF) 1.1:

- (2) Die Anwendbarkeit des NIST Cybersecurity Frameworks (CSF) 1.1 bezieht sich darauf, wie effektiv und vielseitig das Framework in verschiedenen Unternehmen und Organisationseinheiten und Szenarien angewendet werden kann. Diese Anwendbarkeit basiert auf der Fähigkeit des Frameworks, Unternehmen und Organisationseinheiten bei der Identifizierung, dem Schutz und der Erkennung von Sicherheitsvorfällen sowie der angemessenen Reaktion darauf und der Wiederherstellung von IKT-Infrastrukturen nach Unterbrüchen oder Ausfällen durch Cyberangriffen zu unterstützen.
- (3) In der Version 1.1 des NIST CSF werden bewährte Praktiken und Leitlinien für die Entwicklung und Verbesserung von Cybersicherheitsstrategien bereitgestellt. Die Anwendbarkeit des Frameworks zeigt sich darin, dass das Framework flexibel genug ist, um auf unterschiedliche Branchen, Unternehmens- und Organisationseinheitengrößen und spezifische Bedrohungslandschaften angewendet werden zu können.
- (4) Das Framework ermöglicht es Unternehmen und Organisationseinheiten, ihre individuellen Risiken und Vermögenswerte zu identifizieren, geeignete Schutzmassnahmen zu implementieren, frühzeitig auf Bedrohungen zu reagieren, effektive Pläne für die Wiederherstellung nach einem Vorfall zu entwickeln und kontinuierlich ihre Cybersicherheitspraktiken zu verbessern.
- (5) Die Anwendbarkeit des NIST CSF 1.1 erstreckt sich über verschiedene Bereiche da es als Rahmenwerk für eine ganzheitliche Cybersicherheitsstrategie dient. Es ermöglicht Unternehmen und Organisationseinheiten, das Rahmenwerk an ihre spezifischen Anforderungen anzupassen und gleichzeitig eine konsistente und umfassende Herangehensweise an die Cybersicherheit beizubehalten.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



Für die Definition der Anwendbarkeit der Kontrollen im NIST Cybersecurity Frameworks (CSF) 1.1 kann das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" verwendet werden.



Im Anhang befindet sich eine ausführliche Beschreibung für das "VSE & BFE-IKT-Minimalstandard-Assessment-Tool++" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002".



**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.

#### "Statement of Applicability" (SoA) bei ISO 27001:

- (6) Die Anwendbarkeit "Statement of Applicability" (SoA) ist ein wichtiges Dokument im Kontext des ISO/27001,). Die SoA dient dazu, den Anwendungsbereich und die Details festzulegen, wie eine Organisation die Anforderungen des ISO 27001 zum Schutz ihrer Informationswerte umsetzen wird. Hier ist eine Aufschlüsselung der wichtigsten Bestandteile der "Statement of Applicability":
  - **1. Anwendungsbereich:** Die SoA beginnt mit einer klaren Aussage zum Anwendungsbereich des ISMS. Sie legt die Grenzen fest, welche Informationswerte abgedeckt sind und inwieweit die Anforderungen des ISO 27001 angewendet werden.



- **2. Anwendbare Kontrollziele und Kontrollen:** Der Hauptzweck der SoA besteht darin, die spezifischen Kontrollziele und Kontrollen aus dem ISO 27001 aufzulisten, die die Organisation implementiert hat. Diese Kontrollen werden auf Grundlage einer Risikobewertung und des individuellen Kontexts der Organisation ausgewählt. Die SoA enthält die Nummer jeder Kontrolle, ihren Titel und eine kurze Beschreibung, wie sie angewendet wird.
  - **3. Begründung für Ausschlüsse:** Falls es Kontrollziele oder Kontrollen gibt, die die Organisation beschlossen, hat, nicht umzusetzen, sollte die SoA eine klare Begründung für diese Ausschlüsse liefern. Dies ist oft mit einer Risikobewertung verknüpft, bei der die Organisation feststellt, dass eine bestimmte Kontrolle in ihrem Kontext nicht notwendig oder durchführbar ist.
  - **4. Zusätzliche Kontrollen:** In einigen Fällen kann es vorkommen, dass Unternehmen und Organisationseinheiten zusätzliche Kontrollen implementieren, die nicht explizit in dem ISO 27001 aufgeführt sind. Diese können zur SoA hinzugefügt werden, zusammen mit ihren Beschreibungen und Begründungen.
  - **5. Zuständigkeit und Verantwortlichkeiten für Kontrollen:** Die SoA kann auch angeben, wer für die Umsetzung und Aufrechterhaltung jeder Kontrolle verantwortlich ist. Dies stellt sicher, dass innerhalb der Organisation eine Verantwortlichkeit für jede Kontrolle besteht.
  - **6. Überprüfungs- und Aktualisierungsprozess:** Das Dokument sollte den Prozess für die regelmäßige Überprüfung und Aktualisierung der "Statement of Applicability" darlegen. Dies hilft sicherzustellen, dass das ISMS effektiv bleibt, wenn sich der Kontext und die Risiken der Organisation ändern.
- (7) Die "Statement of Applicability" ist ein dynamisches Dokument und sollte regelmässig überprüft und aktualisiert werden, um Veränderungen in der Informationssicherheitsumgebung der Organisation und sich ändernde Risikoprofile widerzuspiegeln. Sie ist ein unverzichtbares Instrument für Unternehmen und Organisationseinheiten, die eine Zertifizierung nach ISO 27001 anstreben, da sie ein klares Verständnis dafür vermittelt, wie Informationssicherheitskontrollen in der Organisation angewendet werden.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



**Für die SoA nach ISO 27001 Annex A soll das "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002" verwendet werden.**



**Im Anhang befindet sich eine ausführliche Beschreibung für das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002".**



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**

### 6.1.5 Geschäftsprozesse aufzeigen und ableiten

- (1) Die Darstellung der Geschäftsprozesse im Zusammenhang mit der Informationssicherheit beinhaltet eine gründliche Analyse und Identifikation aller Aktivitäten und Abläufe innerhalb einer Organisation, die die Sicherheit von Informationen beeinflussen können. Dieser Prozess ist entscheidend, um potentielle Risiken zu verstehen und wirksame Schutzmassnahmen zu implementieren. Zu Beginn werden alle relevanten Geschäftsprozesse ermittelt, die Daten verarbeiten, speichern oder übertragen. Dies schliesst sämtliche Tätigkeiten ein, die in direktem Zusammenhang mit sensiblen Informationen stehen. Die Analyse konzentriert sich darauf, wie Informationen innerhalb dieser Prozesse fliessen - von ihrem Ursprung über Verarbeitung und Speicherung bis hin zur Übertragung.
- (2) Im nächsten Schritt erfolgt eine gründliche Risikobewertung. Dies umfasst die Identifizierung von Schwachstellen und Bedrohungen, die die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen gefährden. Die Risikobewertung ermöglicht es, die Wahrscheinlichkeit und die Auswirkungen von Sicherheitsvorfällen zu bestimmen. Basierend auf den Ergebnissen der Risikobewertung werden gezielte Schutzmassnahmen entwickelt und implementiert. Diese können technischer, organisatorischer oder





personenbezogener Natur sein und dienen dazu, die Sicherheit der Geschäftsprozesse und der darin verarbeiteten Informationen sicherzustellen.

- (3) Es ist wichtig, Sicherheitsrichtlinien und -verfahren in die Geschäftsprozesse zu integrieren. Dadurch wird gewährleistet, dass Sicherheitsaspekte von Anfang an berücksichtigt werden und von den Mitarbeitern in ihren täglichen Aktivitäten beachtet werden. Die Überwachung der Geschäftsprozesse ist ein fortlaufender Prozess. Dies gewährleistet, dass die implementierten Sicherheitsmassnahmen effektiv sind und bei Bedarf angepasst werden können, um auf sich ändernde Bedrohungen oder geschäftliche Anforderungen zu reagieren.
- (4) Insgesamt trägt die umfassende Darstellung der Geschäftsprozesse im Kontext der Informationssicherheit dazu bei, ein tiefgehendes Verständnis für die Sicherheitsanforderungen einer Organisation zu entwickeln und sicherzustellen, dass angemessene Schutzmassnahmen implementiert werden, um die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen zu gewährleisten.

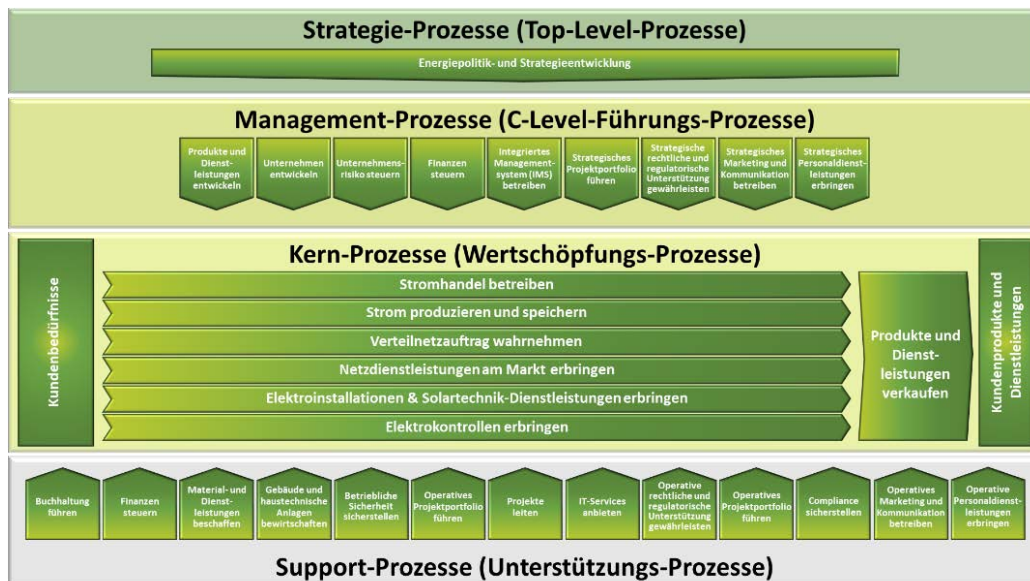


Abbildung 26: Prozesse in Unternehmen und Organisationseinheiten (Quelle VSE)

- (5) Die Prozesse in einer Organisation, welche mit der Informationssicherheit in Verbindung stehen, müssen identifiziert und entsprechend ausgewiesen und inventarisiert werden. Dies muss durch die Unternehmen und Organisationseinheiten in einer entsprechenden Vorgabe verankert werden. Durch die Schulung und Sensibilisierung werden alle involvierten Stellen über diese Vorgaben informiert.

**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**



- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS
- "HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung"

**Empfehlung der VSE Cyber Security Task Force Experten:**



**Das Aufzeigen und Ableiten der Geschäftsprozesse für die Informationssicherheit ist wichtig, um die spezifischen Anforderungen und Risiken zu verstehen, die mit den verschiedenen Unternehmensaktivitäten verbunden sind, und um gezielte Sicherheitsmassnahmen zu entwickeln, die die Geschäftsziele unterstützen und schützen. Die Prozesse sind nicht nur auf Vorgaben im Strom VV zu beschränken. Es wird empfohlen eine Baseline für alle Prozesse der Informationssicherheit einzuführen.**

## 6.1.6 Handlungsfelder für die Informationssicherheit aufzeigen

- (1) Die Definition der Handlungsfelder für die Informationssicherheit anhand der Geschäftsprozesse erfolgt durch einen sorgfältigen Prozess der Analyse, Identifikation und Kategorisierung, um sicherzustellen, dass alle relevanten Aspekte der Informationssicherheit berücksichtigt werden. Zu Beginn wird eine gründliche Analyse der Geschäftsprozesse durchgeführt, um alle Aktivitäten zu identifizieren, die mit der Verarbeitung, Speicherung oder Übertragung von Informationen verbunden sind. Diese Analyse ermöglicht es, die





Informationsflüsse innerhalb der Organisation zu verstehen und diejenigen Prozesse zu identifizieren, die für die Informationssicherheit besonders kritisch sind.

- (2) Nach der Identifikation dieser kritischen Geschäftsprozesse erfolgt eine Risikobewertung. Hierbei werden potenzielle Schwachstellen, Bedrohungen und Risiken analysiert, um festzustellen, welche Aspekte der Informationssicherheit am meisten gefährdet sind. Diese Bewertung hilft bei der Priorisierung der Handlungsfelder und bei der Festlegung von Schwerpunkten für die Sicherheitsmassnahmen. Die Definition der Handlungsfelder bezieht sich dann auf konkrete Massnahmen, die ergriffen werden müssen, um die identifizierten Risiken zu mindern. Dies kann die Einführung technischer Sicherheitsvorkehrungen, die Implementierung von Sicherheitsrichtlinien und -verfahren, Schulungen für Mitarbeiter oder organisatorische Anpassungen umfassen.
- (3) Die Handlungsfelder können sich auf verschiedene Bereiche konzentrieren, wie zum Beispiel den Schutz vor unberechtigtem Zugriff, die Gewährleistung der Integrität von Daten, die Verfügbarkeit von kritischen Systemen oder die Implementierung von Notfallwiederherstellungsplänen. Die Definition dieser Handlungsfelder erfolgt in enger Abstimmung mit den Zielen der Organisation und den spezifischen Anforderungen ihrer Geschäftsprozesse. Es ist ein iterativer Prozess, der eine fortlaufende Überwachung und Anpassung erfordert.
- (4) Die Handlungsfelder können sich im Laufe der Zeit ändern, insbesondere vor dem Hintergrund sich wandelnder Bedrohungslandschaften, neuer Technologien oder geschäftlicher Anforderungen. Durch diese iterative Herangehensweise wird sichergestellt, dass die Informationssicherheit kontinuierlich verbessert wird und auf aktuelle Gegebenheiten reagiert.
- (5) Die Handlungsfelder für die Informationssicherheit müssen durch die Unternehmen und Organisationseinheiten festgelegt und entsprechend dokumentiert werden.

**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**



- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS
- "HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung"

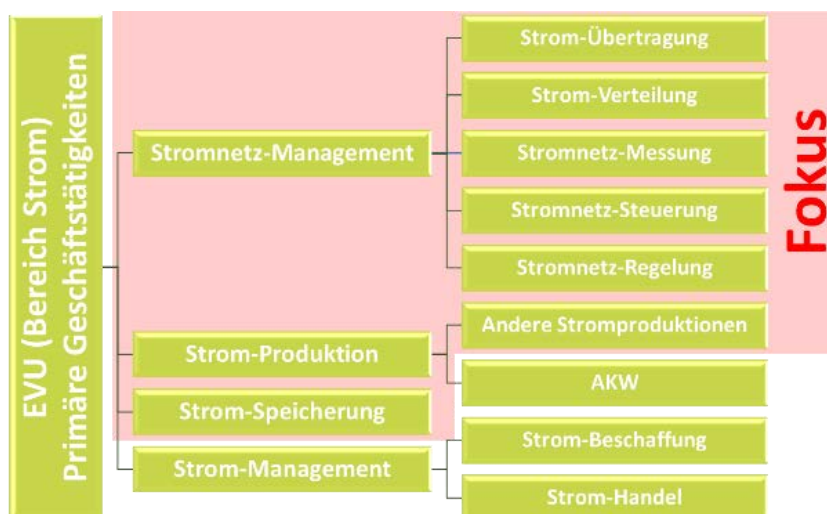


**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Handlungsfelder sind nicht nur auf Vorgaben im Strom VV zu beschränken. Es wird empfohlen eine Baseline für alle Handlungsfelder der Informationssicherheit einzuführen.**

### 6.1.7 Fokus für die Informationssicherheit definieren / anpassen

- (1) Durch die Vorgaben im Strom VV wird der Fokus der Informationssicherheit von versorgungskritischen Unternehmen und Organisationseinheiten festgelegt:



**Abbildung 27:** Festlegen des Fokus gemäss Strom VV (Quelle VSE)



- (2) Jedes Unternehmen und jede Organisationseinheiten muss definieren, wo ihre primären Geschäftstätigkeiten. Folgende Geschäftstätigkeiten<sup>1</sup> werden in diesem Leitfaden als relevant betrachtet und werden weiter behandelt:
- **Stromnetz-Management:** Stromnetzmanagement umfasst Planung, Betrieb, Überwachung und Steuerung von elektrischen Netzwerken für eine zuverlässige Stromversorgung. Es beinhaltet Netzplanung, -design, der tägliche Netzbetrieb sowie die Netzsicherheit und die Integration erneuerbaren Energielösungen. Das Ziel ist eine stabile Stromversorgung, Minimierung von Ausfällen und Erfüllung von Energieeffizienz- und Nachhaltigkeitsanforderungen durch komplexe Infrastrukturkoordination.
  - **Strom-Produktion:** Stromproduktion erzeugt elektrische Energie aus verschiedenen Quellen, darunter fossilen Brennstoffe, erneuerbare Energien wie Wind und Sonne, Wasserkraft und Kernkraft. Dieser Prozess kann zentralisiert oder dezentralisiert sein, abhängig von Technologien und Netzstruktur. Effizienz und Umweltauswirkungen hängen von Energiequelle und Technologie ab. Ziel ist eine zuverlässige, nachhaltige Stromversorgung, erfordert sorgfältige Planung, Infrastrukturinvestitionen und erneuerbare Integration.
  - **Strom-Speicherung:** Energiespeicher sind entscheidend für die moderne Energiewirtschaft, ermöglichen das Speichern und Abrufen von elektrischer Energie bei Bedarf. Das umfasst verschiedene Methoden wie Batterien, Pumpspeicherkraftwerke und thermische Speicher. Die Speicherung gleicht den schwankenden Energiebedarf aus, unterstützt erneuerbare Energien und erhöht die Netzstabilität. Effiziente Energiespeichertechnologien tragen zur Steigerung der Energieeffizienz und Nachhaltigkeit bei, und spielen eine Schlüsselrolle in der Transformation des Energiesektors.
- (3) Die Informationssicherheit soll sich aber nicht nur auf den festgelegten Fokus konzentrieren. Die Informationssicherheit muss die gesamte Organisation ganzheitlich abdecken.
- (4) Der Fokus für die Informationssicherheit muss durch die Unternehmen und Organisationseinheiten festgelegt und entsprechend dokumentiert werden.

**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**



- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS
- "HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung"



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Der Fokus ist zwar auf die Vorgaben im Strom VV zu legen. Dennoch sind alle Bereiche der Informationssicherheit abzudecken. Es wird empfohlen eine Baseline für alle Bereich der Informationssicherheit einzuführen.**

### 6.1.8 Grundsatzentscheid für die Einführung eines ISMS auf Stufe Konzern- oder Geschäftsleitung (C-Level)

- (1) Der Grundsatzentscheid zur Einführung eines Information Security Management Systems (ISMS) auf C-Level-Ebene, also in der Konzern- oder Geschäftsleitung, ist von strategischer Bedeutung. Dieser Beschluss reflektiert die Anerkennung der Wichtigkeit der Informationssicherheit für die Organisation. Es zeigt das Verständnis dafür, dass der Schutz von sensiblen Informationen und die Sicherstellung der IKT-Resilienz wesentlich für den Geschäftsbetrieb und den Ruf des Unternehmens und der Organisationseinheiten sind.
- (2) Der Schritt zur Implementierung eines ISMS auf höchster Führungsebene signalisiert das Engagement für eine umfassende und systematische Herangehensweise an die Informationssicherheit. Es zeigt, dass die Führungsebene bereit ist, die notwendigen Ressourcen bereitzustellen, um ein wirksames ISMS zu etablieren. Dieser Grundsatzentscheid reflektiert auch das Bewusstsein für die steigenden Bedrohungen in der digitalen Landschaft und die Notwendigkeit, proaktiv Schutzmassnahmen zu ergreifen.
- (3) Die Führungsebene legt somit den Grundstein für eine Sicherheitskultur innerhalb der Organisation und setzt klare Prioritäten hinsichtlich der Informationssicherheit. Dieser Entschluss geht über blosse Technologiefragen hinaus und betrifft die gesamte Unternehmensstrategie, da Informationssicherheit eng mit

<sup>1</sup> Gemäss Definition im Strom VV



Geschäftsprozessen, Compliance-Anforderungen und dem Schutz des Unternehmensvermögens verknüpft ist. Insgesamt spiegelt der Grundsatzentscheid zur Einführung eines ISMS auf C-Level-Ebene die Anerkennung wider, dass Informationssicherheit nicht nur eine IT-Frage ist, sondern einen entscheidenden Einfluss auf den gesamten Unternehmenserfolg hat.



**In den folgenden Dokumenten sind Orientierungshilfen und Anleitungen:**

- BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)



**Die Einführung eines ISMS erfordert beträchtliche Ressourcen in den Unternehmen und Organisationseinheiten. Der Aufwand ist nicht zu unterschätzen. Diese Umstände sind zwingend bei der Entscheidung zur Einführung eines ISMS zu berücksichtigen.**



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Der Grundsatzentscheid für die Einführung eines ISMS auf C-Level-Ebene ist wichtig, um die Bedeutung der Informationssicherheit für das gesamte Unternehmen zu betonen, Ressourcen zu mobilisieren und eine klare Führung und Unterstützung für die Umsetzung des ISMS sicherzustellen.**

### 6.1.9 Ziele des ISMS definieren und initiieren



(1) Die Definition der Ziele für das Information Security Management System sollte den SMART-Kriterien entsprechen. Das bedeutet, dass sie spezifisch (Specific), messbar (Measurable), erreichbar (Achievable), relevant (Relevant) und zeitgebunden (Time-bound) sein sollten.

(2) Spezifische Ziele setzen klare Vorgaben, um welche Aspekte der Informationssicherheit es geht. Sie müssen messbar sein, damit Fortschritte überwacht und der Erfolg bewertet werden kann. Zudem sollten die Ziele erreichbar und realistisch sein, um eine Umsetzung zu ermöglichen. Relevanz stellt sicher, dass die Ziele einen direkten Beitrag zur Sicherheit der Informationen leisten sowie die generellen Unternehmensziele unterstützen. Zeitliche Vorgaben sorgen dafür, dass die Ziele in einem festgelegten Zeitrahmen erreicht werden.

(3) Diese SMART-Ziele dienen als Leitlinien für die Planung und Umsetzung von Sicherheitsmassnahmen im Rahmen des ISMS. Sie ermöglichen eine präzise Ausrichtung der Bemühungen auf konkrete Sicherheitsziele, um die Informationssicherheit auf effektive und messbare Weise zu stärken.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS



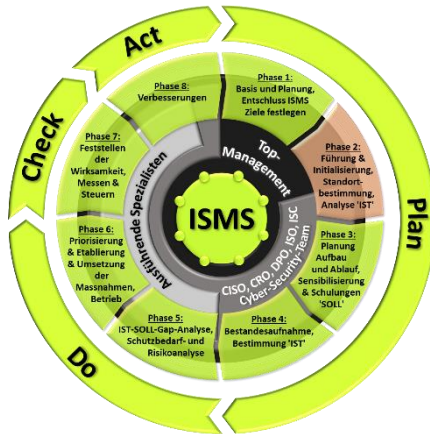
**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Definition von ISMS-Zielen nach dem SMART-Prinzip ist wichtig, um sicherzustellen, dass sie spezifisch, messbar, erreichbar, relevant und zeitgebunden sind, was ihre Wirksamkeit bei der Verbesserung der Informationssicherheit erhöht und klare Leitlinien für den Erfolg festlegt.**



## 6.2 Phase 2: Führung und Initialisierung; Standortbestimmung

- (1) In der zweiten Phase der Einführung eines ISMS werden die Bereiche der Führung und Initialisierung sowie die Standortbestimmung behandelt:



Verantwortlich:	Top-Management, C-Level
Zuständig:	Top-Management, C-Level
Involvierte Stellen:	CISO, CRO, DPO, ISO, ISC, Cyber Security Team externe Experten und Berater
Zu behandelnde Punkte	<ul style="list-style-type: none"> <li>■ Erstellen und Einführen der Politik und Strategie zur Informationssicherheit: Wie ist die Informationssicherheit zu behandeln?</li> <li>■ Rahmen der Informationssicherheit festlegen</li> <li>■ Schaffung der Voraussetzungen</li> <li>■ Ermittlung des Status Quo / IST-Analyse im Bereich Informationssicherheit durchführen</li> <li>■ Geltungsbereich für die Informationssicherheit gemäss Vorgaben Strom VV festlegen</li> <li>■ Zusätzlichen Geltungsbereich für die Informationssicherheit festlegen</li> <li>■ Geltungsbereich des ISMS festlegen</li> <li>■ Sicherheitsorganisation aufbauen / anpassen</li> <li>■ Verantwortlichkeiten definieren / anpassen</li> <li>■ Leistungsindikatoren (KPI) definieren</li> <li>■ Vorgehen für Audits definieren</li> </ul>

Tabelle 8: ISMS Phase 2: Führung und Initialisierung; Standortbestimmung

### 6.2.1 Erstellen und Einführen der Politik und Strategie zur Informationssicherheit: Wie ist die Informationssicherheit zu behandeln?

- (1) Das Erstellen und Einführen einer Politik und Strategie zur Informationssicherheit ist ein zentraler Schritt für die Sicherheit von Unternehmensdaten. Dieser Prozess beinhaltet die Entwicklung klarer Leitlinien und Strategien, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten sowie die generellen Unternehmensziele zu unterstützen. Diese Sicherheitspolitik definiert die grundlegenden Prinzipien und Ziele, während die Strategie konkrete Wege zur Umsetzung dieser Ziele vorgibt. Die Integration dieser Dokumente in den Unternehmensbetrieb und die Kommunikation an alle Beteiligten sind entscheidend, um ein Bewusstsein für Informationssicherheit zu schaffen und eine konsistente Umsetzung zu gewährleisten.
- (2) Es ist wichtig zu beachten, dass eine Sicherheitsstrategie massgeschneidert sein sollte, um den spezifischen Bedürfnissen und Risiken eines Unternehmens und der Organisationseinheiten gerecht zu werden. Darüber hinaus ist die Zusammenarbeit mit Sicherheitsexperten und die Einhaltung bewährter Praktiken entscheidend, um eine effektive Sicherheitsstrategie zu entwickeln und umzusetzen.

Die folgenden Dokumente unterstützen den Anwender bei der Erstellung und Einführung der Politik und Strategie der Informationssicherheit:



- Nationale Cyberstrategie (NCS) vom April 2023
- Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022
- Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022
- Wirksamkeitsüberprüfung «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018 bis 2022»
- Integrierte Sicherheit für Deutschland, Nationale Sicherheitsstrategie



**Empfehlung der VSE Cyber Security Task Force Experten:**

Das Erstellen und Einführen einer Politik und Strategie zur Informationssicherheit ist essenziell, um klare Leitlinien festzulegen, die die Basis für die Sicherung von Informationen bilden und die Ausrichtung aller Aktivitäten und Massnahmen auf dieses Ziel ermöglichen.





## 6.2.2 Rahmen der Informationssicherheit festlegen: Erstellen einer Direktive zur Informationssicherheit und eine Richtlinie zum Rahmen der Informationssicherheit

- (1) Die Festlegung des Rahmens für Informationssicherheit ist ein notwendiger Schritt, um einen klaren Kontext für den Schutz von Informationen zu schaffen. Dieser Prozess umfasst die Definition von Schlüsselaspekten wie Verantwortlichkeiten, Ziele und den Anwendungsbereich der Informationssicherheit. Der Rahmen bildet die Grundlage für Richtlinien, Verfahren und Massnahmen, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sicherzustellen. Eine klare Festlegung des Rahmens schafft ein solides Fundament für das gesamte Informationssicherheitsmanagement und trägt dazu bei, eine kohärente und effektive Sicherheitsstrategie zu entwickeln.
- (2) Die Erstellung einer Informationssicherheitsdirektive erfordert eine gründliche Analyse der Bedürfnisse und Risiken Ihrer Organisation. Sie sollte klare Anweisungen und Prinzipien zur Informationssicherheit bereitstellen und durch die Führungsebene erstellt und unterstützt werden.
- (3) Die Erstellung einer Richtlinie für den Rahmen der Informationssicherheit ist ein zentraler Schritt, um klare Leitlinien für den Schutz von Unternehmensdaten festzulegen. Diese Richtlinie definiert den Kontext, in dem die Informationssicherheit operiert, einschliesslich Verantwortlichkeiten, Ziele und den Geltungsbereich. Sie bildet das grundlegende Regelwerk, auf dem weitere Sicherheitsmassnahmen aufbauen. Eine gut durchdachte Richtlinie stellt sicher, dass alle Beteiligten ein gemeinsames Verständnis für die Sicherheitsanforderungen haben und fördert eine kohärente Umsetzung von Informationssicherheitsmassnahmen im gesamten Unternehmen und Organisationseinheiten.



### In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



### Folgende Dokumente helfen dem Anwender bei der Erstellung und Einführung einer Richtlinie Informationssicherheit und der Richtlinie Bereich Informationssicherheit:

- NIST SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise



### Empfehlung der VSE Cyber Security Task Force Experten:

**Die Festlegung eines Rahmens für die Informationssicherheit ist wichtig, um die Grundprinzipien, Ziele und Verantwortlichkeiten für den Schutz von Informationen zu definieren und sicherzustellen, dass alle Sicherheitsmassnahmen konsistent und effektiv umgesetzt werden.**

## 6.2.3 Schaffung der Voraussetzungen

- (1) Die Schaffung der Voraussetzungen für die Einführung und den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) ist ein wichtiger Schritt, um die Sicherheit von Unternehmensdaten zu gewährleisten. Dieser Prozess beinhaltet die Bereitstellung der notwendigen Ressourcen, die Festlegung von Verantwortlichkeiten und die Etablierung eines klaren Rahmens für das ISMS. Durch die Schaffung dieser Grundlagen wird sichergestellt, dass das ISMS effektiv implementiert und langfristig betrieben werden kann. Eine sorgfältige Vorbereitung legt den Grundstein für den Erfolg des Informationssicherheitsmanagementsystems und gewährleistet einen umfassenden Schutz der Informationen.



### In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



**Die Einführung eines ISMS erfordert beträchtliche Ressourcen in den Unternehmen und Organisationseinheiten. Der Aufwand ist nicht zu unterschätzen. Diese Umstände sind bei der Schaffung der Voraussetzungen zu berücksichtigen.**



### Empfehlung der VSE Cyber Security Task Force Experten:

**Die Schaffung der Voraussetzungen für die Einführung und den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) ist wichtig, um eine strukturierte und effektive Herangehensweise an die Informationssicherheit zu gewährleisten, die Einhaltung von Standards zu fördern und das Vertrauen von Stakeholdern zu stärken.**



#### 6.2.4 Ermittlung des Status Quo / IST-Analyse im Bereich Informationssicherheit durchführen

- (1) Die Ermittlung des Status Quo oder die IST-Analyse im Bereich der Informationssicherheit ist ein grundlegender Schritt, um den aktuellen Stand der Sicherheitspraktiken zu verstehen. Dieser Prozess beinhaltet die gründliche Analyse bestehender Sicherheitsmassnahmen, Schwachstellen und Richtlinien. Durch die IST-Analyse werden die Stärken und Schwächen im Sicherheitsbereich identifiziert, um eine fundierte Grundlage für die Entwicklung von Sicherheitsstrategien zu schaffen. Eine genaue Ermittlung des IST-Zustands ermöglicht es, gezielte Massnahmen zur Verbesserung der Informationssicherheit zu planen und umzusetzen.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



**Für den Status Quo / IST-Analyse im Bereich Informationssicherheit der Kontrollen im Rahmen des NIST Cybersecurity Frameworks (CSF) 1.1 soll das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" verwendet werden.**



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.**



**Für den Status Quo / IST-Analyse im Bereich Informationssicherheit der Kontrollen im Rahmen der ISO 27001 Annex A soll das "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002" verwendet werden.**



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**



**Im Anhang befindet sich eine ausführliche Beschreibung für das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002".**

#### 6.2.5 Geltungsbereich des gesamten ISMS festlegen

- (1) Die Festlegung des Geltungsbereichs im Rahmen der Informationssicherheit ist ein essenzieller Schritt bei der Implementierung eines Information Security Management Systems. Dabei wird präzise definiert, welche Teile der Organisation und welche Informationssysteme im ISMS berücksichtigt werden. Dieser Prozess umfasst die Identifizierung von Assets, Geschäftsprozessen und externen Partnern, die in den Anwendungsbereich des ISMS fallen.
- (2) Eine klare Festlegung des Geltungsbereichs schafft die Grundlage für die Entwicklung von Sicherheitsrichtlinien und -Massnahmen. Die Festlegung ermöglicht es, Risiken angemessen zu identifizieren, zu bewerten und entsprechende Schutzmassnahmen zu implementieren. Dies trägt dazu bei, eine effektive und zielgerichtete Informationssicherheitsstrategie zu entwickeln und sicherzustellen, dass alle relevanten Bereiche der Organisation angemessen geschützt sind.
- (3) Es ist wichtig zu betonen, dass der Geltungsbereich nicht statisch ist und im Laufe der Zeit eventuell angepasst werden muss. Änderungen in der Organisationsstruktur, Geschäftsprozessen oder der Bedrohungslandschaft können eine Anpassung des Geltungsbereichs erforderlich machen. Daher ist es wichtig, den Geltungsbereich regelmässig zu überprüfen und bei Bedarf anzupassen.
- (4) Die Festlegung des Geltungsbereichs bildet die Grundlage für die Entwicklung von Sicherheitszielen, die Implementierung von Sicherheitsmassnahmen und die Durchführung von Audits im Rahmen des ISMS. Ein klar definierter Geltungsbereich ermöglicht es der Organisation, ihre Informationssicherheitsbemühungen gezielt auf die relevanten Bereiche zu konzentrieren und sicherzustellen, dass das ISMS effektiv und effizient eingesetzt wird.
- (5) Der Geltungsbereich für die Informationssicherheit für die Unternehmen und Organisationseinheiten ist durch die Vorgaben im Strom VV definiert und muss somit von den Unternehmen und Organisationseinheiten übernommen bzw. abgedeckt werden.



- (6) Unternehmen und Organisationseinheiten müssen entscheiden, ob sie den Geltungsbereich für die Informationssicherheit nicht nur auf die Vorgaben im Strom VV begrenzen werden.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-02-01: Richtlinie Bereich Informationssicherheit: Informationssicherheits-Rahmen
- HoP-01-01-02: Richtlinie Bereich Informationssicherheit: Geltungsbereich, Aufbau und Organisation des ISMS



Die VSE Cyber Security Task Force Experten empfehlen den Geltungsbereich für die Informationssicherheit auf das gesamte Unternehmen auszuweiten und nicht nur auf die Vorgaben des Strom VV zu beschränken. Es sollen alle Bereiche des Unternehmens ganzheitlich und vollumfänglich abgedeckt werden. Dabei muss entschieden werden, ob die Vorgaben im Strom VV für den gesamten Bereich der Informationssicherheit übernommen wird oder ob für die nicht durch das Strom VV regulierten Bereiche eigene Vorgaben definiert werden.

#### 6.2.6 Sicherheitsorganisation aufbauen und anpassen

- (1) Der Aufbau einer Sicherheitsorganisation zur Steigerung der IKT-Resilienz ist unerlässlich, um sicherzustellen, dass Unternehmen und Organisationseinheiten widerstandsfähig gegenüber Störungen, Katastrophen und Sicherheitsbedrohungen im digitalen Bereich ist. Ein typischer Aufbau einer Sicherheitsorganisation im Zusammenhang mit der Steigerung der IKT-Resilienz ist unter Punkt 5.4.7. aufgeführt.
- (2) Die genaue Struktur und Verantwortlichkeiten können je nach Unternehmen und Organisationseinheiten variieren und sollten an die spezifischen Anforderungen und Risiken der Unternehmen und Organisationseinheiten angepasst werden. Eine gut koordinierte Sicherheitsorganisation, die sich auf IKT-Resilienz konzentriert, ist entscheidend, um sicherzustellen, dass das Unternehmen und die Organisationseinheiten in der Lage ist, auf IKT-Störungen und Sicherheitsbedrohungen effektiv zu reagieren und ihren digitalen Betrieb aufrechtzuerhalten.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-02-01: Richtlinie Bereich Informationssicherheit: Informationssicherheits-Rahmen
- HoP-01-01-02: Richtlinie Bereich Informationssicherheit: Geltungsbereich, Aufbau und Organisation des ISMS



Empfehlung der VSE Cyber Security Task Force Experten:

Beim Aufbau der Sicherheitsorganisation müssen alle Elemente der Informationssicherheit abgedeckt werden. Die bedingt auch, dass die Schnittstellen zu externen Stakeholdern wie Hersteller / Lieferanten, SOC, CERT usw. definiert werden.

#### 6.2.7 Verantwortlichkeiten definieren / anpassen

- (1) Die Definition der Verantwortlichkeiten im Rahmen der Informationssicherheit und des Information Security Management Systems (ISMS) ist ein wichtiger Schritt, um sicherzustellen, dass alle relevanten Akteure klare Rollen und Zuständigkeiten im Sicherheitskontext verstehen und erfüllen. Dieser Prozess beginnt oft mit der Identifikation der Schlüsselakteure und ihrer spezifischen Aufgaben.
- (2) Die Festlegung von Verantwortlichkeiten beginnt auf höchster Führungsebene. Die Geschäftsleitung oder das Top-Management trägt die Gesamtverantwortung für die Sicherheit der Informationssysteme. Dies schließt die Festlegung von Sicherheitsrichtlinien, Zielen und Ressourcenallokation ein.
- (3) Auf der nächsten Ebene sind Sicherheitsverantwortliche oder Information Security Officer (ISO) oft für die Umsetzung und Überwachung der Informationssicherheitsstrategie verantwortlich. Sie stellen sicher, dass die Sicherheitsvorgaben auf operativer Ebene durchgesetzt werden.
- (4) IT/OT-Verantwortliche spielen ebenfalls eine Schlüsselrolle, da sie für die technische Umsetzung von Sicherheitsmassnahmen, den Schutz von Systemen und die Kontrolle des Datenzugriffs verantwortlich sind. Netzwerkadministratoren, Systemadministratoren und andere technische Teams können spezifische Verantwortlichkeiten im Rahmen der technischen Sicherheit haben.
- (5) Auf Mitarbeiterebene tragen alle Benutzer eine gewisse Verantwortung für die Sicherheit der Informationen, insbesondere im Hinblick auf den sicheren Umgang mit Daten und die Einhaltung von Sicherheitsrichtlinien. Schulungen und Awareness-Programme sind entscheidend, um sicherzustellen, dass alle Mitarbeiter ihre Rolle im Sicherheitskonzept verstehen.



- (6) Compliance-Beauftragte könnten für die Einhaltung von Sicherheitsstandards und externen Vorschriften verantwortlich sein. Datenschutzbeauftragte (DSB) kümmern sich um die Einhaltung der Datenschutzbestimmungen.
- (7) Die Zusammenarbeit zwischen den verschiedenen Verantwortlichkeiten ist entscheidend, um eine ganzheitliche und effektive Sicherheitsstrategie zu gewährleisten. Klar definierte Verantwortlichkeiten fördern die Transparenz, erleichtern die Koordination von Sicherheitsmassnahmen und erleichtern die Identifizierung von Schwachstellen oder Handlungsbedarf.
- (8) Weiter müssen die Verantwortlichen für die Schnittstellen zu externen Stakeholdern wie Hersteller / Lieferanten, Bundesstellen wie BACS, SOC, CERTs, Partnern usw. bestimmt werden
- (9) Insgesamt ist die Definition von Verantwortlichkeiten ein dynamischer Prozess, der sich an die sich ändernden Anforderungen und Bedrohungen anpasst. Es erfordert kontinuierliche Kommunikation und Zusammenarbeit, um sicherzustellen, dass alle Stakeholder ihre Rolle im Rahmen der Informationssicherheit verstehen und aktiv dazu beitragen.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-02-01: Richtlinie Bereich Informationssicherheit: Informationssicherheits-Rahmen
- HoP-01-01-02: Richtlinie Bereich Informationssicherheit: Geltungsbereich, Aufbau und Organisation des ISMS



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Definition der Verantwortlichkeiten im Rahmen der Informationssicherheit und des ISMS ist wichtig, um klare Zuständigkeiten festzulegen, die Sicherheitsmassnahmen effektiv umzusetzen, Risiken zu minimieren und die Integrität der Informationssicherheit zu gewährleisten.**

#### 6.2.8 Leistungsindikatoren (KPI) definieren

- (1) Die Definition von Leistungsindikatoren (KPIs) im Rahmen der Informationssicherheit und des ISMS ist entscheidend für die Messung und kontinuierliche Verbesserung der Sicherheitsmassnahmen. KPIs sind quantitative Messgrössen, die die Leistung in Schlüsselbereichen der Informationssicherheit ausweisen.
- (2) Die Auswahl der KPIs basiert auf den strategischen Zielen des ISMS und den spezifischen Sicherheitsanforderungen der Organisation. Beispiele für KPIs könnten die Anzahl der Sicherheitsvorfälle pro Monat, die durchschnittliche Behebungszeit von Schwachstellen, die Erfolgsquote von Sicherheitsschulungen oder die regelmässige Überprüfung von Zugriffsprotokollen sein.
- (3) Die Definition der KPIs erfordert eine klare Verbindung zu den Sicherheitszielen, z.B. die Reduzierung von Sicherheitsvorfällen. KPIs sollten spezifisch, messbar, erreichbar, relevant und zeitgebunden (SMART) sein. Die regelmässige Überprüfung und Anpassung der KPIs ist wichtig, um den aktuellen Sicherheitskontext und sich ändernde Geschäftsanforderungen zu berücksichtigen.
- (4) Die Definition von KPIs geht oft Hand in Hand mit der Ermittlung einer Baseline für die Leistungsmessung. Eine klare Kommunikation der KPIs an Stakeholder fördert ein gemeinsames Verständnis und trägt zur Erreichung der Sicherheitsziele der Organisation bei. Insgesamt bieten gut definierte KPIs im ISMS eine objektive Grundlage für die Bewertung der Sicherheitsleistung und ermöglichen eine gezielte Verbesserung im Einklang mit den strategischen Unternehmenszielen.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-02-01: Richtlinie Bereich Informationssicherheit: Informationssicherheits-Rahmen
- HoP-01-01-02: Richtlinie Bereich Informationssicherheit: Geltungsbereich, Aufbau und Organisation des ISMS



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Definition von Leistungsindikatoren (KPIs) für die Informationssicherheit und das ISMS ist wichtig, um die Effektivität der Sicherheitsmassnahmen zu messen, Schwachstellen zu identifizieren und kontinuierliche Verbesserungen zu ermöglichen.**

#### 6.2.9 Vorgehen für Audits definieren

- (1) Das Vorgehen bei Audits im Rahmen der Informationssicherheit und des Information Security Management Systems (ISMS) ist ein strukturierter Prozess, der die Einhaltung von Sicherheitsrichtlinien, -verfahren und -standards überprüft. Audits sind entscheidend für die Effektivität des ISMS und die kontinuierliche Verbesserung der Informationssicherheit.





- (2) Der Auditprozess beginnt mit der Festlegung des Prüfungsbereichs und der Prüfziele, die im Einklang mit den Sicherheitszielen des ISMS und den Unternehmenszielen stehen. Die Durchführung des Audits beinhaltet die systematische Überprüfung von Sicherheitsdokumentationen, Prozessen und technischen Implementierungen, einschliesslich dem Miteinbezug von Verantwortlichen Rollen und Funktionen.
- (3) Die Analyse der Audit-Ergebnisse identifiziert Abweichungen von Standards und bewertet positive Aspekte. Der daraus resultierende Auditbericht enthält Empfehlungen für Verbesserungen, identifizierte Schwachstellen und positive Aspekte. Dieser Bericht wird an relevante Stakeholder und die Führungsebene weitergeleitet.
- (4) Die Umsetzung von Korrekturmassnahmen ist ein entscheidender Schritt, um identifizierte Schwachstellen zu beheben und die Informationssicherheit zu stärken. Dieser transparente Prozess beinhaltet die Rückmeldung der Audit-Ergebnisse an die betroffenen Bereiche. Insgesamt ermöglicht das strukturierte Vorgehen bei Audits im ISMS eine objektive Bewertung der Informationssicherheit und trägt zur kontinuierlichen Verbesserung bei, um sicherzustellen, dass die Sicherheitsmassnahmen den definierten Standards entsprechen und auf aktuelle Bedrohungen ausgerichtet sind.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-02-01: Richtlinie Bereich Informationssicherheit: Informationssicherheits-Rahmen
- HoP-01-01-02: Richtlinie Bereich Informationssicherheit: Geltungsbereich, Aufbau und Organisation des ISMS

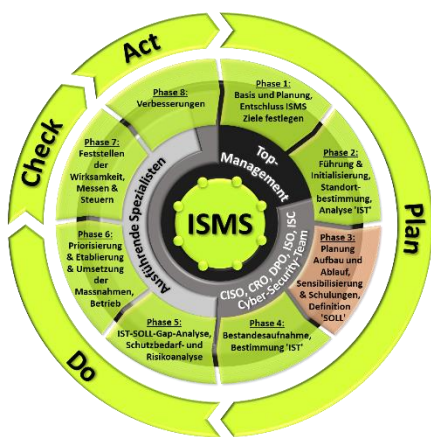


**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Erstellung eines Auditplans hilft den Verantwortlichen, die Audits angemessen über das Jahr zu planen und die notwendigen Ressourcen zu allozieren. Ebenfalls gibt es eine Übersicht über die Sicherheitsbereiche, welche überprüft werden sollen.

### 6.3 Phase 3: Planung Aufbau und Ablauf; Sensibilisierung und Schulungen; Definition 'SOLL'

- (1) In der dritten Phase der Einführung eines ISMS steht die Planung, der Aufbau und Ablauf des ISMS sowie Sensibilisierung und Schulungen und die Ziel-Definition (SOLL) im Vordergrund:



<b>Verantwortlich:</b>	Top-Management, C-Level
<b>Zuständig:</b>	CISO, CRO, DPO, ISO, ISC, Cyber Security Team
<b>Involvierte Stellen:</b>	Spezifische Mitarbeiter der Informationssicherheit, externe Experten und Berater
<b>Zu behandelnde Punkte</b>	<ul style="list-style-type: none"> <li>■ ISMS implementieren, etablieren, anpassen und erweitern</li> <li>■ Dokumentenlenkung einführen / anpassen</li> <li>■ Dokumente mit Fokus auf die Baseline des ISMS (Richtlinien, Guidelines, Arbeitsanleitungen usw.) erstellen, ergänzen und anpassen</li> <li>■ Sicherheitsorganisation etablieren / befähigen / anpassen</li> <li>■ Mitarbeiter im Bereich Informationssicherheit einbinden</li> <li>■ Awareness &amp; Schulungen einführen / erweitern / anpassen</li> <li>■ Das 'Soll' für die Informationssicherheit definieren</li> <li>■ Massnahmenkatalog erstellen</li> <li>■ Audits planen</li> </ul>

**Tabelle 9:** ISMS Phase 3: Planung Aufbau und Ablauf; Sensibilisierung und Schulungen; Definition 'SOLL'

#### 6.3.1 ISMS einführen, anpassen und erweitern

- (1) Die Implementierung, Etablierung, Anpassung und Erweiterung eines Information Security Management Systems (ISMS) ist ein fortlaufender Prozess, der darauf abzielt, die Informationssicherheit einer Organisation sicherzustellen und kontinuierlich zu verbessern.
  - **Implementierung des ISMS:** Beginnt mit der Festlegung eines klaren Rahmens, inklusive Kontext, Geschäftsziele und Anwendungsbereich. Klare Verantwortlichkeiten und eine Risikobewertung führen zur Festlegung konkreter Sicherheitsziele, die als Grundlage für Richtlinien, Verfahren und Prozesse dienen.



- **Etablierung des ISMS:** Erfordert starkes Engagement des Top-Managements, aktive Beteiligung und Ressourcenbereitstellung. Ein Mechanismus für kontinuierliche Verbesserungen wird eingeführt, begleitet von Schulungen und Sensibilisierungsmassnahmen für Mitarbeiter. Interne Audits überprüfen die Effektivität des ISMS.
  - **Anpassung des ISMS:** Ein dynamischer Prozess, bei dem die Organisation auf Veränderungen in Umfeld, Technologie und Bedrohungen reagiert. Das Top-Management spielt eine zentrale Rolle, um sicherzustellen, dass das ISMS aktuellen Anforderungen entspricht. Kontinuierliche Schulungen und Audits dienen der regelmässigen Überprüfung und Anpassung.
  - **Erweiterung des ISMS:** Beinhaltet die Integration mit anderen Managementsystemen, um eine ganzheitliche Herangehensweise sicherzustellen. Die Organisation stellt sicher, dass das ISMS Compliance-Anforderungen erfüllt. Neue Technologien und sich wandelnde Bedrohungen werden berücksichtigt, um das ISMS kontinuierlich zu erweitern und zu verbessern.
- (2) Insgesamt erfordert dieser Prozess eine proaktive Haltung, kontinuierliche Überwachung und Anpassung. Durch eine fortlaufende Verpflichtung kann die Organisation sicherstellen, dass ihr ISMS robust und effektiv bleibt und den sich ständig ändernden Anforderungen an die Informationssicherheit gerecht wird.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-02-01: Richtlinie Bereich Informationssicherheit: Informationssicherheits-Rahmen
- HoP-01-01-02: Richtlinie Bereich Informationssicherheit: Geltungsbereich, Aufbau und Organisation des ISMS



In den folgenden Dokumenten sind Orientierungshilfen und Anleitungen:

- BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)



**Empfehlung der VSE Cyber Security Task Force Experten:**

ISMS einführen, anpassen und erweitern ist ein Prozess, welcher stetig angepasst und kontinuierlich verbessert wird. Es ist wichtig, dass die notwendigen Vorgaben und Dokumente stets auf den neusten Stand und allen betroffenen Mitarbeitenden jederzeit zur Verfügung stehen.

### 6.3.2 Dokumentenlenkung einführen / anpassen

- (1) Die Einführung der Dokumentenlenkung im ISMS gewährleistet systematisch erstellte, genehmigte, überwachte und aktualisierte Sicherheitsdokumente. Dieser Schritt umfasst die Identifikation relevanter Dokumente und die Festlegung von klaren Verfahren und Verantwortlichkeiten für ihre Erstellung. Versionskontrollen gewährleisten die Verwendung aktueller Dokumente, während Genehmigungsverfahren sicherstellen, dass sie vor Inkrafttreten überprüft werden.
- (2) Regelmässige Überwachung und Aktualisierung, besonders bei Änderungen von Sicherheitsanforderungen oder Gesetzen, gewährleisten die Aktualität der Dokumente. Das effektive Dokumentenlenkungssystem fördert Transparenz, Zugänglichkeit und erleichtert die Einhaltung von Standards im ISMS.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01-01-04: Arbeitsanleitung Bereich Informationssicherheit: Dokumentenlenkung



**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Einführung einer Dokumentenlenkung und deren kontinuierliche Anpassungen sind wichtig, um die Konsistenz und Aktualität von Policies und Sicherheitsdokumentationen sicherzustellen, was die Effektivität des Informationssicherheitsmanagementsystems erhöht und die Einhaltung von Standards fördert. Die Dokumentlenkung wird im Bereich Integrierte Management Systeme (IMS) erstellt und verwaltet. Somit ist eine Absprache mit den anderen Bereichen im Unternehmen zwingend erforderlich.

### 6.3.3 Baseline-Dokumente mit Fokus auf die Baseline des ISMS (Richtlinien, Guidelines, Arbeitsanleitungen usw.) erstellen, ergänzen und anpassen

- (1) Die Erstellung von Dokumenten mit Fokus auf die Baseline des Information Security Management Systems im Rahmen der Informationssicherheit ist ein entscheidender Prozess, um klare und verbindliche Richtlinien, Guidelines und Arbeitsanleitungen zu schaffen. Diese Dokumente dienen als Grundlage für die Sicherheitspraktiken innerhalb der Organisation und tragen dazu bei, ein kohärentes Sicherheitsumfeld zu etablieren.



- (2) Der Prozess beginnt mit einer umfassenden Analyse der Sicherheitsanforderungen und -ziele der Organisation. Hierbei werden die spezifischen Bedrohungen, Risiken und geschäftlichen Anforderungen berücksichtigt. Auf Grundlage dieser Analyse werden die erforderlichen Dokumente identifiziert, wie Sicherheitsrichtlinien, Guidelines und Arbeitsanleitungen.
- (3) Die Erstellung von Sicherheitsrichtlinien erfordert eine klare Formulierung der Grundsätze und Verhaltensregeln im Bereich der Informationssicherheit. Diese Richtlinien sollten die strategischen Ziele des ISMS widerspiegeln und allgemeinverständlich sein, um von allen Mitarbeitern umgesetzt werden zu können.
- (4) Guidelines bieten detaillierte Anleitungen und Empfehlungen für spezifische Sicherheitsaspekte. Dies kann beispielsweise die sichere Konfiguration von Systemen, die Handhabung von Zugriffsrechten oder die sichere Nutzung von IT-Ressourcen umfassen. Guidelines ergänzen die Richtlinien, indem sie konkrete Handlungsanweisungen bereitstellen.
- (5) Arbeitsanleitungen bieten detaillierte Schritte und Abläufe für bestimmte Aufgaben im Zusammenhang mit der Informationssicherheit. Dies könnte die Durchführung von Sicherheitsüberprüfungen, die Meldung von Sicherheitsvorfällen oder die Umsetzung von Sicherheitsmassnahmen beinhalten.
- (6) Die Erstellung dieser Dokumente erfordert eine enge Zusammenarbeit zwischen den Verantwortlichen für Informationssicherheit, Fachexperten und relevanten Stakeholdern. Es ist wichtig sicherzustellen, dass die Dokumente präzise, konsistent und für die Zielgruppe verständlich sind.
- (7) Die Versionierung und Aktualisierung dieser Dokumente ist notwendig, um sicherzustellen, dass sie den aktuellen Bedrohungen und technologischen Entwicklungen entsprechen. Regelmässige Überprüfungen und Aktualisierungen sollten in den Prozess der Dokumentenerstellung integriert werden.
- (8) Die Erstellung von Dokumenten mit Fokus auf die Baseline des ISMS spielt eine zentrale Rolle bei der Festlegung von Standards und Best Practices im Bereich der Informationssicherheit. Gut strukturierte und verständliche Dokumente tragen wesentlich dazu bei, dass Sicherheitsrichtlinien und -verfahren effektiv umgesetzt werden können.



Mit Hilfe des "VSE-NIST-CSF-1.1\_HoP-Mapping-Tool" können die einzelnen Punkte aus dem NIST CSF 1.1 den entsprechenden Dokumenten zugewiesen werden. So wird sichergestellt, dass alle Punkte behandelt werden.



Im "VSE-ISO27002-Annex-A\_HoP-Mapping-Tool" können im Vorfeld zur Erstellung der Dokumente die einzelnen Elemente der ISO 27001 Annex A zu den Dokumenten im HoP zugewiesen werden. So wird sichergestellt, dass alle Punkte behandelt werden.



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**



**In den Beilagen sind Musterbeispiele, welche angewendet werden können:**

- HoP-01-00-00 Richtlinie Integrierte Management Systeme (IMS)
- HoP-01-00-00-01 Arbeitsanleitung Bereich IMS: House of Prozess
- HoP-01-00-00-02 Arbeitsanleitung Bereich IMS: House of Policy
- HoP-01-00-00-03 Arbeitsanleitung Bereich IMS: Dokumentenlenkung
- HoP-01-00-01-04 Arbeitsanleitung Bereich IMS: Audits
- HoP-01-01 Direktive Informationssicherheit & Informationssicherheitsmanagement ISM
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-01-01 Arbeitsanleitung Bereich ISM: Informationssicherheit Organisation
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS
- HoP-01-01-03-01 Arbeitsanleitung Bereich ISMS: Grundsatz Informationssicherheit (Datensicherheit)
- HoP-01-01-03-02 Arbeitsanleitung Bereich ISMS: IT-OT-Risiko-Management
- HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung
- HoP-01-01-03-04 Arbeitsanleitung Bereich ISMS: Schulung und Sensibilisierung
- HoP-01-01-03-05 Arbeitsanleitung Bereich ISMS: Physische Sicherheit der IKT-Assets
- HoP-01-01-03-06 Arbeitsanleitung Bereich ISMS: Zugriffskontrolle
- HoP-01-01-03-07 Arbeitsanleitung Bereich ISMS: Multi Faktor Authentisierung
- HoP-01-01-03-08 Arbeitsanleitung Bereich ISMS: Management von privilegierten Zugriffsrechten



- HoP-01-01-03-09 Arbeitsanleitung Bereich ISMS: Systeme (Server und Client)
- HoP-01-01-03-10 Arbeitsanleitung Bereich ISMS: Leittechnikkomponenten
- HoP-01-01-03-11 Arbeitsanleitung Bereich ISMS: Betriebssysteme und Applikationen
- HoP-01-01-03-12 Arbeitsanleitung Bereich ISMS: Verschlüsselung
- HoP-01-01-03-13 Arbeitsanleitung Bereich ISMS: Netzwerke
- HoP-01-01-03-14 Arbeitsanleitung Bereich ISMS: Backup & Backup-Checkliste
- HoP-01-01-03-15 Arbeitsanleitung Bereich ISMS: Medienbereinigung
- HoP-01-01-03-16 Arbeitsanleitung Bereich ISMS: LOG-Management
- HoP-01-01-03-17 Arbeitsanleitung Bereich ISMS: Malware- und Schwachstellenmanagement
- HoP-01-01-03-18 Arbeitsanleitung Bereich ISMS: Management von Informationssicherheitsvorfällen (Incident Management)
- HoP-01-01-03-19 Arbeitsanleitung Bereich ISMS: Betriebskontinuitätsmanagement (BCM)
- HoP-01-01-03-20 Arbeitsanleitung Bereich ISMS: Notfallmanagement
- HoP-01-01-03-21 Arbeitsanleitung Bereich ISMS: Sicherheitsmassnahmen für Dienstleister
- HoP-01-01-03-22 Arbeitsanleitung Bereich ISMS: Lieferanten Management
- HoP-01-01-03-23 Arbeitsanleitung Bereich ISMS: Informationssicherheit im Personalbereich
- HoP-01-01-03-24 Arbeitsanleitung Bereich ISMS: Informationssicherheit in Projekten
- HoP-01-01-03-25 Arbeitsanleitung Bereich ISMS: Nutzung von Cloud-Services
- HoP-01-01-03-26 Arbeitsanleitung Bereich ISMS: Verwendung von maschinellem Lernen und künstlicher Intelligenz
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten
- HoP-01-01-04-01 Arbeitsanleitung Bereich ISM: Nutzung von mobilen Geräten
- HoP-01-01-04-02 Arbeitsanleitung Bereich ISM: Nutzung von OT-Assets



**Die Erstellung der Vorgabedokumente für die Baseline erfordert viel Ressourcen. Es müssen genügend Ressourcen zur Verfügung gestellt werden. Wichtig ist, dass alle Punkte vollumfänglich behandelt werden und die Dokumente für das Zielpublikum verständlich ist.**



#### **Empfehlung der VSE Cyber Security Task Force Experten:**

**Für die Erstellung der Dokumente der Baseline im ISMS wird ein systematisches Vorgehen vorgeschlagen. Zuerst sollen alle notwendigen Punkte zu jeder Vorgabe und jedem Dokument gesammelt werden und in die Grunddokumente eingefügt werden. Anschliessend können die Vorgaben und Dokumente gegliedert und in die definitive Form gebracht werden. Wichtig ist, dass die Dokumente kontinuierlich angepasst werden müssen, um so auf die aktuellsten Bedrohungen zu reagieren und die Massnahmen zu priorisieren.**

### **6.3.4 Sicherheitsorganisation etablieren / befähigen / anpassen**

- (1) Die Etablierung und Befähigung der Sicherheitsorganisation im Rahmen der Informationssicherheit und des Information Security Management Systems (ISMS) ist ein umfassender Prozess, der darauf abzielt, eine robuste Struktur zu schaffen und die notwendigen Ressourcen bereitzustellen, um die Informationssicherheit effektiv zu gewährleisten.
- (2) Zu Beginn steht die Definition der Sicherheitsorganisation, einschliesslich der Benennung von Schlüsselpositionen und Verantwortlichkeiten. Dies könnte die Rolle des Chief Information Security Officers (CISO) oder eines Sicherheitsverantwortlichen, Datenschutzbeauftragten, IT-Sicherheitsexperten und anderer Funktionen umfassen. Die Verantwortlichkeiten sollten klar definiert sein und sich auf die strategischen Ziele des ISMS beziehen.
- (3) Die Etablierung der Sicherheitsorganisation erfordert auch die Integration von Sicherheitsaspekten in die organisatorische Struktur. Dies bedeutet, dass die Sicherheitsfunktion nicht isoliert, sondern in die verschiedenen Abteilungen und Ebenen der Organisation integriert wird. Dies fördert eine ganzheitliche Sicherheitskultur.
- (4) Die Befähigung der Sicherheitsorganisation beinhaltet die Bereitstellung von Schulungen und Ressourcen, um sicherzustellen, dass die Sicherheitsfachleute und Mitarbeiter in der Organisation über die erforderlichen Fähigkeiten und Kenntnisse verfügen. Schulungen könnten Themen wie sichere Programmierung, Datenschutz, Risikomanagement und andere relevante Sicherheitsaspekte abdecken.
- (5) Die Sicherheitsorganisation sollte über die notwendigen Befugnisse verfügen, um Sicherheitsentscheidungen zu treffen und Massnahmen durchzusetzen. Dies könnte die Einführung von Sicherheitsrichtlinien, die Überwachung der Einhaltung von Sicherheitsstandards und die Durchführung von Sicherheitsaudits umfassen.





- (6) Es ist wichtig sicherzustellen, dass die Sicherheitsorganisation effektiv mit anderen relevanten Funktionen der Organisation zusammenarbeitet. Dazu gehören die IT/OT-Organisationseinheiten, die Rechtsabteilung, das Risikomanagement und andere relevante Bereiche. Die Kommunikation und Zusammenarbeit zwischen diesen Funktionen sind entscheidend, um eine ganzheitliche Sicherheitsstrategie zu entwickeln und umzusetzen.
- (7) Die Sicherheitsorganisation sollte auch in der Lage sein, auf sich verändernde Bedrohungen und Technologien zu reagieren. Dies erfordert eine regelmässige Überprüfung und Anpassung der Sicherheitsstrategie sowie die Integration von Best Practices und Innovationen in die Sicherheitspraktiken.
- (8) Insgesamt ist die Etablierung und Befähigung der Sicherheitsorganisation ein kontinuierlicher Prozess, der auf die Schaffung einer starken Sicherheitskultur abzielt. Eine gut aufgestellte und befähigte Sicherheitsorganisation ist entscheidend für den Erfolg des ISMS und die effektive Bewältigung von Informationssicherheitsrisiken.



**Die Etablierung, Befähigung und das Anpassen der Sicherheitsorganisation sind die ersten Schritte zu einer erfolgreichen Initialisierung der Wirkung des ISMS.**



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Eine den Bedürfnissen des Unternehmens und der Organisationseinheiten entsprechende Sicherheitsorganisation muss aufgebaut, etabliert und befähigt werden. Die betroffenen Funktionen müssen sich ihrer Verantwortung bewusst sein und über die entsprechenden Fähigkeiten und Kompetenzen verfügen.**

### 6.3.5 Einbinden aller Mitarbeitenden für die Etablierung einer unternehmensweiten Sicherheitskultur

- (1) Die Mitarbeiterintegration im ISMS zielt darauf ab, eine umfassende Sicherheitskultur zu etablieren und die ISMS-Effektivität zu maximieren. Klare Kommunikation auf allen Ebenen betont die Bedeutung von Informationssicherheit für jeden Mitarbeitenden.
- (2) Schulungen und Awareness-Programme sensibilisieren für Gefahren und Best Practices, angepasst an die Organisation. Integration in Arbeitsabläufe, Mitarbeit im Entwicklungsprozess von Sicherheitsrichtlinien und -verfahren sowie klare Kommunikation fördern eine aktive Beteiligung und Eigenverantwortung der Mitarbeitenden. Feedback-Mechanismen und Meldewege für Sicherheitsvorfälle schaffen und schulen, sowie eine offene Kommunikationskultur etablieren. Einbeziehung von Mitarbeitern in die Gestaltung von Sicherheitsprozessen und -Massnahmen fördert eine partizipative Sicherheitskultur.
- (3) Die kontinuierliche Einbindung trägt dazu bei, eine breite Unterstützung für Informationssicherheit zu schaffen, die ISMS-Effektivität zu stärken und das Sicherheitsbewusstsein in der gesamten Organisation zu fördern.



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Einbindung aller Mitarbeitenden im Bereich der Informationssicherheit soll zeitnah und wiederkehrend erfolgen. Die Mitarbeitenden sind die Basis einer Sicherheitskultur jedes Unternehmens, welche durch deren Einbindung gestärkt wird.**

### 6.3.6 Awareness & Schulungen einführen / erweitern / anpassen

- (1) Die Planung, Einführung, Erweiterung und Anpassung eines Programms für Awareness und Schulungen im Bereich Informationssicherheit und Information Security Management System (ISMS) sind kritische Schritte, um sicherzustellen, dass Mitarbeiter über die erforderlichen Kenntnisse verfügen, um die Informationssicherheit der Organisation zu gewährleisten.
  - **Planung des Awareness- und Schulungsprogramms:** Die Planung beginnt mit einer umfassenden Analyse der Schulungsbedürfnisse. Dies beinhaltet die Identifizierung von Mitarbeitern, die in sicherheitsrelevanten Funktionen arbeiten, sowie die Bestimmung von Schlüsselbereichen, in denen das Bewusstsein gestärkt werden muss. Der Plan umfasst auch die Auswahl geeigneter Schulungsmethoden, einschliesslich Schulungen, Schulungsmaterialien, Workshops und möglicherweise Simulationen. Die Festlegung klarer Ziele, wie die Verbesserung des Verständnisses für Sicherheitsrichtlinien und die Sensibilisierung für potentielle Bedrohungen, ist ebenfalls von entscheidender Bedeutung.
  - **Einführung des Awareness- und Schulungsprogramms:** Die Einführung erfolgt durch klare Kommunikation an die Mitarbeiter. Das Top-Management spielt eine Schlüsselrolle, indem es die



Bedeutung von Informationssicherheit betont und die Notwendigkeit der Teilnahme an Schulungen unterstreicht. Die Implementierung umfasst die Bereitstellung von Ressourcen, Schulungsmaterialien und die Planung von Schulungsterminen. Es ist wichtig, dass die Schulungen auf die Bedürfnisse der Zielgruppe zugeschnitten sind und interaktive Elemente enthalten, um das Engagement zu fördern. Die Messung des Erfolgs erfolgt durch die Bewertung des Sicherheitsbewusstseins vor und nach den Schulungen.

- **Erweiterung des Awareness- und Schulungsprogramms:** Die Erweiterung des Programms beinhaltet die Integration neuer Schulungsinhalte in Reaktion auf sich ändernde Bedrohungen und Technologien. Dies kann die Einführung von Schulungen zu spezifischen Sicherheitsrichtlinien, Datenschutzbestimmungen oder neuen Technologien umfassen. Die Organisation strebt danach, das Bewusstsein der Mitarbeiter kontinuierlich zu schärfen, indem sie auf aktuelle Entwicklungen im Bereich der Informationssicherheit reagiert. Neue Schulungsmethoden oder -plattformen können ebenfalls integriert werden, um die Wirksamkeit des Programms zu steigern.
  - **Verbessern und Anpassungen des Awareness- und Schulungsprogramms:** Die Verbesserung und Anpassung erfolgt in Reaktion auf Rückmeldungen, Überprüfungen und veränderte Anforderungen. Regelmässige Bewertungen des Schulungsprogramms werden durchgeführt, um festzustellen, ob die Ziele erreicht wurden und ob Anpassungen erforderlich sind. Mitarbeiterfeedback wird aktiv gesammelt, um die Relevanz und Effektivität der Schulungen zu bewerten. Das Programm wird flexibel gehalten, um Änderungen in der Unternehmensstruktur, neue Technologien oder sich wandelnde Bedrohungen zu berücksichtigen.
- (2) Insgesamt erfordert ein erfolgreiches Awareness- und Schulungsprogramm eine durchdachte Planung, klare Kommunikation, kontinuierliche Anpassung und Erweiterung, um mit den sich ständig ändernden Anforderungen an die Informationssicherheit Schritt halten zu können.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-03-04 Arbeitsanleitung Bereich ISMS: Schulung und Sensibilisierung



**In den folgenden Dokumenten sind Orientierungshilfen und Anleitungen:**

- Schulungsprogramm nach NIST Special Publication 800-50



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Es wird empfohlen ein Schulungsprogramm nach NIST Special Publication 800-50 aufzubauen und umzusetzen.**

### 6.3.7 Das 'Soll' für die Informationssicherheit definieren (Definition des "Ziel")

- (1) Die Definition des "Soll"-Zustands für die Informationssicherheit im Rahmen des Information Security Management Systems (ISMS) ist ein entscheidender Schritt, um klare Zielsetzungen und Standards für die Sicherheit von Informationen in einer Organisation festzulegen. Der "Soll"-Zustand repräsentiert die angestrebte Vision der Informationssicherheit, die den geschäftlichen Anforderungen, gesetzlichen Vorgaben und Risikotoleranzen der Organisation entspricht.
- (2) In dieser Phase werden umfassende Sicherheitsziele und -anforderungen identifiziert, die auf den strategischen Zielen der Organisation basieren. Dies könnte die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, die Einhaltung gesetzlicher Vorschriften, die Reduzierung von Risiken und die Förderung einer Sicherheitskultur umfassen.
- (3) Die Definition des "Soll"-Zustands erfordert eine gründliche Analyse der Geschäftsprozesse, der Informationsflüsse und der zugrundeliegenden Technologien. Dabei werden mögliche Bedrohungen und Schwachstellen berücksichtigt, um sicherzustellen, dass die Sicherheitsziele präzise und umfassend sind.
- (4) Die Integration von Best Practices und branchenspezifischen Standards, wie beispielsweise ISO 27001, kann dabei helfen, einen robusten "Soll"-Zustand zu definieren. Diese Standards bieten Rahmenwerke für die Informationssicherheit, die von vielen Unternehmen und Organisationseinheiten weltweit akzeptiert werden.
- (5) Der "Soll"-Zustand sollte auch klare Vorgaben für Sicherheitsrichtlinien, Verfahren und Kontrollen beinhalten. Dies umfasst technische Aspekte wie Netzwerksicherheit, Zugriffskontrollen, Verschlüsselung, aber auch organisatorische Aspekte wie Schulungen, Bewusstseinsbildung und Incident-Response-Pläne.



- (6) Es ist wichtig, dass der "Soll"-Zustand nicht statisch ist, sondern sich an die sich wandelnden Geschäftsanforderungen, Technologien und Bedrohungen anpasst. Daher sollten regelmässige Überprüfungen und Aktualisierungen des "Soll"-Zustands durchgeführt werden, um sicherzustellen, dass er aktuell, realistisch und wirksam bleibt.
- (7) Die Definition des "Soll"-Zustands bildet die Grundlage für die gesamte Implementierung und den Betrieb des ISMS. Sie dient als Leitfaden für alle Sicherheitsaktivitäten und ermöglicht eine gezielte Ausrichtung der Ressourcen, um die angestrebten Sicherheitsziele zu erreichen. Der "Soll"-Zustand fungiert als Orientierungspunkt für die gesamte Informationssicherheitsstrategie und unterstützt die Organisation dabei, eine widerstandsfähige und effektive Sicherheitsumgebung aufzubauen.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



**Durch die Vorgaben des BFE im Strom VV sind die SOLL-Vorgaben gemäss NIST CSF 1.1 bereits definiert. Die verpflichteten Vorgaben müssen von den betroffenen Unternehmen und Organisationseinheiten in den entsprechenden Bereichen der Informationssicherheit als minimales Ziel übernommen werden.**



**Für die SOLL-Definition im Bereich Informationssicherheit der Kontrollen im Rahmen des NIST Cybersecurity Frameworks (CSF) 1.1 kann das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" verwendet werden. Die Vorgaben des BFE im Strom VV sind im Tool schon ersichtlich.**



**Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.**



**Für die SOLL-Definition im Informationssicherheit der Kontrollen im Rahmen der ISO 27001 Annex A soll das "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002" verwendet werden.**



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**



**Im Anhang befindet sich eine ausführliche Beschreibung für das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002".**



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Für die Durchführung der SOLL-Definitionen sollen die Tools angewendet werden, welche vom VSE zur Verfügung gestellt sind. Die "SOLL-Definition" soll so gewählt werden, dass die Ziele auch erreicht werden können!!!**

### 6.3.8 Massnahmenkatalog erstellen, Festlegen der anzuwendenden Massnahmen

- (1) Die Auswahl bzw. Festlegung der anzuwendenden Massnahmen in einen Massnahmenkatalog ist ein komplexer umfangreicher Prozess und entscheidend für das weitere Vorgehen. Zuerst müssen die Unternehmen und Organisationseinheiten festlegen, in welchem Bereich welche Massnahmen von welchen Frameworks oder Standards ausgewählt werden sollen. Unternehmen und Organisationseinheiten müssen sich auf eine Familie von Massnahmen, eventuell auch auf einen Mix zwischen den vorhandenen Quellen wie z.B. NIST Publication 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix und ISO 27002 festlegen. Viele Massnahmen in den aufgeführten Quellen sind identisch, darum muss genau entschieden werden, auf welche Quelle man sich fokussiert. Im Rahmen des IKT-Minimalstands findet eine Konzentration auf NIST Publication 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix statt, da diese umfangreich sind und alle Anforderungen für die Steigerung der IKT-Resilienz abdecken. Durch die Definition der Anwendbarkeit und der SoA wurden schon in einem ersten Schritt die notwendigen Bereiche festgelegt. Somit muss der Massnahmenkatalog nur für die festgelegten Bereiche erstellt werden.



- (2) Die Massnahmen aus ISO 27002 decken die notwendigen Anforderungen nur global und nicht vollumfänglich ab. Aus diesem Grund wird die Anwendung der Massnahmen aus ISO 27002 nur als Ergänzung empfohlen.
- (3) Ein weiterer Ansatz verfolgt das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem Grundsatz Kompendium. Dabei werden Prozess- und auch System-Bausteine für die notwendigen Massnahmen-Bereiche abgebildet. Diese können anschliessend für die Festlegung des Massnahmenkataloges verwendet werden. Somit hat das BSI einen vollumfänglichen und ganzheitlichen Ansatz für die Erstellung des Massnahmenkatalogs geschaffen. Die Massnahmen korrespondieren jedoch auch mit den oben genannten Quellen.
- (4) Für spezifische Bereiche sollen und müssen auch Standards beigezogen werden, welche bei Bedarf den Massnahmenkatalog erweitern. Diese Standards sind z.B. IEC/EN 62443, IEC/EN 62351, IEC/EN 60850, IEC/EN 61850, IEEE usw.
- (5) Die Erstellung des Massnahmenkatalogs stellt das Unternehmen und die Organisationseinheiten vor grosse Herausforderungen. Es muss dabei entschieden werden, welche Kontrollen bzw. Massnahmen von welchem Standard angewendet werden sollen.



**Empfehlung der VSE Cyber Security Task Force Experten:**

Es wird empfohlen die Massnahmen nach NIST Publication 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix anzuwenden. Der Massnahmenkatalog soll aus diesen drei Quellen erfolgen. Es soll dabei das vom VSE zur Verfügung gestellte Tool als Basis zur Anwendung gebracht werden. Die Massnahmen können mit den Punkten von ISO 27002 ergänzt werden. Zur Unterstützung können die CSF-Tools unter <https://csf.tools/> verwendet werden.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



Die Erstellung des Massnahmenplanes mit den Kontrollen aus NIST Publication 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix bilden nur die Grundlage. Für spezifische Bereiche muss der Massnahmenkatalog mit Kontrollen aus den Standards wie z.B. IEC/EN 62443, IEC/EN 62351, IEC/EN 60850, IEC/EN 61850, IEEE usw. erweitert werden.



Die Erstellung des Massnahmenkataloges ist ein umfangreicher Prozess, welcher Ressourcen intensiv ist. Dieser Prozess muss aber durch die Unternehmen und Organisationseinheiten zwingend umgesetzt werden, da dieser entscheidend für die Ganzheitlichkeit und Effektivität ist.



Mit dem "VSE&BFE-Tool\_for\_NIST-CSF-1.1\_Checkpoints\_acc.to\_NIST-SP800-53\_CCM\_CIS" kann der Massnahmenplan erstellt werden.



Die NIST CSF-Tools unter <https://csf.tools/> unterstützen die Unternehmen und Organisationseinheiten bei der Suche und Festlegung der notwendigen Massnahmen. In den Tools wird das gesamte NIST Cyber Security Framework mit den Massnahmen aus NIST Publication 800-53, CIS Critical Security Controls, CSA Cloud Controls Matrix vernetzt.



**In den folgenden Dokumenten sind Orientierungshilfen und Anleitungen:**

- BSI IT-Grundsatz Kompendium

### 6.3.9 Audits planen

- (1) Die Planung von Audits im Rahmen eines Information Security Management Systems (ISMS) ist ein entscheidender Schritt, um sicherzustellen, dass die Sicherheitsprozesse und -kontrollen effektiv sind. Die Planung ist darauf ausgerichtet, systematisch die Konformität mit den festgelegten Sicherheitsstandards zu prüfen und potentielle Verbesserungsbereiche zu identifizieren.
- (2) Zunächst erfolgt die Festlegung des Auditumfangs, der die Bereiche und Prozesse definiert, die während des Audits überprüft werden sollen. Dies beinhaltet oft eine Analyse der kritischen Geschäftsprozesse und der damit verbundenen Informationen. Parallel dazu werden die Ziele des Audits festgelegt, die in der Regel darauf abzielen, die Einhaltung von Sicherheitsrichtlinien und -verfahren zu überprüfen, Schwachstellen aufzudecken und sicherzustellen, dass die Sicherheitsziele erreicht werden.





- (3) Die Auswahl der Auditoren ist ein weiterer wesentlicher Aspekt der Planung. Die Auditoren sollten über die erforderlichen Fachkenntnisse im Bereich Informationssicherheit verfügen und gleichzeitig unabhängig und objektiv sein.
- (4) Die Planung berücksichtigt auch den Zeitrahmen für das Audit und stellt sicher, dass ausreichend Zeit für eine gründliche Überprüfung aller relevanten Aspekte vorhanden ist. Ein Auditplan wird erstellt, der den detaillierten Ablauf des Audits skizziert. Dies umfasst den Zeitplan, die zu überprüfende Bereiche, die beteiligten Personen und die zu verwendenden Ressourcen.
- (5) Die Kommunikation mit den betroffenen Parteien, einschliesslich derjenigen, die auditiert werden, ist entscheidend, um Transparenz und Kooperation zu fördern. Während des Audits werden verschiedene Methoden zur Datenerhebung und -prüfung angewendet, darunter Interviews, Dokumentenüberprüfungen und möglicherweise technische Tests.
- (6) Die Ergebnisse werden dokumentiert, um einen klaren Überblick über die Einhaltung der Sicherheitsstandards und identifizierten Verbesserungsmöglichkeiten zu geben. Nach Abschluss des Audits erfolgt die Berichterstattung, in der die Ergebnisse, Feststellungen und Empfehlungen festgehalten werden. Diese Berichte sind grundlegend für die kontinuierliche Verbesserung des ISMS. Die Organisation leitet dann Massnahmen ab, um eventuelle Mängel zu beheben und den Sicherheitsstatus weiter zu optimieren.
- (7) Insgesamt ist die Planung von Audits im Rahmen eines ISMS ein strategischer Prozess, der sicherstellt, dass die Überprüfung der Informationssicherheit systematisch, objektiv und wirksam durchgeführt wird.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

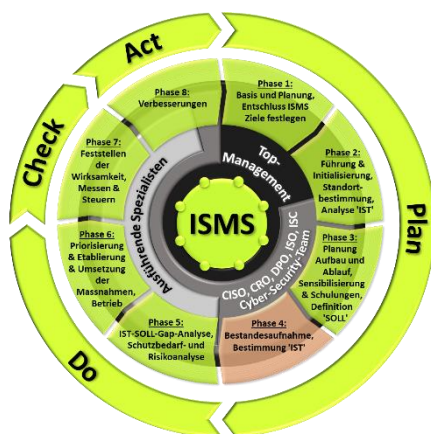
- HoP-01-00-01-04 Arbeitsanleitung Bereich IMS: Audits



**Empfehlung der VSE Cyber Security Task Force Experten: Die Planung der Audits wird im Bereich Integrierte Management Systeme (IMS) erstellt und verwaltet. Somit ist eine Absprache mit den anderen Bereichen im Unternehmen und in den Organisationseinheiten zwingend erforderlich.**

## 6.4 Phase 4: Bestandesaufnahme; Bestimmung 'IST'

- (1) In vierte Phase steht ganz im Zeichen der Bestandesaufnahme und die Bestimmung des 'IST'-Zustandes:



<b>Verantwortlich:</b>	Top-Management, C-Level
<b>Zuständig:</b>	CISO, CRO, DPO, ISO, ISC, Cyber Security Team
<b>Involvierte Stellen:</b>	Spezifische Mitarbeiter der Informationssicherheit, (Externe Experten und Berater)
<b>Zu behandelnde Punkte</b>	<ul style="list-style-type: none"> <li>■ Detailliertes Inventar durchführen</li> <li>■ Identifizierung der Wirkungskette</li> <li>■ Umgesetzte Massnahmen ermitteln zur Informationssicherheit ermitteln</li> <li>■ «IST-Audits» durchführen</li> <li>■ IST-Assessment durchführen</li> <li>■ Risikoregister erstellen</li> <li>■ Baseline für KPI ermitteln</li> </ul>

**Tabelle 10:** ISMS Phase 4: Bestandesaufnahme; Bestimmung 'IST'

### 6.4.1 Detailliertes Inventar erheben

- (1) Die Erhebung eines detaillierten Asset-Inventars im Rahmen der Informationssicherheit und des Information Security Management Systems (ISMS) ist ein essenzieller Schritt, um einen umfassenden Überblick über die genutzten Informationsressourcen einer Organisation zu erhalten. Dieser Prozess zielt darauf ab, sämtliche Assets zu identifizieren, zu klassifizieren und zu dokumentieren, um ihre Sicherheit effektiv zu gewährleisten.
- (2) Die Durchführung beginnt mit der Identifikation aller Informationswerte und -ressourcen innerhalb der Organisation. Dazu gehören nicht nur physische Geräte wie Server und Computer, sondern auch Datenbanken, Software, Netzwerkgeräte, Informationsflüsse und andere relevante Elemente. Eine sorgfältige Analyse ist entscheidend, um sicherzustellen, dass keine wichtigen Assets übersehen werden.



- (3) Im nächsten Schritt erfolgt die Klassifizierung der identifizierten Assets. Dies beinhaltet die Bewertung ihrer Sensibilität, Bedeutung und ihre Auswirkung auf die Geschäftsprozesse. Die Klassifizierung hilft dabei, Prioritäten zu setzen und Ressourcen entsprechend der Wichtigkeit der Assets zuzuweisen.
- (4) Die Dokumentation der Assets ist ein wesentlicher Bestandteil dieses Prozesses. Hierbei werden detaillierte Informationen zu jedem Asset erfasst, einschliesslich Standort, Eigentümer, Nutzungsberechtigungen, technische Spezifikationen und Abhängigkeiten von anderen Assets. Eine sorgfältige Dokumentation erleichtert die spätere Verwaltung und den Schutz der Assets.
- (5) Parallel dazu erfolgt die Bewertung der Risiken im Zusammenhang mit jedem Asset. Dies umfasst die Identifikation potenzieller Bedrohungen, Schwachstellen und mögliche Auswirkungen auf die Sicherheit des Assets. Die Risikobewertung ist entscheidend, um gezielte Sicherheitsmassnahmen zu entwickeln und sicherzustellen, dass die vorhandenen Ressourcen effizient eingesetzt werden.
- (6) Die Durchführung des detaillierten Asset-Inventars erfordert oft die Zusammenarbeit verschiedener Organisationseinheiten und Stakeholder innerhalb des Unternehmens und der Organisationseinheiten. IT/OT-Abteilungen, Datenschutzbeauftragte und Geschäftseinheiten müssen ihre jeweiligen Perspektiven einbringen, um sicherzustellen, dass alle relevanten Assets erfasst werden.
- (7) Der gesamte Prozess ist nicht einmalig, sondern muss regelmässig wiederholt werden. Neue Assets, Veränderungen in der IKT-Infrastruktur oder der Geschäftsprozessen erfordern eine kontinuierliche Aktualisierung des Inventars, um sicherzustellen, dass die Informationssicherheit auf dem neuesten Stand ist.
- (8) Insgesamt ermöglicht die Durchführung eines detaillierten Asset-Inventars eine fundierte Grundlage für die Entwicklung und Umsetzung einer effektiven Informationssicherheitsstrategie. Durch die genaue Kenntnis aller genutzten Ressourcen kann die Organisation sicherstellen, dass ihre Informationswerte angemessen geschützt werden.
- (9) Folgende Elemente umfasst ein detailliertes Inventar zur Informationssicherheit:
  - Geschäftsfelder und deren Geschäftsprozesse
  - Informationen und Daten (alle relevanten Daten zur Behandlung der Geschäftsprozesse)
  - Hardware-Ressourcen wie Server, Computer, Netzwerkkomponenten usw.
  - Betriebssysteme, Datenbanken, Firmware, Treibersoftware, Anwendungsprogramme, Softwaretools usw.
  - MAC- und IP-Adressen
  - Dienste, Protokolle und Ports
  - Zertifikate
  - Datenflüsse und Wirkungskette
  - Anwender (User)



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung



**Der Aufwand zur Erstellung des vollumfänglichen Inventars ist nicht zu unterschätzen. Das ganzheitliche und aktuelle Inventar ist aber von elementarer Bedeutung für die gesamte Informationssicherheit im. Nur auf Basis eines aktuellen und vollumfänglichen Inventars können Verwundbarkeiten identifiziert werden.**



**Empfehlung der VSE Cyber Security Task Force Experten: Zur Erstellung des vollumfänglichen Inventars ist ein systematischer Ansatz zu wählen. Softwaretools und Applikationen helfen den Unternehmen und Organisationseinheiten die Inventarisierung zu automatisieren. Wichtig ist, dass das Inventar jederzeit aktuell ist.**

#### 6.4.2 Identifizierung der Wirkungskette

- (1) Die Identifizierung der Wirkungskette im ISMS ist ein proaktiver Ansatz, um Zusammenhänge zwischen Ereignissen, Schwachstellen und potenziellen Auswirkungen auf die Informationssicherheit zu verstehen. Beginnend mit der Erfassung verschiedener Ereignisse analysiert sie systematisch deren Verbindung und Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie auf die Reputation der Organisation. Die resultierende Wirkungskette zeigt kaskadierende Auswirkungen und ermöglicht die Identifikation von Schwachstellen und kritischen Pfaden.



- (2) Die Einbeziehung verschiedener Stakeholder und regelmässige Aktualisierungen gewährleisten eine ganzheitliche Sicht. Dieser proaktive Ansatz bildet eine fundierte Grundlage für die Entwicklung von Risikominderungsstrategien im ISMS.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung



**Empfehlung der VSE Cyber Security Task Force Experten: Die Identifizierung der Wirkungskette ist wichtig, dass die Zusammenhänge zwischen den einzelnen Elementen aufgezeigt werden können. Somit können mögliche Angriffsvektoren besser erkannt und verstanden werden. Dies untermauert die Tatsache, dass Angriffe oft nicht direkt auf Systeme oder Elemente ausgeführt werden, sondern über die Lieferketten oder vernetzte Elemente erfolgen.**

#### 6.4.3 Umgesetzte Massnahmen zur Informationssicherheit ermitteln

- (1) Die Ermittlung der umgesetzten Massnahmen im ISMS ist entscheidend, um die Wirksamkeit der Sicherheitsvorkehrungen zu gewährleisten. Der Prozess beginnt mit der Überprüfung der Sicherheitsrichtlinien und -pläne, einschliesslich technischer, organisatorischer und personeller Massnahmen.
- (2) Technische Aspekte werden anhand von Software, Netzwerkkonfigurationen und physischen Sicherheitsmassnahmen bewertet. Organisatorische Massnahmen, wie Schulungen und Sensibilisierung, werden auf ihre Umsetzung in den betrieblichen Abläufen überprüft. Die Zuweisung von Verantwortlichkeiten und die Überwachung von Sicherheitsvorfällen sind ebenfalls zentrale Aspekte.
- (3) Die Zusammenarbeit zwischen verschiedenen Organisationseinheiten und regelmässige Überprüfungen sind entscheidend, um die Informationssicherheit auf einem angemessenen Niveau zu halten und auf aktuelle Bedrohungen angemessen zu reagieren.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung



**Mit dem "VSE&BFE-Tool\_for\_NIST-CSF-1.1\_Checkpoints\_acc.to\_NIST-SP800-53\_CCM\_CIS" können die umgesetzten Massnahmen mit ihrer Maturität erfasst werden.**



**Der Aufwand zur Ermittlung der umgesetzten Massnahmen ist nicht zu unterschätzen. Die Ermittlung muss vollumfänglich und ganzheitlich über den gesamten Bereich der Informationssicherheit gemacht werden.**



**Empfehlung der VSE Cyber Security Task Force Experten: Ein strukturierter Ansatz hilft bei der Ermittlung der umgesetzten Massnahmen. Die Verwendungen von geeigneten Tools ist zwingend notwendig.**

#### 6.4.4 «IST-Audits» Ist-Zustand der Informationssicherheit ermitteln

- (1) Die Durchführung von «IST-Audits» im Rahmen der Informationssicherheit und des Information Security Management Systems (ISMS) ist ein proaktiver Ansatz, um die tatsächliche Umsetzung von Sicherheitsmassnahmen zu überprüfen und sicherzustellen, dass diese den festgelegten Standards und Richtlinien entsprechen. Diese Audits sind entscheidend, um Schwachstellen zu identifizieren, Verbesserungsmöglichkeiten aufzudecken und sicherzustellen, dass die Informationssicherheit auf einem angemessenen Niveau ist.
- (2) Der Prozess beginnt oft mit der Festlegung der Prüfungsbereiche und -ziele. Dies beinhaltet die Definition der zu überprüfenden Systeme, Prozesse und Kontrollmechanismen sowie die klare Festlegung der Ziele des Audits. Es ist wichtig, dass diese Ziele mit den Sicherheitsrichtlinien und -zielen der Organisation in Einklang stehen.
- (3) Die eigentliche Durchführung des «IST-Audits» umfasst die Überprüfung von Dokumentationen, Prozessen und technischen Implementierungen. Dies kann die Analyse von Sicherheitsrichtlinien, Schulungsunterlagen, Zugriffsberechtigungen, Systemkonfigurationen und anderen relevanten Unterlagen



einschliessen. Gleichzeitig erfolgt eine Überprüfung vor Ort, um sicherzustellen, dass die dokumentierten Prozesse in der Praxis effektiv umgesetzt und durch die Organisationseinheiten gelebt werden.

- (4) Ein wesentlicher Bestandteil des «IST-Audits» ist die Kommunikation und Zusammenarbeit mit den Verantwortlichen und Mitarbeitern. Die Auditoren interagieren mit den relevanten Stakeholdern, um Informationen zu sammeln, Verständnis für die Abläufe zu erhalten und sicherzustellen, dass die Sicherheitsmassnahmen in der täglichen Praxis effektiv funktionieren.
- (5) Die Analyse der Ergebnisse erfolgt in enger Abstimmung mit den Zielen des Audits. Es werden mögliche Abweichungen von den festgelegten Standards identifiziert und bewertet. Diese können technischer, organisatorischer oder prozessualer Natur sein. Gleichzeitig werden positive Aspekte und erfolgreiche Umsetzungen hervorgehoben.
- (6) Nach der Analyse erfolgt die Erstellung eines Berichts mit den Audit-Ergebnissen. Dieser Bericht enthält Empfehlungen für Verbesserungen, identifizierte Schwachstellen und positive Aspekte. Er wird an die relevanten Stakeholder und die Führungsebene der Organisation weitergeleitet.
- (7) Die Umsetzung von Korrekturmassnahmen ist ein entscheidender Schritt nach einem IST-Audit. Hierbei werden die identifizierten Schwachstellen behoben, und es werden Massnahmen ergriffen, um die Informationssicherheit weiter zu stärken. Dieser Prozess sollte transparent sein und die Rückmeldung der Auditergebnisse an die betroffenen Bereiche beinhalten.
- (8) Insgesamt bietet die Durchführung von «IST-Audits» eine wertvolle Gelegenheit zur kontinuierlichen Verbesserung der Informationssicherheit. Die Ergebnisse dieser Audits dienen nicht nur dazu, bestehende Schwächen zu beheben, sondern auch dazu, die Sicherheitsstrategie der Organisation weiter zu verfeinern und auf aktuelle Bedrohungen einzustellen.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-00-01-04 Arbeitsanleitung Bereich IMS: Audits
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung



**Der Aufwand zur Ermittlung für die Durchführung von Audits ist nicht zu unterschätzen. Ein Audit braucht eine akribische Vorbereitung und eine detaillierte Überprüfung. Die anschliessende Auswertung legt den aktuellen Stand fest und gilt als Grundlage für Korrekturmassnahmen.**



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Durchführung von Audits ist zwingend notwendig. Nur so kann der aktuelle Stand ermittelt und nötige Korrekturmassnahmen eingeleitet werden.**

#### 6.4.5 IST-Assessment durchführen

- (1) Das IST-Assessment im ISMS bewertet den aktuellen Status der Informationssicherheit in einer Organisation. Zunächst werden Prüfungsbereiche und -ziele definiert, die mit den Sicherheitsrichtlinien und -zielen in Einklang stehen.
- (2) Das Assessment analysiert Dokumentationen, Prozesse und technische Implementierungen, sowohl durch Dokumentenprüfung als auch vor Ort. Die Kommunikation mit Verantwortlichen und Mitarbeitern ist dabei entscheidend. Die Analyse der Ergebnisse identifiziert Abweichungen von Standards und hebt positive Aspekte hervor.
- (3) Ein abschliessender Bericht mit Empfehlungen für Verbesserungen wird an Stakeholder und die Führungsebene weitergeleitet. Die Umsetzung von Korrekturmassnahmen schliesst den Prozess ab, wodurch das IST-Assessment eine Chance zur kontinuierlichen Verbesserung der Informationssicherheit bietet.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS



**Für das IST-Assessment im Bereich Informationssicherheit der Kontrollen im Rahmen des NIST Cybersecurity Frameworks (CSF) 1.1 soll das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" verwendet werden. Die Vorgaben des BFE im Strom VV sind im Tool schon ersichtlich.**







Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.



Für das IST-Assessment im Informationssicherheit der Kontrollen im Rahmen der ISO 27001 Annex A soll das "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002" verwendet werden.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.



Im Anhang befindet sich eine ausführliche Beschreibung für das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002".



**Empfehlung der VSE Cyber Security Task Force Experten:**  
Für die Durchführung des IST-Assessment sollen die Tools angewendet werden, welche vom VSE zur Verfügung gestellt sind.

#### 6.4.6 Risikoregister erstellen

- (1) Die Erstellung eines Risikoregisters im ISMS ist entscheidend, um Risiken systematisch zu erfassen und zu überwachen. Der Prozess beginnt mit der Identifikation aller potenziellen Gefahren für die Informationssicherheit, sowohl intern als auch extern.
- (2) Die Bewertung der Risiken analysiert ihre Auswirkungen und die Wahrscheinlichkeit ihres Eintretens. Priorisierte Risiken werden ins Risikoregister aufgenommen, welches detaillierte Informationen, Verantwortlichkeiten und den Status der Risikobehandlung enthält.
- (3) Regelmässige Aktualisierungen und transparente Kommunikation mit Stakeholdern gewährleisten die Effektivität des Registers und ermöglichen eine proaktive Reaktion auf Gefahren.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01-03-02 Arbeitsanleitung Bereich ISMS: IT-OT-Risiko-Management



**Empfehlung der VSE Cyber Security Task Force Experten:**  
Zur Identifizierung möglicher Risiken kann auf die Risikofunktionen im Unternehmen und in den Organisationseinheiten zurückgegriffen werden. Ebenfalls eignen sich BIA's hervorragend, um die effektiven Risiken zu identifizieren.

#### 6.4.7 Baseline für KPI ermitteln

- (1) Die Ermittlung der Baseline für KPIs im ISMS ist ein strategischer Prozess zur Festlegung von Ausgangspunkten für die Leistungsmessung der Informationssicherheit. Dies beginnt mit der Analyse der ISMS-Ziele, die als Grundlage für die Auswahl relevanter KPIs dienen. Die identifizierten KPIs sollten direkt mit den Sicherheitszielen verknüpft sein und kritische Bereiche abdecken.
- (2) Die Baseline wird durch die Erfassung von Ausgangsdaten gebildet, die aktuelle Leistungsniveaus für die ausgewählten KPIs repräsentieren. Während der Ermittlung ist es wichtig, Schwankungen und saisonale Einflüsse zu berücksichtigen. Die Baseline sollte regelmässig überprüft und aktualisiert werden, um den Fortschritt im Kontext sich ändernder Geschäftsanforderungen genau zu bewerten.
- (3) Eine aussagekräftige Baseline ist entscheidend, um Fortschritte zu überwachen und gezielt auf Schwachstellen oder Verbesserungsmöglichkeiten im Bereich Informationssicherheit zu reagieren.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting



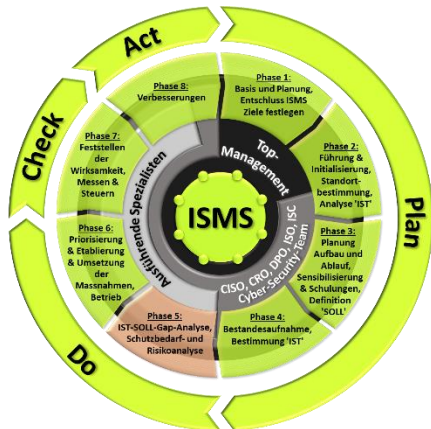
**Empfehlung der VSE Cyber Security Task Force Experten:**  
Die Festlegung der Baseline für Key Performance Indicators (KPIs) ist wichtig, weil sie als Referenzpunkt dient, um den Fortschritt und die Leistung zu messen. Ohne eine klare Baseline ist es schwierig, den Erfolg oder Misserfolg von Initiativen oder Massnahmen zu bewerten. Die Baseline



ermöglicht es, Veränderungen im Laufe der Zeit zu verfolgen und zu verstehen, ob Ziele erreicht werden. Sie bildet auch die Grundlage für die Festlegung realistischer Ziele und die Entwicklung von Strategien zur Leistungsverbesserung.

## 6.5 Phase 5: IST-SOLL-Gap-Analyse; Schutzbedarf- und Risikoanalyse

(1) In fünfte Phase steht ganz im Zeichen der IST-SOLL-Gap-Analyse, der Schutzbedarf- und Risikoanalyse:



<b>Verantwortlich:</b>	Top-Management, C-Level, CISO, CRO, DPO, ISO
<b>Zuständig:</b>	ISC, Cyber Security Team, Ausführende Spezialisten
<b>Involvierte Stellen:</b>	Spezifische Mitarbeiter der Informationssicherheit (Externe Experten und Berater)
<b>Zu behandelnde Punkte</b>	<ul style="list-style-type: none"> <li>■ IST-SOLL-Gap-Analyse</li> <li>■ Schutzbedarf für zusätzlichen Geltungsbereich im ISMS definieren</li> <li>■ Risikomanagement-Methodik festlegen</li> <li>■ Risikokategorien und -kriterien festlegen</li> <li>■ Bestimmung der Risikoeigentümer(Risk-Owner)</li> <li>■ Risikomanagement durchführen</li> <li>■ Risikoanalyse auf Bedrohungen</li> </ul>

Tabelle 11: ISMS Phase 5: IST-SOLL-Gap-Analyse; Schutzbedarf- und Risikoanalyse

### 6.5.1 IST-SOLL-Gap-Analyse

- (1) Die IST-SOLL-Gap-Analyse im Information Security Management System (ISMS) ist entscheidend, um bestehende Sicherheitspraktiken mit den angestrebten Zielen zu vergleichen. Die Analyse identifiziert Lücken zwischen dem aktuellen (IST) und gewünschten Zustand (SOLL).
- (2) Zu Beginn werden aktuelle Sicherheitspraktiken umfassend bewertet, einschliesslich Richtlinien, Prozesse und Technologien. Dabei sind technische, organisatorische und prozessuale Aspekte zu berücksichtigen.
- (3) Anschliessend definiert die Organisation angestrebte Ziele basierend auf Sicherheitsstandards, gesetzlichen Anforderungen oder branchenspezifischen Richtlinien. Der SOLL-Zustand repräsentiert ideale Sicherheitspraktiken.
- (4) Die eigentliche Gap-Analyse vergleicht IST und SOLL durch Identifizierung von Abweichungen. Dies umfasst quantitative und qualitative Aspekte, inklusive Risikobewertung. Identifizierte Lücken werden dokumentiert und priorisiert.
- (5) Die Ergebnisse bilden die Grundlage für einen Massnahmenplan zur Lückenschliessung. Dieser definiert klare Ziele, Verantwortlichkeiten, Zeitrahmen und Ressourcenanforderungen.
- (6) Die IST-SOLL-Gap-Analyse ist kein einmaliger Prozess, sondern sollte regelmässig wiederholt werden, besonders bei sich ändernden Anforderungen, Bedrohungslandschaften oder Sicherheitsstandards. So ermöglicht sie kontinuierliche Anpassung und Verbesserung im ISMS.



In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS



Für die GAP-Analyse im Bereich Informationssicherheit der Kontrollen im Rahmen des NIST Cybersecurity Frameworks (CSF) 1.1 soll das "VSE&BFE-Assement-Tool\_NIST-CSF-1.1\_++" verwendet werden.



Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.





Für die GAP-Analyse im Informationssicherheit der Kontrollen im Rahmen der ISO 27001 Annex A soll das "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002" verwendet werden.



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Für die Durchführung der IST-SOLL-Gab-Analyse sollen die Tools angewendet werden, welche vom VSE zu Verfügung gestellt werden.**

### 6.5.2 Schutzbedarf für zusätzlichen Geltungsbereich im ISMS definieren

- (1) Durch die Vorgaben im Strom VV ist der Schutzbedarf gemäss Schutzniveau definiert. Dennoch wird empfohlen, im übrigen Bereich der Informationssicherheit eine Schutzbedarfsanalyse durchzuführen.
- (2) Die Definition des Schutzbedarfs im Rahmen des ISMS zielt darauf ab, spezifische Anforderungen und Risiken für bestimmte Informationswerte oder Systeme zu bestimmen. Dies erfolgt durch eine detaillierte Inventarisierung und Kategorisierung der Werte oder Systeme im zusätzlichen Geltungsbereich, basierend auf ihrer Bedeutung und potenziellen Schadenswirkung.
- (3) Eine Risikobewertung analysiert Bedrohungen, Schwachstellen und potenzielle Auswirkungen unter Berücksichtigung externer und interner Faktoren. Basierend darauf wird der Schutzbedarf definiert, inklusive erforderlichem Schutzniveau und geeigneten Sicherheitsmassnahmen.
- (4) Die Schutzbedarfsdefinition erfolgt in Abstimmung mit den strategischen Zielen und dem Gesamt-ISMS. Sie orientiert sich an Risikomanagementgrundsätzen, um Sicherheitsentscheidungen an den Geschäftszielen auszurichten.
- (5) Die Dokumentation des Schutzbedarfs ist wesentlich und bildet die Grundlage für konkrete Sicherheitsmassnahmen im zusätzlichen Geltungsbereich. Der iterative Prozess sollte regelmässig überprüft und aktualisiert werden, insbesondere bei sich ändernden organisatorischen Anforderungen, Bedrohungslandschaften oder Sicherheitsstandards. Dies ermöglicht eine dynamische Anpassung der Schutzmassnahmen für angemessene Informationssicherheit.



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Durch die Vorgaben im Strom VV ist der minimale Schutzbedarf für die Bereiche gemäss Schutzniveau definiert. Es wird aber empfohlen, dass in den restlichen Bereichen der Informationssicherheit im Unternehmen und in den Organisationseinheiten dennoch eine Schutzbedarfsanalyse durchgeführt wird.**

### 6.5.3 Risikomanagement-Methodik festlegen

- (1) Die Methodik zum Risikomanagement im ISMS ist entscheidend, um Risiken proaktiv zu identifizieren und angemessene Sicherheitsmassnahmen zu implementieren. Der Prozess beginnt mit der Definition des Anwendungsbereichs, um den Fokus zu bewahren. Die Identifikation von Risiken beinhaltet die Analyse von Bedrohungen, Schwachstellen und potenziellen Auswirkungen unter Einbeziehung relevanter Stakeholder.
- (2) Nach der Identifikation erfolgt die Bewertung der Risiken hinsichtlich Eintrittswahrscheinlichkeit und potenzieller Auswirkungen. Die Festlegung von Risikobehandlungsstrategien basiert auf den Ergebnissen, unter Berücksichtigung von Unternehmens- und den Organisationseinheitenzielen, Ressourcen und Risikotoleranzen.
- (3) Die Implementierung von Sicherheitsmassnahmen ist integraler Bestandteil der Risikobehandlung und erfolgt gemäss der Methodik. Die kontinuierliche Überwachung und Überprüfung der Risiken beinhaltet die regelmässige Evaluierung der implementierten Massnahmen und Anpassung bei Änderungen.
- (4) Die flexible Anpassung der Methodik an veränderte Bedingungen und Anforderungen sowie die kontinuierliche Verbesserung des Risikomanagementprozesses sind entscheidend. Eine durchdachte Methodik trägt insgesamt dazu bei, die Informationssicherheit auf angemessenem Niveau zu halten, indem sie einen systematischen Ansatz für Identifikation, Bewertung und Behandlung von Risiken bietet.





**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-03-02 Arbeitsanleitung Bereich ISMS: IT-OT-Risiko-Management



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Das Risikomanagement ist wichtig, weil es Unternehmen dabei hilft, potenzielle Gefahren zu identifizieren, zu bewerten und zu bewältigen, bevor sie zu ernsthaften Problemen werden. Durch die Anwendung einer strukturierten Methodik können Organisationen Risiken proaktiv angehen, um Verluste zu minimieren, Chancen zu nutzen und langfristige Stabilität zu gewährleisten. Eine effektive Risikomanagement-Methodik bietet auch Transparenz und Vertrauen für Investoren, Kunden und andere Stakeholder, was letztendlich das Unternehmenswachstum und die Nachhaltigkeit fördert.**

#### 6.5.4 Risikokategorien und -kriterien festlegen

- (1) Die Festlegung von Risikokategorien und -kriterien im Rahmen des ISMS ist ein strategischer Prozess zur Identifikation, Klassifizierung und Bewertung von Risiken. Diese bilden die Grundlage für die spätere Risikoanalyse.
- (2) Zu Beginn werden Risikokategorien identifiziert, indem potenzielle Risiken aufgrund gemeinsamer Merkmale in Gruppen eingeteilt werden, wie technische, organisatorische, personelle oder externe Risiken. Anschliessend werden Kriterien für die Risikobewertung festgelegt, um eine einheitliche und vergleichbare Bewertung zu ermöglichen, sei es quantitativ oder qualitativ.
- (3) Die enge Verknüpfung von Risikokategorien und -kriterien mit den Geschäftszielen und -prozessen der Organisation ist entscheidend. Dies gewährleistet, dass die Identifikation und Bewertung auf die spezifischen Anforderungen abgestimmt sind, unter Einbeziehung relevanter Stakeholder.
- (4) Die Festlegungen sind nicht statisch, sondern sollten regelmässig überprüft und angepasst werden, um sich an veränderte Anforderungen, Bedrohungslandschaften und Geschäftsstrategien anzupassen. Die Flexibilität ermöglicht eine stets aktuelle und relevante Risikobewertung.
- (5) Die Ergebnisse dienen als Grundlage für die Risikoanalyse im ISMS, erleichtern die systematische Identifikation und Bewertung von Risiken und ermöglichen so die Entwicklung effektiver Sicherheitsmassnahmen. Insgesamt etabliert die Festlegung von Risikokategorien und -kriterien einen konsistenten und organisationsweit akzeptierten Ansatz für das Risikomanagement.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-03-02 Arbeitsanleitung Bereich ISMS: IT-OT-Risiko-Management



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Risikokategorien helfen, verschiedene Arten von Risiken zu identifizieren (z.B. finanziell, operationell). Kriterien bewerten Risiken basierend auf Auswirkungen und Eintrittswahrscheinlichkeiten, um Prioritäten festzulegen und Ressourcen effektiv zu nutzen.**

#### 6.5.5 Bestimmung der Risikoeigentümer (Risk-Owner)

- (1) Die Bestimmung der Risikoeigentümer (Risk-Owner) im ISMS ist entscheidend, um klare Verantwortlichkeiten für die Identifikation, Bewertung und Behandlung von Risiken sicherzustellen. Der Risikoeigentümer ist die Person oder Organisationseinheit, die letztendlich für ein spezifisches Risiko verantwortlich ist und Entscheidungen dazu trifft.
- (2) Die Bestimmung der Risikoeigentümer beginnt mit der Identifikation und Bewertung von Risiken, bei der jedes identifizierte Risiko einem Risikoeigentümer zugeordnet wird. Dieser sollte die erforderliche Expertise und Autorität haben, um Entscheidungen im Zusammenhang mit dem Risiko zu treffen.
- (3) Die Verantwortlichkeiten des Risikoeigentümers umfassen die kontinuierliche Überwachung, die Aktualisierung der Risikobewertung, die Festlegung von Massnahmen zur Risikominderung und die Kommunikation von Risikoinformationen an relevante Stakeholder. Die Bestimmung der Risikoeigentümer erfolgt in enger Abstimmung mit den Stakeholdern, um klare Verantwortlichkeiten sicherzustellen.
- (4) Dieser Prozess ist dynamisch und sollte regelmässig überprüft und angepasst werden, insbesondere bei organisatorischen Veränderungen, neuen Geschäftsprozessen oder sich ändernden Risikoprofilen. Die klare Definition der Risikoeigentümer trägt insgesamt dazu bei, Risiken effizient und effektiv zu managen, indem klare Verantwortlichkeiten und Entscheidungsprozesse etabliert werden.







**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung
- HoP-01-01-03-02 Arbeitsanleitung Bereich ISMS: IT-OT-Risiko-Management



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Bestimmung der Risikoeigentümer ist wichtig, um klare Verantwortlichkeiten für die Risikobewältigung innerhalb des Unternehmens festzulegen und sicherzustellen, dass Risiken aktiv gemanagt werden.**

### 6.5.6 Risikomanagement durchführen

- (1) Das Risikomanagement im ISMS ist ein kontinuierlicher, mehrstufiger Prozess. Es beginnt mit der Identifikation von potenziellen Bedrohungen und Schwachstellen in Zusammenarbeit mit Stakeholdern. Die Risiken werden dann anhand vordefinierter Kriterien bewertet und priorisiert, um sich auf wesentliche Herausforderungen zu konzentrieren.
- (2) Die Risikobehandlung folgt, bei der Strategien festgelegt werden, wie z.B. die Implementierung von Sicherheitsmassnahmen oder die Akzeptanz bestimmter Risiken. Die Überwachung der implementierten Massnahmen gewährleistet, dass der gewünschte Schutz aufrechterhalten wird, wobei Anpassungen bei Veränderungen in der Organisation oder der Bedrohungslandschaft vorgenommen werden.
- (3) Der gesamte Prozess wird regelmässig wiederholt, wobei neue Informationen und Erfahrungen in Sicherheitsvorfällen zu Aktualisierungen der Risikobewertung und Anpassungen der Risikobehandlungsstrategien führen können. Das Ziel ist eine proaktive Sicherheitsstrategie, die durch kontinuierliche Verbesserungen eine flexible Reaktion auf sich ändernde Bedingungen ermöglicht und die Informationssicherheit auf optimalem Niveau hält.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung
- HoP-01-01-03-02 Arbeitsanleitung Bereich ISMS: IT-OT-Risiko-Management



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Anwendung des Risikomanagements im ISMS ist wichtig, um potenzielle Gefahren zu identifizieren, zu bewerten und angemessen darauf zu reagieren, um die Informationssicherheit zu gewährleisten und Risiken zu minimieren.**

### 6.5.7 Risikoanalyse auf TOP-Bedrohungen

- (1) Die Risikoanalyse auf TOP-Bedrohungen im ISMS konzentriert sich auf die gravierendsten Gefahren für die Informationssicherheit. Die Identifikation erfolgt durch eine umfassende Analyse der Bedrohungslandschaft, unter Berücksichtigung interner und externer Risiken.
- (2) Die Bewertung der TOP-Bedrohungen erfolgt anhand vorher definierter Kriterien, die sowohl technische Aspekte als auch geschäftliche, regulatorische und strategische Bedeutungen berücksichtigen. Es folgt die Entwicklung von gezielten Risikominderungsmassnahmen, die darauf abzielen, die grössten Risiken effektiv zu adressieren und die Informationssicherheit zu stärken.
- (3) Die Umsetzung der Massnahmen erfolgt in enger Abstimmung mit relevanten Stakeholdern und Risikoeigentümern. Der dynamische Prozess erfordert regelmässige Wiederholungen, um auf Veränderungen in der Bedrohungslandschaft, neuen Technologien oder geschäftlichen Anpassungen flexibel reagieren zu können.
- (4) Insgesamt ermöglicht die Risikoanalyse auf TOP-Bedrohungen der Organisation, begrenzte Ressourcen auf die kritischsten Herausforderungen zu fokussieren. Dies trägt zur Entwicklung einer effektiven und effizienten Informationssicherheitsstrategie bei, um sicherzustellen, dass die wichtigsten Risiken angemessen adressiert werden.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03-03 Arbeitsanleitung Bereich ISMS: Asset Management und Informationsklassifizierung



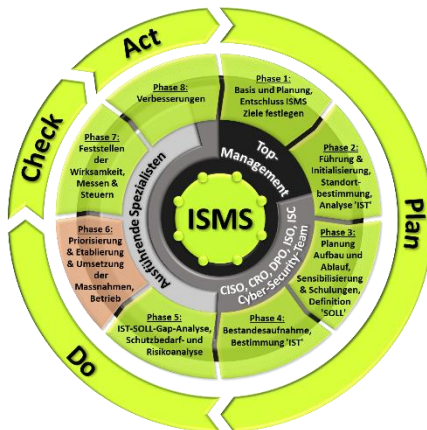


**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Risikoanalyse auf Top-Bedrohungen im ISMS ist wichtig, um sich auf die gravierendsten Risiken zu konzentrieren, Ressourcen effektiv zu nutzen und gezielte Sicherheitsmassnahmen zur Minimierung dieser Risiken zu entwickeln. Die Risikoanalyse soll somit im ersten Schritt auf die aktuellen TOP-Bedrohungen durchgeführt werden. Folgend kann eine Priorisierung der Massnahmen vereinfacht werden und der Schutz auf aktuellen Umständen fokussiert werden.

## 6.6 Phase 6: Priorisierung, Etablierung und Umsetzung der Massnahmen; Betrieb

- (1) Die sechste Phase steht ganz im Zeichen der Priorisierung, Etablierung und Umsetzung der Massnahmen. Weiter wird der Betrieb zur kontinuierlichen Umsetzung der Massnahmen behandelt:



Verantwortlich:	Top-Management, C-Level, CISO, CRO, DPO, ISO
Zuständig:	ISC, Cyber Security Team, Ausführende Spezialisten
Involvierte Stellen:	Spezifische Mitarbeiter der Informationssicherheit (Externe Experten und Berater)
Zu behandelnde Punkte	<ul style="list-style-type: none"> <li>Massnahmenplan aus GAP- oder Risikoanalyse erarbeiten</li> <li>Massnahmen priorisieren</li> <li>Personelle Anforderungen und Kompetenzen festlegen</li> <li>Massnahmenumsetzung gemäss Priorisierung durchführen</li> <li>Kommunikations-, Trainings- und Awareness Massnahmen umsetzen</li> <li>Betrieb zur kontinuierlichen Umsetzung der Massnahmen</li> </ul>

**Tabelle 12:** ISMS Phase 6: Priorisierung, Etablierung und Umsetzung der Massnahmen; Betrieb

### 6.6.1 Massnahmenplan aus GAP- oder Risikoanalyse erarbeiten

- (1) Die Erarbeitung eines Massnahmenplans aus der GAP-Analyse und Risikoanalyse im ISMS ist entscheidend, um Defizite und Risiken zu identifizieren und entsprechende Schutzmassnahmen zu entwickeln. Die GAP-Analyse vergleicht bestehende Sicherheitsmassnahmen mit Sicherheitszielen, identifiziert Lücken und bildet die Grundlage für den Massnahmenplan. Die Risikoanalyse konzentriert sich auf die Bewertung von Bedrohungen und Schwachstellen, um Prioritäten für Schutzmassnahmen festzulegen.
- (2) Der Massnahmenplan, in Zusammenarbeit mit relevanten Stakeholdern entwickelt, beinhaltet klare Ziele, Verantwortlichkeiten, Zeitpläne und Ressourcen für jede Massnahme. Die Priorisierung erfolgt basierend auf der Risikobewertung und Dringlichkeit. Mitarbeiterkommunikation und Schulungen sind integraler Bestandteil, ebenso wie die schrittweise Umsetzung und kontinuierliche Überwachung.
- (3) Die Evaluierung der Massnahmen erfolgt durch regelmässige Überprüfungen, Audits und Sicherheitsmetriken. Dies fliesst in den kontinuierlichen Verbesserungszyklus des ISMS ein. Insgesamt stärkt die Entwicklung des Massnahmenplans die Informationssicherheit, passt das ISMS an aktuelle Anforderungen an und fördert eine kontinuierliche Verbesserung des Sicherheitsniveaus.

**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**



- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



Für den Massnahmenplan soll das "VSE&BFE-Tool\_for\_NIST-CSF-1.1\_Checkpoints\_acc.to\_NIST-SP800-53\_CCM\_CIS" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002" verwendet werden.





Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.



Die einzelnen Punkte aus dem Massnahmenplan sind bei den entsprechenden House of Policy Dokumenten (Richtlinien und Arbeitsanleitungen) einzupflegen und entsprechend zu behandeln.



**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Erarbeitung eines Massnahmenplans aus GAP- oder Risikoanalyse ist wichtig, um identifizierte Lücken zu schliessen und Risiken zu mindern, damit das Unternehmen besser auf potenzielle Herausforderungen vorbereitet ist.

## 6.6.2 Massnahmen priorisieren

- (1) Die Priorisierung der Massnahmen aus der GAP-Analyse und Risikoanalyse im ISMS ist ein strategischer Prozess, der Schutzmassnahmen gezielt auf die wichtigsten Herausforderungen ausrichtet. Die GAP-Analyse identifiziert Unterschiede zwischen aktuellen Massnahmen und Standards. Die Risikoanalyse bewertet potenzielle Bedrohungen. Die Priorisierung basiert auf ganzheitlicher Betrachtung, berücksichtigt Schwere, Auswirkungen, Wahrscheinlichkeit und externe Faktoren wie gesetzliche Anforderungen. Ressourcenaspekte und Umsetzbarkeit spielen eine Rolle.
- (2) Ein iterativer Dialog mit Stakeholdern, darunter Sicherheitsverantwortliche und Führungskräfte, ist entscheidend. Der resultierende Priorisierungsplan gibt klare Anweisungen für die Umsetzung, berücksichtigt verschiedene Arten von Massnahmen und orientiert sich am Zeitrahmen. Regelmässige Überprüfung und Anpassung sind unerlässlich, um Schutzmassnahmen kontinuierlich an sich ändernde Bedingungen anzupassen und effiziente Ressourcennutzung sicherzustellen.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



Für den Massnahmenplan und die Priorisierung soll das "VSE&BFE-Tool\_for\_NIST-CSF-1.1\_Checkpoints\_acc.to\_NIST-SP800-53\_CCM\_CIS" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.Controls\_acc.to\_ISO27002" verwendet werden.



Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.



Die Priorisierung der Massnahmen ist, wenn nötig, in entsprechenden House of Policy Dokumenten (Richtlinien und Arbeitsanleitungen) einzupflegen und entsprechend zu behandeln.



**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Priorisierung von Massnahmen aus der GAP-Analyse und Risikoanalyse ist wichtig, um Ressourcen effektiv zu nutzen und sich auf die kritischsten Bereiche zu konzentrieren, um die grössten Verbesserungen zu erzielen und Risiken zu minimieren.



### 6.6.3 Personelle Anforderungen und Kompetenzen festlegen

- (1) Die Festlegung der personellen Anforderungen und Kompetenzen im ISMS ist entscheidend für die effektive Implementierung der priorisierten Massnahmen. Dies erfordert eine gründliche Bewertung der erforderlichen Fähigkeiten, einschliesslich technischem Fachwissen in Bereichen wie Netzwerksicherheit oder Compliance. Die Auswahl von Teammitgliedern sollte ein ausgewogenes Team mit vielfältigen Fähigkeiten und Erfahrungen schaffen, angepasst an die Art der Massnahmen. Sensibilisierung für aktuelle Entwicklungen, Anpassungsfähigkeit und proaktive Denkweise sind wesentliche Kompetenzen.
- (2) Die Einbindung relevanter Stakeholder und regelmässige Schulungen sind entscheidend, um sicherzustellen, dass die Teams den strategischen Zielen entsprechen und auf dem neuesten Stand bleiben. Kommunikations- und Teamfähigkeiten sind ebenso wichtig wie technischen Fachkenntnisse, um sicherzustellen, dass Massnahmen nicht nur technisch effektiv, sondern auch organisatorisch umsetzbar sind. Insgesamt ist die Festlegung der personellen Anforderungen und Kompetenzen ein dynamischer Prozess, der sich an ändernden Anforderungen und Bedrohungen anpasst. Ein gut zusammengestelltes Team mit den richtigen Fähigkeiten ist entscheidend, um Sicherheitsmassnahmen effektiv umzusetzen und die Informationssicherheit zu stärken.

#### In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:



- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-01-01 Arbeitsanleitung Bereich ISM: Informationssicherheit Organisation
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



**Die personellen Anforderungen und Kompetenzen sind in den betroffenen House of Policy Dokumenten (Richtlinien und Arbeitsanleitungen) einzupflegen und entsprechend zu behandeln.**



#### Empfehlung der VSE Cyber Security Task Force Experten:

**Die Festlegung der personellen Anforderungen und Kompetenzen im ISMS ist entscheidend, um sicherzustellen, dass das Team über die erforderlichen Fähigkeiten verfügt, um die priorisierten Massnahmen effektiv umzusetzen und das Informationssicherheitsmanagementsystem erfolgreich zu betreiben. Oft ist es nötig, dass externe Ressourcen beigezogen werden müssen.**

### 6.6.4 Massnahmenumsetzung gemäss Priorisierung durchführen

- (1) Die Umsetzung priorisierter Massnahmen im ISMS ist entscheidend, um Sicherheitslücken zu schliessen und Risiken angemessen zu minimieren. Teams erhalten klare Verantwortlichkeiten und arbeiten eng mit Stakeholdern zusammen. Technische, organisatorische und prozessuale Massnahmen werden implementiert, darunter neue Technologien, Schulungen und notwendige Prozesse.
- (2) Kontinuierliche Kommunikation und Überwachung sind Schlüsselfaktoren, um Hindernisse zu identifizieren und den Fortschritt zu bewerten. Eine flexible Anpassung an Änderungen und eine enge Zusammenarbeit zwischen Teams und Stakeholdern sind unerlässlich.
- (3) Der iterative Prozess erfordert klare Planung, transparente Kommunikation und kontinuierliche Überwachung, um die Sicherheit der Organisation zu stärken und die gesteckten ISMS-Ziele zu erreichen.

#### In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:



- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-01-01 Arbeitsanleitung Bereich ISM: Informationssicherheit Organisation
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



**Als Hilfe für die Umsetzung der Massnahmen soll das "VSE&BFE-Tool\_for\_NIST-CSF-1.1\_Checkpoints\_acc.to\_NIST-SP800-53\_CCM\_CIS" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.Controls\_acc.to\_ISO27002" verwendet werden.**







Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.



Die Priorisierung der Massnahmen ist, wenn nötig, in entsprechenden House of Policy Dokumenten (Richtlinien und Arbeitsanleitungen) einzupflegen und entsprechend zu behandeln.



**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Massnahmenumsetzung gemäss Priorisierung im ISMS ist wichtig, muss zeitnah und kontinuierlich umgesetzt werden, um Ressourcen effektiv zu nutzen und sich auf die kritischsten Bereiche zu konzentrieren, um die Informationssicherheit wirksam zu verbessern und Risiken zu minimieren.

### 6.6.5 Kommunikations-, Trainings- und Awareness Massnahmen umsetzen

- (1) Die Umsetzung von Kommunikations-, Trainings- und Awareness-Massnahmen im ISMS ist entscheidend, um das Sicherheitsbewusstsein der Mitarbeiter zu stärken. Kommunikationsmassnahmen vermitteln die Bedeutung der Informationssicherheit durch interne Kanäle aber auch an externen Stakeholdern wie Dienstleister/Hersteller, Partner und Kunden durch eine zielgerichtete externe Kommunikation.
- (2) Schulungsmassnahmen bieten spezifisches Wissen, inklusive technischer und organisatorischer Aspekte. Awareness-Massnahmen sensibilisieren für sicherheitsrelevante Themen durch Informationsmaterial und Simulationen.
- (3) Eine klare Kommunikation, Ressourcen für Schulungen und ein positives Sicherheitsklima sind entscheidend. Die Evaluation der Massnahmen gewährleistet Anpassungen an sich ändernde Bedrohungen und Anforderungen. Dieser ganzheitliche Ansatz schafft ein kulturelles Bewusstsein für Informationssicherheit durch kontinuierliche Anstrengungen.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-03-04 Arbeitsanleitung Bereich ISMS: Schulung und Sensibilisierung
- HoP-01-01-03-21 Arbeitsanleitung Bereich ISMS: Sicherheitsmassnahmen für Dienstleister
- HoP-01-01-03-22 Arbeitsanleitung Bereich ISMS: Lieferanten Management
- HoP-01-01-03-23 Arbeitsanleitung Bereich ISMS: Informationssicherheit im Personalbereich
- HoP-01-01-03-24 Arbeitsanleitung Bereich ISMS: Informationssicherheit in Projekten



**In den folgenden Dokumenten sind Orientierungshilfen und Anleitungen:**

- Schulungsprogramm nach NIST Special Publication 800-50



**Es muss sichergestellt sein, dass die erforderlichen Kommunikations-, Trainings- und Awareness Massnahmen auch bei Dienstleistern, Lieferanten und in Projekten zur Anwendung kommen.**



**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Umsetzung von Kommunikations-, Trainings- und Awareness-Massnahmen im ISMS ist wichtig und müssen kontinuierlich umgesetzt werden, um das Verständnis für Informationssicherheit zu fördern, Mitarbeiter zu sensibilisieren und ihre Fähigkeiten zur Risikominimierung zu verbessern, was letztendlich die Sicherheit des Unternehmens und der Organisationseinheiten erhöht. Es wird empfohlen ein Schulungsprogramm nach NIST Special Publication 800-50 aufzubauen und umzusetzen.

### 6.6.6 Kontinuierlichen Umsetzung der Massnahmen

- (1) Die kontinuierliche Umsetzung der Informationssicherheitsmassnahmen im ISMS ist ein fortlaufender Prozess, der Monitoring, Audits und regelmässige Aktualisierungen umfasst. Durch Sicherheitsinformationen und -ereignisse werden potenzielle Vorfälle frühzeitig erkannt. Audits sichern die Wirksamkeit, identifizieren Schwachstellen und gewonnene Erkenntnisse fliessen in den Verbesserungsprozess ein.



- (2) Die regelmässige Anpassung von Sicherheitsrichtlinien erfolgt in Zusammenarbeit mit Stakeholdern. Kontinuierliche Schulungen und Sensibilisierung sind essenziell, ebenso wie die fortwährende Überprüfung und Anpassung der Risikobewertung. Die Integration von Incident-Response-Plänen mit klaren Verfahren im Falle eines Vorfalls ist entscheidend, und regelmässige Übungen testen deren Effektivität. Die enge Zusammenarbeit zwischen den Organisationseinheiten im ISMS fördert die Anpassung an veränderte Bedingungen.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-01-01 Arbeitsanleitung Bereich ISM: Informationssicherheit Organisation
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



Als Hilfe für die kontinuierliche Umsetzung der Massnahmen soll das "VSE&BFE-Tool\_for\_NIST-CSF-1.1\_Checkpoints\_acc.to\_NIST-SP800-53\_CCM\_CIS" und "VSE-Assessment-Tool\_ISO27001-Annex-A\_incl.\_Controls\_acc.to\_ISO27002" verwendet werden.



Die Verwendung aller NIST-Dokumente und -Standards sind kostenlos und können somit uneingeschränkt verwendet werden.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.



Die Priorisierung der Massnahmen ist, wenn nötig, in entsprechenden House of Policy Dokumenten (Richtlinien und Arbeitsanleitungen) einzupflegen und entsprechend zu behandeln.



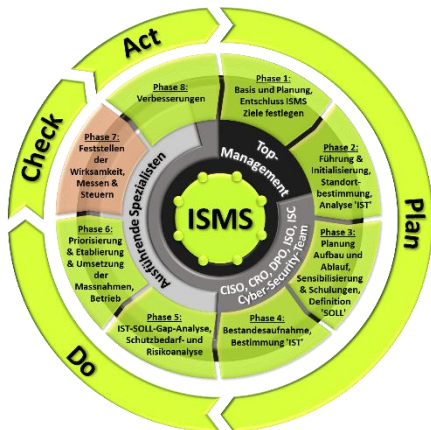
**Empfehlung der VSE Cyber Security Task Force Experten:**

Die kontinuierliche Umsetzung der Massnahmen im ISMS ist wichtig und muss aktiv gefördert werden, um die Informationssicherheit fortlaufend zu gewährleisten, sich an sich ändernde Bedrohungen anzupassen und die Effektivität des Systems aufrechtzuerhalten.



## 6.7 Phase 7: Feststellen der Wirksamkeit; Messen und Steuern

- (1) Die siebte Phase steht ganz im Zeichen der Überprüfung der Wirksamkeit des ISMS. Weiter wird das Messen und Steuern des ISMS behandelt.



Verantwortlich:	Top-Management, C-Level
Zuständig:	CISO, CRO, DPO, ISO, ISC, Cyber Security Team
Involvierte Stellen:	Spezifische Mitarbeiter der Informationssicherheit, (Externe Experten und Berater)
Zu behandelnde Punkte	<ul style="list-style-type: none"> <li>■ Umgesetzte Massnahmen auf ihre Wirksamkeit überprüfen</li> <li>■ Interne- sowie Lieferanten-Audits durchführen</li> <li>■ Überwachung des ISMS</li> <li>■ Leistungsindikatoren (KPI) behandeln</li> <li>■ Regelbetrieb mit Monitoring und Reporting etablieren</li> <li>■ Dokumentationsprozesse sicherstellen</li> </ul>

Tabelle 13: ISMS Phase 7: Feststellen der Wirksamkeit; Messen und Steuern

### 6.7.1 Umgesetzte Massnahmen auf ihre Wirksamkeit überprüfen

- (1) Die Überprüfung der ISMS-Massnahmen ist entscheidend, um den gewünschten Schutz und die Sicherheitsziele sicherzustellen. Dieser Prozess erfordert klare Kriterien, die mit den ISMS-Zielen verknüpft sind. Systematische Audits und Überwachungen evaluieren technische, organisatorische und prozessuale Aspekte.
- (2) Die Ergebnisse identifizieren Schwachstellen, die in den kontinuierlichen Verbesserungsprozess einfließen. Die Kommunikation erfolgt auf verschiedenen Ebenen, einschliesslich auf Stufe Management. Die Überprüfung ist ein fortlaufender Zyklus, der das ISMS agil gegenüber neuen Bedrohungen und Technologien macht und langfristige Anpassungen ermöglicht.
- (3) Insgesamt ist die Überprüfung ein essenzieller Bestandteil des ISMS-Lebenszyklus, der die Informationssicherheit als dynamischen Prozess betrachtet.



#### Empfehlung der VSE Cyber Security Task Force Experten:

Die Überprüfung der umgesetzten Massnahmen auf ihre Wirksamkeit im ISMS ist wichtig, um sicherzustellen, dass sie tatsächlich die beabsichtigten Ergebnisse liefern und die Informationssicherheit verbessern, sowie um Anpassungen vorzunehmen, falls erforderlich. Die Überprüfung der umgesetzten Massnahmen kann auf verschiedene Weise erfolgen:

- Penetrationstests
- Überprüfung des Know-how
- Interne und externe Audits
- usw.

### 6.7.2 Interne sowie Lieferanten-Audits durchführen

- (1) Die Durchführung von internen und Lieferanten-Audits im Rahmen des ISMS gewährleistet die effektive Umsetzung der Sicherheitsrichtlinien und -prozesse in der gesamten Lieferkette. Interne Audits prüfen die Einhaltung von Sicherheitsrichtlinien und die Effektivität des ISMS. Lieferanten-Audits konzentrieren sich auf das Sicherheitsniveau externer Partner und Lieferanten.
- (2) Die klare Planung, Auswahl objektiver Auditoren und systematische Überprüfungen sind entscheidend. Die Ergebnisse führen zu Empfehlungen für Verbesserungen, die mit den beteiligten Parteien geteilt werden.
- (3) Die Umsetzung von Schulungen, Anpassungen von Sicherheitsrichtlinien und technischen Verbesserungen erfolgt als Reaktion auf die Audit-Ergebnisse. Insgesamt sind diese Audits integral für das ISMS, um effektive Sicherheitsmassnahmen sicherzustellen und die Einhaltung von Standards zu gewährleisten.



#### In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:

- HoP-01-00-01-04 Arbeitsanleitung Bereich IMS: Audits
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen



- HoP-01-01-01 Arbeitsanleitung Bereich ISM: Informationssicherheit Organisation
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



**Empfehlung der VSE Cyber Security Task Force Experten:**

Interne und Lieferanten-Audits im ISMS sind wichtig und müssen aktiv gefördert werden, um die Einhaltung von Sicherheitsstandards zu überprüfen, potenzielle Schwachstellen aufzudecken und sicherzustellen, dass alle beteiligten Parteien die erforderlichen Sicherheitsmassnahmen implementieren und aufrechterhalten. Das Recht auf Lieferanten-Audits muss in Verträgen mit Lieferanten enthalten sein. Definieren Sie die Kontroll-Punkte, die Sie überprüfen wollen, sowie die Risikoüberprüfung von Sub-Lieferanten.

### 6.7.3 Überwachung des ISMS

- (1) Die Überwachung des ISMS in der Informationssicherheit ist entscheidend, um die Wirksamkeit der Sicherheitsmassnahmen sicherzustellen, Anpassungen an Bedrohungen vorzunehmen und Sicherheitsstandards einzuhalten. Dies beinhaltet die kontinuierliche Prüfung von Sicherheitskontrollen, technischen Massnahmen wie Protokollanalysen und Penetrationstests. Organisatorische Aspekte wie Schulungen und Mitarbeiter-Compliance werden ebenfalls überwacht. Die Einhaltung von gesetzlichen Anforderungen wird dokumentiert und regelmässig aktualisiert.
- (2) Die Überwachung umfasst auch die Bewertung von Sicherheitsvorfällen, um Ursachen zu identifizieren und präventive Massnahmen zu implementieren. Die regelmässige Berichterstattung informiert die Stakeholder über die Effektivität des ISMS und dient als Grundlage für strategische Entscheidungen. Die Identifizierung von Verbesserungsmöglichkeiten basiert auf der Analyse von Überwachungsergebnissen und dem erhaltenen Feedback.
- (3) Zusammenfassend gewährleistet die Überwachung, dass Informationssicherheitsmassnahmen agil sind und sich kontinuierlich verbessern, um sich ändernden Bedrohungen und Geschäftsanforderungen gerecht zu werden.



**Hinweise auf weiterführende und ergänzende Dokumente:**

- BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)
- ISO/IEC 27004 ISMS Monitoring, measurement, analysis and evaluation



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-00-01-04 Arbeitsanleitung Bereich ISM: Audits
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-01-01 Arbeitsanleitung Bereich ISM: Informationssicherheit Organisation
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



**Empfehlung der VSE Cyber Security Task Force Experten:**

Die Überwachung des ISMS ist entscheidend, um sicherzustellen, dass Sicherheitsrichtlinien und -verfahren wirksam sind, potenzielle Bedrohungen frühzeitig erkannt werden und die Integrität der Informationssicherheit gewährleistet ist. Zur Überwachung des ISMS soll das vom VSE zur Verfügung gestellt Tool verwendet werden.



Zur Überwachung des ISMS kann das Tool "VSE-Tool\_ISO27001-ISMS\_Assessment-Goals" verwendet werden.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.





#### 6.7.4 Leistungsindikatoren (KPI) behandeln

- (1) Die Behandlung von KPI's im ISMS ist zentral, um die Wirksamkeit von Sicherheitsmassnahmen zu messen, Sicherheitsziele zu überwachen und kontinuierliche Verbesserungen zu fördern. Geeignete KPI's werden durch klare Zieldefinitionen im ISMS festgelegt, die sich an den strategischen Zielen der Organisation orientieren. Die Umsetzung beinhaltet die Festlegung quantifizierbarer Messgrössen, die regelmässig überwacht werden.
- (2) Das Monitoring erfolgt kontinuierlich, wobei automatisierte Tools Echtzeitinformationen bereitstellen. Die Interpretation der KPI's erfordert eine umfassende Analyse, um Trends oder Abweichungen zu identifizieren und proaktiv auf Risiken zu reagieren. Die Kommunikation der Ergebnisse an das Management und andere Stakeholder fördert das Verständnis für die Sicherheitssituation.
- (3) Die Nutzung der KPI's als Grundlage für kontinuierliche Verbesserungen schliesst den Prozess ab, indem die Ergebnisse in den Regelbetrieb integriert werden. Insgesamt ist die KPI-Behandlung ein iterativer Prozess, der durch klare Zieldefinitionen, systematische Umsetzung, kontinuierliches Monitoring, umfassende Analyse und Integration von Erkenntnissen in den Regelbetrieb eine gezielte Verbesserung des ISMS ermöglicht.



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Behandlung der Leistungsindikatoren (KPIs) im ISMS ist wichtig und muss aktiv gefördert werden, um die Effektivität des Informationssicherheitsmanagementsystems zu messen, Schwachstellen zu identifizieren und Verbesserungen zu ermöglichen.**

#### 6.7.5 Regelbetrieb mit Monitoring und Reporting etablieren

- (1) Die Etablierung des Regelbetriebs mit Monitoring und Reporting im ISMS gewährleistet die Effektivität der implementierten Sicherheitsmassnahmen. Klare Rollen und Verantwortlichkeiten werden systematisch umgesetzt, während das Monitoring Netzwerkaktivitäten und andere sicherheitsrelevante Ereignisse überwacht.
- (2) Das Reporting wandelt Monitoring-Ergebnisse in regelmässige Berichte um, die Sicherheitsvorfälle, Compliance-Status und Effektivität der Kontrollen enthalten. Automatisierte Reporting-Mechanismen erleichtern diesen Prozess und ermöglichen zeitnahe Berichterstattung.
- (3) Das Management spielt eine zentrale Rolle bei der Bewertung der Berichte, der Festlegung von Prioritäten und der Initiierung von Anpassungen im ISMS. Insgesamt ist die Etablierung des Regelbetriebs ein fortlaufender Prozess, der sicherstellt, dass die Informationssicherheitsmassnahmen aktuell, effektiv und anpassungsfähig bleiben.



**In den folgenden Dokumenten sind Orientierungshilfen und Anleitungen:**

- BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)



**In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**

- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-02-01 Arbeitsanleitung Bereich ISMS: Key Performance Indicators (KPI) und Reporting
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Der Regelbetrieb mit Monitoring und Reporting im ISMS muss etabliert werden und aktiv gefördert werden, um kontinuierlich die Informationssicherheit zu überwachen, potenzielle Bedrohungen frühzeitig zu erkennen und angemessen darauf zu reagieren, um die Integrität, Vertraulichkeit und**



### 6.7.6 Dokumentationsprozesse sicherstellen

- (1) Die Sicherstellung der Dokumentationsprozesse im ISMS ist zentral, um klare, präzise und aktuelle Informationen sicherzustellen. Der Prozess beginnt mit der Identifikation erforderlicher Dokumentation, darunter Sicherheitsrichtlinien, Verfahrensanweisungen und Protokolle. In enger Zusammenarbeit mit Sicherheitsexperten und Verantwortlichen entstehen die notwendigen Dokumente, welche Branchenstandards und gesetzliche Anforderungen berücksichtigen.
- (2) Die Aktualität wird durch regelmässige Überprüfungen und Updates gewährleistet, insbesondere bei Veränderungen in der Unternehmens- und Organisationseinheitenstruktur. Ein Dokumentenmanagement-Team oder Sicherheitsbeauftragte sind für die Pflege verantwortlich, während Schulungen sicherstellen, dass Mitarbeiter die Dokumente verstehen und befolgen. Regelmässige Audits sichern die Einhaltung von Standards und identifizieren Verbesserungsmöglichkeiten.
- (3) Das Vorgehen ist ein kontinuierlicher und iterativer Prozess, der durch klare Identifikation, präzise Erstellung, regelmässige Aktualisierung, angemessene Zugänglichkeit und Schulungen die Effektivität und Anpassungsfähigkeit der Informationssicherheitsdokumentation sicherstellt.

#### **In folgenden Musterdokumenten in den Beilagen sind die Punkte abgebildet:**



- HoP-01-00-00-02 Arbeitsanleitung Bereich IMS: House of Policy
- HoP-01-00-00-03 Arbeitsanleitung Bereich IMS: Dokumentenlenkung
- HoP-01-00-01-04 Arbeitsanleitung Bereich IMS: Audits
- HoP-01-01-01 Richtlinie Bereich ISM: Informationssicherheit Rahmen
- HoP-01-01-01-01 Arbeitsanleitung Bereich ISM: Informationssicherheit Organisation
- HoP-01-01-02 Richtlinie Bereich ISM: Geltungsbereich, Aufbau und Betrieb des ISMS
- HoP-01-01-03 Richtlinie Bereich ISM: Baseline im ISMS und dazugehörige Arbeitsanleitungen
- HoP-01-01-04 Richtlinie Informationssicherheit Benutzer von Informationswerten und dazugehörigen Arbeitsanleitungen



#### **Empfehlung der VSE Cyber Security Task Force Experten:**

**Die Sicherstellung des Dokumentationsprozesses im ISMS ist wichtig, muss gelebt und muss aktiv gefördert werden, um Richtlinien, Verfahren und Entscheidungen festzuhalten, was die Nachverfolgung, Einhaltung und kontinuierliche Verbesserung der Informationssicherheit ermöglicht. Zur Sicherstellung des Dokumentationsprozesses im ISMS soll das vom VSE zur Verfügung gestellte Tool verwendet werden.**



**Zur Sicherstellung des Dokumentationsprozesses des ISMS kann das Tool "VSE-Tool\_ISO27001-ISMS\_Assessment-Goals" verwendet werden.**

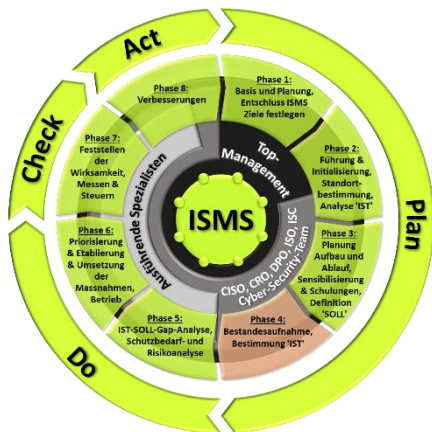


**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**



6.8 Phase 8: Verbesserungen

(1) Die achte Phase steht ganz im Zeichen der Verbesserungen:



Verantwortlich:	Top-Management, C-Level
Zuständig:	CISO, CRO, DPO, ISO, ISC, Cyber Security Team
Involvierte Stellen:	Spezifische Mitarbeiter der Informationssicherheit, Ausführende Spezialisten (Externe Experten und Berater)
Zu behandelnde Punkte	<ul style="list-style-type: none"><li>■ Korrektur und Vorbeugungsmassnahmen</li><li>■ Prüfung von Verbesserungsmöglichkeiten</li><li>■ Kontinuierlicher Verbesserungsprozess leben</li></ul>

Tabelle 14: ISMS Phase 8: Verbesserungen

6.8.1 Korrektur und Vorbeugungsmassnahmen

- (1) Das Vorgehen für Korrektur- und Vorbeugungsmassnahmen im ISMS ist ein systematischer Prozess zur Behebung von Sicherheitsvorfällen und zur Verhinderung zukünftiger Ereignisse. Bei einem Vorfall sind Sofortmassnahmen entscheidend, um den Schaden zu begrenzen und die Systemintegrität wiederherzustellen.
- (2) Nach der Korrekturphase erfolgt eine eingehende Untersuchung, um die Ursachen zu identifizieren und präventive Massnahmen zu entwickeln. Diese können Sicherheitsrichtlinien, neue Kontrollen, Schulungen oder technologische Verbesserungen umfassen. Die Wirksamkeit wird durch regelmässige Überprüfungen und Audits bewertet. Die Integration in das ISMS dokumentiert erfolgreiche Massnahmen und sichert nachhaltige Veränderungen in der Sicherheitskultur der Organisation.
- (3) Das wiederholende Vorgehen ermöglicht eine stetige Verbesserung der Informationssicherheit und eine effektive Reaktion auf sich ändernde Bedrohungen.



**Empfehlung der VSE Cyber Security Task Force Experten:**  
Die Korrekturen und Vorbeugungsmassnahmen im ISMS sind wichtig und müssen aktiv gefördert werden, um aufgetretene Probleme zu beheben und zukünftige Sicherheitsvorfälle zu verhindern, wodurch die Informationssicherheit verbessert und Risiken minimiert werden. Zur Verbesserung des ISMS soll das vom VSE zur Verfügung gestellt Tool verwendet werden.



Zur Verbesserung des ISMS kann das Tool "VSE-Tool\_ISO27001-ISMS\_Assessment-Goals" verwendet werden.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.

6.8.2 Prüfung von Verbesserungsmöglichkeiten

- (1) Die Prüfung von Verbesserungsmöglichkeiten im ISMS ist ein essenzieller Prozess zur Identifikation von Schwachstellen, ineffektiven Sicherheitsmassnahmen und zur Steigerung der Gesamteffizienz. Der Prozess beginnt mit einer gründlichen Analyse bestehender Sicherheitsmassnahmen durch interne Audits und Sicherheitsüberprüfungen.
- (2) Schwachstellen und Risiken, sowohl technischer als auch organisatorischer Natur, werden ermittelt. Die gesammelten Daten dienen als Grundlage zur Identifikation von Verbesserungsbereichen, in denen das ISMS nicht den Standards entspricht oder Effizienzsteigerungen möglich sind. Es folgt die Entwicklung korrigierender Massnahmen, die während der Implementierung kontinuierlich überwacht werden.
- (3) Eine umfassende Bewertung der Ergebnisse erfolgt nach der Implementierung, unter Einbeziehung von Feedback aus verschiedenen Organisationseinheiten. Erfolgreiche Massnahmen werden als bewährte Verfahren dokumentiert und in die Sicherheitsrichtlinien integriert. Insgesamt ist die Prüfung von



Verbesserungsmöglichkeiten ein iterativer Prozess, der es der Organisation ermöglicht, sich effektiv an sich ändernde Bedrohungen und Anforderungen anzupassen.



Hinweise auf weiterführende und ergänzende Dokumente:

- BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)
- ISO/IEC 27004 ISMS Monitoring, measurement, analysis and evaluation



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Zur Prüfung von Verbesserung im ISMS soll das vom VSE zur Verfügung gestellt Tool verwendet werden.**



**Zur Prüfung der Verbesserungsmöglichkeiten für des ISMS kann das Tool "VSE-Tool\_ISO27001-ISMS\_Assessment-Goals" verwendet werden.**



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**

### 6.8.3 Kontinuierlicher Verbesserungsprozess leben

- (1) Der kontinuierliche Verbesserungsprozess im ISMS gewährleistet die fortlaufende Optimierung der Sicherheitspraktiken und -prozesse einer Organisation. Dieser Prozess durchläuft wiederkehrend Zyklen, die auf die Identifikation von Schwachstellen, die Etablierung bewährter Verfahren und die Förderung einer robusten Sicherheitskultur abzielen. Der kontinuierliche Verbesserungsprozess beginnt mit der Datensammlung über bestehende Sicherheitsmassnahmen durch interne Audits, Überwachungen, Sicherheitsvorfälle und Mitarbeiterfeedback.
- (2) Die gesammelten Informationen bilden die Grundlage zur Identifikation von Verbesserungsbereichen. Klar definierte Ziele und Massnahmen, wie die Aktualisierung von Sicherheitsrichtlinien oder Schulungen für Mitarbeiter, werden festgelegt. Die Ziele sind messbar, um den Fortschritt zu überwachen. Während der Implementierungsphase werden die Massnahmen umgesetzt, begleitet von einer Überwachung, die technische Überprüfungen und Simulationen von Sicherheitsvorfällen einschliessen kann.
- (3) Die Ergebnisse werden analysiert, um sicherzustellen, dass die implementierten Massnahmen die beabsichtigten Verbesserungen bringen. Die Überprüfung und Bewertung sind entscheidend, wobei Feedback von Mitarbeitenden und Führungskräften berücksichtigt wird. Der kontinuierliche Verbesserungsprozess-Zyklus schliesst mit der Standardisierung ab. Erfolgreiche Massnahmen werden als bewährte Verfahren dokumentiert und in die Sicherheitsrichtlinien integriert. Dies gewährleistet, dass positive Veränderungen nachhaltig in die Unternehmenskultur eingebettet werden. Der iterative Lebenszyklus des kontinuierliche Verbesserungsprozess stellt sicher, dass die Informationssicherheit kontinuierlich optimiert und an sich wandelnde Bedrohungen angepasst wird.



**Empfehlung der VSE Cyber Security Task Force Experten:**

**Der kontinuierliche Verbesserungsprozess im ISMS muss gelebt werden und gefördert werden, um durch regelmässiges Feedback und Anpassungen die Effektivität des Informationssicherheitsmanagementsystems zu steigern und mit sich verändernden Bedrohungen Schritt zu halten.**





## 7. Zusammenspiel der VSE Dokumente und der VSE-Tools

Die folgende Grafik zeigt auf, wie die VSE-Dokumente und die VSE-Tools zur Steigerung der IKT-Resilienz in Zusammenhang stehen. Es wird dargestellt, wo welche Inputs der Unternehmen und Organisationseinheiten erforderlich sind.

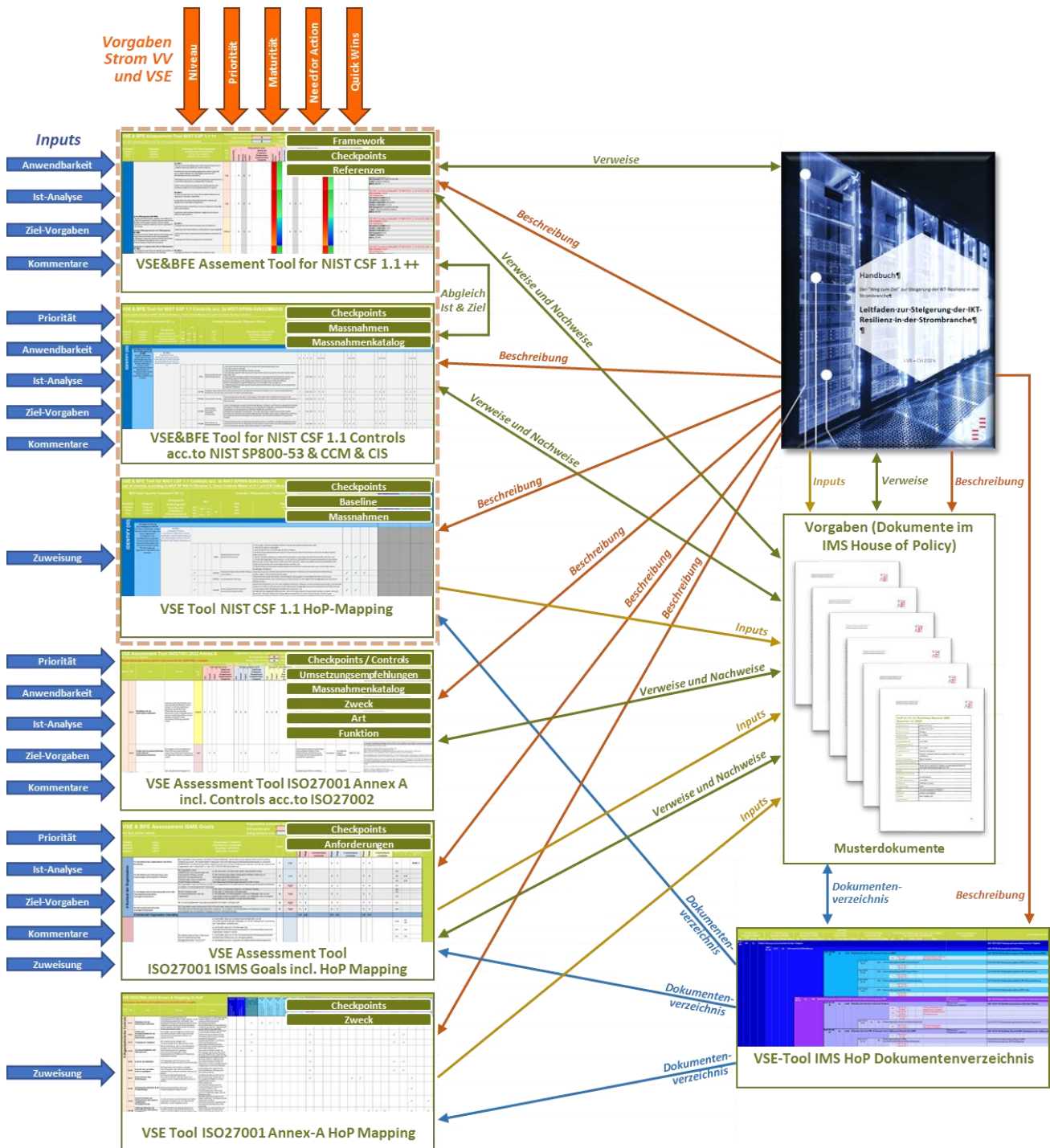


Abbildung 28: Zusammenspiel der VSE-Dokumente mit den VSE-Tools zur Steigerung der IKT-Resilienz (Quelle VSE)



## 8. Schlussfolgerung und Zusammenfassung

- (1) Die Schlussfolgerungen des Leitfadens zur Steigerung der IKT-Resilienz im Bereich der Informationssicherheit unterstreichen die Bedeutung eines ganzheitlichen Ansatzes, um die Widerstandsfähigkeit der Informations- und Kommunikationstechnologie gegenüber Bedrohungen und Störungen zu stärken.
- (2) Der Leitfaden unterstreicht die Notwendigkeit einer umfassenden Risikobewertung, um die spezifischen Schwachstellen und Risiken in der IKT-Infrastruktur zu identifizieren. Dies ermöglicht es, gezielte Massnahmen zur Stärkung der Resilienz zu entwickeln. Der Fokus liegt dabei nicht nur auf technologischen, sondern auch auf organisatorischen und prozessualen Aspekten.
- (3) Ein zentraler Aspekt ist die Berücksichtigung der IKT-Resilienz in alle Phasen des IKT-Lebenszyklus, von der Planung und Implementierung bis zur Überwachung und kontinuierlichen Verbesserung. Dies erfordert eine enge Zusammenarbeit zwischen IKT-Experten, Sicherheitsbeauftragten und Entscheidungsträgern auf allen Ebenen der Organisation.
- (4) Der Leitfaden hebt auch die Bedeutung von Schulungen und Bewusstseinsbildung hervor, um sicherzustellen, dass alle Mitarbeiter in der Organisation ein Verständnis für die Rolle der IKT-Resilienz haben und aktiv dazu beitragen können. Dies schliesst auch Massnahmen zur Sensibilisierung für Sicherheitsrisiken und zur Schulung im Umgang mit möglichen Sicherheitsvorfällen ein.
- (5) Eine entscheidende Schlussfolgerung ist die Notwendigkeit einer kontinuierlichen Überwachung und Anpassung der IKT-Resilienz Massnahmen. Da sich die Bedrohungslandschaft ständig verändert, ist es wichtig, dass Unternehmen und Organisationseinheiten flexibel auf neue Herausforderungen reagieren können. Dies erfordert regelmässige Überprüfungen, Aktualisierungen von Richtlinien und die Integration neuer Technologien, um den sich wandelnden Anforderungen gerecht zu werden.
- (6) Zusätzlich wird betont, dass die Zusammenarbeit auf sektoraler und internationaler Ebene eine wichtige Rolle spielt. Informationen und Best Practices sollten zwischen Unternehmen und Organisationseinheiten geteilt werden, um gemeinsam eine widerstandsfähigere IKT-Infrastruktur aufzubauen. Dies erfordert eine offene Kommunikation und die Bereitschaft, voneinander zu lernen.
- (7) Insgesamt verdeutlicht der Leitfaden zur Steigerung der IKT-Resilienz im Bereich der Informationssicherheit, dass Resilienz nicht nur als Reaktion auf Bedrohungen betrachtet werden sollte, sondern als integraler Bestandteil der strategischen Planung und Umsetzung von IKT-Systemen. Eine proaktive Herangehensweise, kontinuierliche Anpassung und die Zusammenarbeit auf verschiedenen Ebenen sind entscheidend, um die Widerstandsfähigkeit gegenüber Cyber-Bedrohungen und anderen Risiken zu stärken.



## Anhang A: Glossar

Begriff	Beschreibung
Anti-Virus	Software Auch Virens Scanner genannt. Programm, welches den Computer vor Viren, Würmern und Trojanischen Pferden schützt.
Attachment	(Anhang). An eine E-Mail angehängte Datei. Viele bösartige Programme (Malware, Crimeware) werden so verbreitet und durch das Öffnen der Nachricht oder das Öffnen des Anhangs aktiviert. Anhänge sollten deshalb nur geöffnet werden, wenn man Anti-Virus Software einsetzt und den Absender der Nachricht kennt.
Backup	Vorgang, bei dem durch Speicherung der Daten auf externen Speichermedien deren möglicher Verlust verhindert wird.
Benutzername	(Username) Wird meist in Verbindung mit einem Passwort zur Anmeldung an einem Dienst (z.B. Internet) oder einem Programm verwendet. Betriebssystem Systemsoftware, in der englischen Kurzform als «OS» (Operating System) bezeichnet. Es handelt sich um eine Sammlung von speziellen Programmen, welche den Computer und die Anwendungsprogramme (z.B. Microsoft Word oder Excel) nutzbar machen.
Browser	Programm, das man benutzt, um im Internet Informationen abzurufen. (z.B. Internet Explorer, Opera oder Firefox)
Business Continuity Management (BCM)	Business Continuity Management (BCM) ist ein unternehmensweiter Ansatz, mit dem sichergestellt wird, dass kritische Geschäftsprozesse im Falle von massiven, einschneidenden internen oder externen Ereignissen aufrechterhalten werden können. BCM zielt auf eine Minimierung der operationellen, finanziellen, rechtlichen und reputationsbezogenen Auswirkungen solcher Ereignisse hin (Quelle BCM Weisung)
Business Impact Analysis (BIA)	Die Business Impact Analysis (BIA) ist eine Analyse, die die Auswirkungen von Unterbrechungen auf Geschäftsprozesse bewertet, um kritische Funktionen und Ressourcen zu identifizieren und geeignete Notfallmassnahmen zu planen.
Client	Computer, der an einem Netzwerk angeschlossen ist und mit anderen Computern in Verbindung steht.
Cracker	Ein Hacker, der sein Wissen und seine Erfahrung nutzt, um anderen Schaden zuzufügen.
Crimeware	Sammelbegriff für Programme, die von Crackern und anderen kriminellen Computerbenutzern eingesetzt werden, um anderen Computerbenutzern Schaden zuzufügen. Meist zielt Crimeware darauf ab, Geld oder wertvolle Information (z.B. Kreditkarten-Nummer) zu stehlen. Eine weniger aggressive Form wird als Spyware bezeichnet.
Cybersecurity	Unter dem Begriff «Cybersecurity» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen sowohl der IT als auch der OT verstanden.
Datendiode	Eine Datendiode ist ein Netzwerkgerät, welches den Netzwerkverkehr nur in eine Richtung zulässt. Dabei gilt, dass Daten nur aus einer sicheren Netzwerkzone in eine unsichere Netzwerkzone ausgetauscht werden können, jedoch nicht von der unsicheren in die sichere Zone.
Defense-in-depth	Als „Defense-in-Depth“ werden mehrstufige Sicherheitskonzepte verstanden, die über die rein technische IT-Sicherheit hinausgehen. „Defense-In-Depth“-Konzepte berücksichtigen zusätzlich zum Beispiel auch physische Sicherheit, Business Continuity Management, Prozesse, Menschen und externe Dienstleister
Demilitarized Zone (DMZ)	Unter entmilitarisierte Zone versteht man ein logisch und / oder physisch abgetrenntes Sub-Netz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Systeme.
Dienstleistungsvereinbarung (SLA)	Die Abkürzung “SLA” steht für “Service Level Agreement“. Darunter wird eine vertraglich vereinbarte Leistung verstanden, zu deren Erfüllung sich der IT-Dienstleister verpflichtet hat. Üblicherweise werden in SLA maximal zulässige Ausfall- und Reaktionszeiten definiert.
Facilitymanagement	Siehe Gebäudeleittechnik



Begriff	Beschreibung
Feldbus	Ein Feldbus ist ein Netzwerkelement, welches mehrere Geräte in einem OT-Umfeld miteinander verbindet. Feldbus-Geräte sind per Definition echtzeitfähig. Typischerweise werden in einer Anlage Feldgeräte wie Messfühler (Sensoren) und Stellglieder (Aktoren) zwecks Kommunikation mit einem Automatisierungsgerät verbunden.
Feldbus	Ein Feldbus ist ein Netzwerkelement, welches mehrere Geräte in einem OT-Umfeld miteinander verbindet. Feldbus-Geräte sind per Definition echtzeitfähig. Typischerweise werden in einer Anlage Feldgeräte wie Messfühler (Sensoren) und Stellglieder (Aktoren) zwecks Kommunikation mit einem Automatisierungsgerät verbunden.
Feldgerät	Ein Feldgerät ist eine technische Einrichtung im Bereich der Automatisierungstechnik, die mit einem Produktionsprozess in direkter Beziehung steht. „Feld“ bezeichnet in der Automatisierungstechnik den Bereich ausserhalb von Schaltschränken bzw. Leitwarten.
Feldleittechnik	«Vor-Ort»-Steuerung und «Vor-Ort»-Überwachung einzelner Schaltfelder
Fernwirk-Kopf	Datenkonzentrator wird als Fernwirkgerät zur Automatisierung der Ortsnetzstation und zur Erfassung von Zählerdaten angewendet.
Fernwirktechnik	Unter Fernwirken wird die Fernüberwachung und -steuerung räumlich entfernter Objekte mittels signalumsetzender Verfahren, von einem oder mehreren Orten aus, verstanden. (Quelle Wikipedia)
Field devices	Siehe Feldgerät
Feldbus	Siehe Feldbus
Firewall	Eine Firewall (besser mit Sicherheitgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln. (Quelle BSI)
Frontend	Siehe Fernwirk-Kopf
Gateway	Das Wort Gateway bezeichnet in der Informatik eine Komponente (Hard- und/oder Software), welche zwischen zwei Systemen eine Verbindung herstellt. (Quelle Wikipedia)
Gebäudeleittechnik	Gebäudeleittechnik bezeichnet die Verwaltung und Bewirtschaftung von Gebäuden sowie deren technische Anlagen und Einrichtungen.
Hacker	Spezialist, der über ein enormes Wissen über Computer und Netzwerke verfügt und vorhandene Fehler erkennt und ausnutzt. Im Gegensatz zum Cracker haben Hacker keine illegalen Absichten.
Härtung	Unter Härten versteht man in der Computertechnik, die Sicherheit eines Systems zu erhöhen, indem nur dedizierte Software eingesetzt wird, die für den Betrieb des Systems notwendig ist, und deren unter Sicherheitsaspekten korrekter Ablauf garantiert werden kann. Das System soll dadurch besser vor externen Angriffen geschützt sein. (Quelle Wikipedia)
Hausleittechnik	Siehe Gebäudeleittechnik
House of Policy	Das "House of Policy" im Kontext eines Information Security Management Systems (ISMS) beschreibt die Struktur und Prozesse der Vorgaben zur Informationssicherheit.
House of Processes	Das "House of Processes" ist ein Modell zur Darstellung von Prozessmanagement, das verschiedene Aspekte wie Input, Prozesse, Output und Kundenbedürfnisse in einem Hausdiagramm integriert. Es dient dazu, Prozesse besser zu verstehen und zu optimieren.
Human Maschine Interface (HMI)	Die Benutzerschnittstelle wird auch „Mensch-Maschine-Schnittstelle“ (MMS) oder Englisch „Human Machine Interface“ (HMI) oder „Man Machine Interface“ (MMI) genannt und erlaubt dem Bediener unter Umständen über das Bedienen der Maschine hinaus das Beobachten der Anlagenzustände und das Eingreifen in den Prozess.
Industrial Control Systems (ICS)	Industrial Control Systems werden in der Industrie sowie im Bereich kritischer Infrastrukturen für Steuerungs-, Mess- und Regelfunktionalitäten eingesetzt.



Begriff	Beschreibung
Instant Messenger	Programm, mit dem in Echtzeit kurze Textnachrichten ausgetauscht werden können.
Intelligent Electronic Device (IED)	Ein Intelligent Electronic Device (IED) ist ein Begriff, der in der Elektrizitätsindustrie verwendet wird, um mikroprozessorbasierte Steuerungen von Stromversorgungssystemen, wie etwa Leistungsschalter, Transformatoren und Kondensatorbänke, zu beschreiben.
Information Communications Technology (ICT)	Siehe Informations- und Kommunikationstechnik
Information Security Management System (ISMS)	Das Information Security Management ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
Informationssicherheitsstrategie (ISS)	Die Informationssicherheitsstrategie (ISS) ist eine übergeordnete Planung, die die langfristige Ausrichtung und Ziele für den Schutz von Informationen in einer Organisation festlegt. Sie legt den Rahmen für Sicherheitsmassnahmen und -initiativen fest.
Informationssicherheitspolitik (ISP)	Die Informationssicherheitspolitik (ISP) ist eine umfassende Richtlinie, die die Grundsätze und Verfahren festlegt, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in einer Organisation zu schützen.
Informations- und Kommunikationstechnik (IKT)	Informations- und Kommunikationstechnologien (IKT) sind die Methoden und Technologien, die die Übertragung, den Empfang und die Verarbeitung von Informationen (einschliesslich digitaler Technologien) realisieren.
Integrität	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. (Quelle: BSI)
Intrusion Detection System (IDS)	Intrusion Detection System ist ein System zur automatisierten Erkennung von Angriffen auf Computernetzwerke.
Intrusion prevention System (IPS)	Ein Intrusion Prevention System ist in der Lage Angriffe auf Netzwerke oder Computersysteme zu erkennen und automatische Abwehrmassnahmen zu ergreifen.
IP-Adresse	Numerische Adresse, das Geräte in einem Netzwerk (z.B. Internet) eindeutig identifiziert.
IT-Security	Siehe IT-Sicherheit
IT-Sicherheit	Unter «IT-Sicherheit» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen verstanden. Information Technology (IT) meint dabei Technologien zur Datenverarbeitung, welche nicht direkt mit der Bereitstellung von Elektrizität zu tun haben (z.B. Kundendatenmanagement, Rechenzentren).
Junk-Mail	(Abfall-Mail) Unerwünschte elektronische Post, meist Werbung, wird auch als Spam bezeichnet.
KPI	Der Begriff Key Performance Indicator (KPI) bzw. Leistungskennzahl bezeichnet Kennzahlen, anhand derer der Fortschritt oder der Erfüllungsgrad hinsichtlich wichtiger Zielsetzungen oder kritischer Erfolgsfaktoren innerhalb einer Organisation gemessen und/oder ermittelt werden kann.
Lean-Methoden	Lean-Methoden zielen darauf ab, Verschwendung zu minimieren und kontinuierliche Verbesserung zu fördern. Schlüsselprinzipien umfassen Wertschöpfung, Pull-Prinzip, kontinuierlicher Fluss, Standardisierung, 5S-Methode, Kanban und visuelle Steuerungssysteme. Ziel ist die Schaffung effizienter, qualitativ hochwertiger Prozesse.





Begriff	Beschreibung
Legacy-System	Der Begriff Altsystem bezeichnet in der Informatik eine etablierte, historisch gewachsene Anwendung im Bereich Unternehmenssoftware.
Leittechnik	Die Leittechnik fasst die Datenströme der untergeordneten Ebenen, dem Feld oder einzelner Zellen, wie zum Beispiel Signale der Mess-, Steuer- und Regelungstechnik zusammen, um dadurch den gesamten Fertigungsprozess zu steuern und zu überwachen.
Local Area Network (LAN)	Local area network ist ein Rechnernetz, das Computer und intelligente Geräte in eine limitierte geografischen Zone verbindet (normalerweise unter 10 km).
Malware	Auch Malicious Code genannt. Sammelbegriff für bösartige und schädliche Programme, wie z.B. Viren, Würmer oder Trojanische Pferde
Man-Machine Interface (MMI)	Siehe Human Maschine Interface
Media Access Control Address (MAC Address)	Media Access Control Address wird die eindeutige Hardware-Adresse in einem Netzwerkadapter genannt. Diese wird vom Hersteller unveränderlich in das ROM eines gebrannt. Die Einträge werden weltweit einmalig vergeben.
Mensch-Maschine-Schnittstelle (MMS)	Siehe Human Maschine Interface
Multiprotocol Label Switching - Transport Profile (MPLS-TP)	Das MPLS-TP wurde speziell für Metro-, Aggregation- und Access-Netze optimiert. Die Ziele dabei: Vergleichbare Funktionalitäten wie TDM-basierte (Time Division Multiplexing) Technologien bereitstellen zu können und die Unterstützung von Point-to-Point- und Any-to-Any-Verbindungen mit einem ähnlich hohen Grad an Berechenbarkeit, Zuverlässigkeit und OAM-Funktionalitäten (Operations-, Administration-and-Management), wie sie die langjährig bewährten TDM-Netze bieten.
Multiprotocol Label Switching (MPLS)	Multiprotocol Label Switching ermöglicht die verbindungsorientierte Übertragung von Datenpaketen in einem verbindungslosen Netz entlang eines zuvor aufgebauten („signalisierten“) Pfads. Dieses Vermittlungsverfahren wird überwiegend von Betreibern grosser Transportnetze eingesetzt, die Sprach- und Datendienste auf Basis von IP anbieten. (Quelle Wikipedia)
Network access control (NAC)	Network access control oder Netzwerkszugangskontrolle ist eine Technik angewendet, um sich gegen unautorisierte Netzwerkzugriffe zu schützen.
Network Address Translation (NAT)	Network Address Translation (NAT) bezeichnet ein Verfahren zum automatischen und transparenten Ersetzen von Adressinformationen in Datenpaketen. NAT-Verfahren kommen meist auf Routern und Sicherheits-Gateways zum Einsatz, vor allem, um den beschränkten IPv4-Adressraum möglichst effizient zu nutzen und um lokale IP-Adressen gegenüber öffentlichen Netzen zu verbergen. (Quelle BSI)
Netzeleittechnik	Umfasst die Mess-, Steuerungs- und Regelungstechnik von Netzen wie zum Beispiel den Stromnetzen. Die Netzeleittechnik ist ein Spezialgebiet der Prozessleittechnik; sie gehört zu den Angewandten Ingenieurwissenschaften.
Normalbetrieb	Anlagezustand innerhalb spezifischer Betriebsgrenzen und gemäss geltender Vorschriften (Quelle ENSI)
OEM	Original Equipment Manufacturer, übersetzt «Originalausrüstungshersteller». Darunter versteht man einen Hersteller von Komponenten oder Produkten, der diese in seinen eigenen Fabriken produziert, sie aber nicht selbst in den Einzelhandel bringt. OEM-Software kann sich von der sogenannten Vollversion (Retail) durch einen geringeren Lieferumfang oder eingeschränkte Funktionalität unterscheiden.
Office-IT	"Office-IT" bezieht sich auf Informationstechnologien, die in Büroumgebungen eingesetzt werden, um die Büroarbeit zu unterstützen. Dies umfasst typischerweise Softwareanwendungen, Netzwerke, Computerhardware und IT-Infrastruktur für Büroaufgaben.
OT-Sicherheit	Unter «OT-Sicherheit» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen zur Überwachung und Steuerung der Anlagen zur Elektrizitätsverteilung (und -produktion) sowie der Schutz von Personen und Anlagen verstanden. Operational Technology (OT) meint dabei Technologien, welche direkt für die Bereitstellung oder Lieferung von Elektrizität notwendig sind (z.B. SCADA,



Begriff	Beschreibung
	PIA, Remote Access auf Installationen in Unterwerken, Rundsteuerung, Smart Meter).
Patch	(Pflaster) Aktualisierung von Programmen, bei welchen Fehler entdeckt wurden. Siehe auch Update.
Penetration Test	Unter «Penetration Test» wird ein umfassender Sicherheitstest einzelner Systeme oder Netzwerke verstanden. Es geht um die Prüfung der technischen Umsetzung der Cyber-Sicherheitsmassnahmen. Penetration Tests sind ein Bestandteil eines Sicherheitsaudits.
PDCA-Zyklus	Der PDCA-Zyklus ist ein kontinuierlicher Verbesserungsprozess, bestehend aus Planung, Umsetzung, Überprüfung und Anpassung, der dazu dient, Prozesse effizienter zu gestalten und die Qualität kontinuierlich zu verbessern.
PGP	(Pretty Good Privacy, deutsch: «ziemlich gute Privatsphäre») Programm zur Verschlüsselung von Daten.
Pharming	Erweiterter Phishing-Angriff, der den Computer des Opfers so manipuliert, dass der Angriff nur noch von professionellen Sicherheits- oder Netzwerkspezialisten erkennbar ist. In Anbetracht dieser Angriffsmethode ist der Einsatz eines Virenschanners, einer Firewall und das tägliche Patchen des Computers höchst empfohlen.
Phishing	Angriffsmethode, die ein Opfer dazu verleiten will, Login-Angaben zu finanzrelevanten Diensten (z.B. eBanking) an einen Angreifer zu übermitteln; entweder via E-Mail oder den Besuch auf einer als Original getarnten Internet-Seite.
Port	(Pforte, Tor) Numerische Angabe, die einen Dienst auf einem Rechner adressierbar macht. Damit ist die eindeutige Unterscheidung von verschiedenen Datenpaketen im Netzwerk möglich.
Primärtechnik	Ausser den zur Umspannung notwendigen Transformatoren sind im Umspannwerk auch Schaltanlagen für die ober- und unterspannungsseitig abgehenden Leitungen vorhanden. Die technischen Einrichtungen (Transformatoren, Sammelschienen etc.) sowie die Leitungen sind in der Regel redundant ausgelegt, so dass bei Ausfall eines Betriebsmittels die Versorgung weiterhin gewährleistet ist.
Programmable logical control (PLC)	Siehe Speicherprogrammierbare Steuerung
Provider	Anbieter eines Zuganges zu Netzwerken (z.B. Internet). Bekannte Provider sind Bluewin, Sunrise oder Cablecom.
Prozesskoppelsystem	Das Prozesskoppelsystem stellt das Verbindungselement zwischen der Prozessebene und der Leitebene dar.
Prozessleittechnik	Als Prozessleittechnik bezeichnet man Mittel und Verfahren, die dem Steuern, Regeln und Sichern verfahrenstechnischer Anlagen dienen. Zentrales Mittel sind dabei das Prozessleitsystem und die Speicherprogrammierbare Steuerung.
RASCI-Modell	Das RASCI-Modell ist ein Verantwortlichkeitsmodell, das Rollen und Verantwortlichkeiten in einem Projekt oder Prozess definiert. Es weist die Buchstaben R, A, S, C und I den Begriffen "Responsible" (Verantwortlich), "Accountable" (Rechenschaftspflichtig), "Support" (Unterstützung), "Consulted" (Konsultiert) und "Informed" (Informiert) zu.
Remote Access	Entfernter Zugriff auf ein Netzwerk oder einen Computer, in der Regel über das Internet. Solche Zugriffe sollten nur unter Zuhilfenahme von Sicherheitstechnologien wie Firewalls und VPN ermöglicht werden.
Remote Terminal Unit (RTU)	Als Remote Terminal Unit (RTU, deutsch Fernbedienungsterminal) wird ein regeltechnisches bzw. steuerungstechnisches Instrument zur Fernsteuerung bezeichnet.
Resilienz	Resilienz bezeichnet die Fähigkeit eines Systems, sich nach Störungen zu erholen, sich anzupassen und gestärkt daraus hervorzugehen.
Risiko	Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der



Begriff	Beschreibung
	Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmass dieses Schadens. (Quelle BSI)
Router	Gerät, das Netzwerke miteinander verbindet. Auch als ADSL-Router bekannt.
Sandbox	Eine Sandbox ist ein isolierter Bereich innerhalb einer Anwendung oder eines Betriebssystems. Sie verhindert, dass unerwünschte Aktionen ausserhalb des kontrollierten Umfelds ausgeführt werden können. Dadurch werden die Gefahren und Auswirkungen von Schadprogrammen abgewehrt. (Quelle BSI)
SCADA (Supervisory Control and Data Acquisition)	Unter Supervisory Control and Data Acquisition versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems. Synonym: ICS-System (Industrial Control System)
Schadsoftware	Siehe Malware
Schutzobjekt	Schutzobjekte sind Infrastrukturen, Services, Systeme, Anwendungen, Netzwerke, Datensammlungen, etc., die zur Erfüllung des Unternehmensauftrags eingesetzt und somit geschützt werden müssen.
Schutzsysteme	Sicherungssystem bestehend aus Sensoren, Logik und Steuerelementen, um einen Prozess in einen sicheren Zustand zurückzuführen, wenn vor-definierte Konditionen verletzt wurden.
Schutzziel	Schutzziele beschreiben Schutzobjekte, die mit den entsprechenden Massnahmen geschützt werden.
Sekundärtechnik	Unter den Begriff Sekundärtechnik fallen die Einrichtungen eines Umspannwerks, die an der Umspannung in direktem Sinn nicht beteiligt sind. Darunter versteht man z.B. lokale Steuerung, Spannungsregelung, Netzschutz, Energiezählung, Fernsteuerung, usw.
Server	Computer, der in einem Netzwerk anderen Rechnern (Clients) Dienste zur Verfügung stellt. (z.B. Mail-Server)
Sicherheitsaudit	Unter «Sicherheitsaudit» wird eine umfassende Prüfung der organisatorischen und technischen Cyber-Sicherheitsmassnahmen verstanden. Es geht um die Analyse von Schwachstellen der Cyber-Sicherheit im Bereich der Konzeption/Architektur, Implementierung, Betrieb, menschliches Fehlverhalten und Standortsicherheit sowie die Sicherheit der einzelnen Systemkomponenten.
Sicherheitskultur	Sicherheitskultur umfasst von den Mitgliedern der Organisation des Betreibers einer Kernanlage geteilte Werte, Weltbilder, verbales und non-verbales Verhalten sowie Merkmale der vom Menschen geschaffenen physischen Umgebung. Zur Sicherheitskultur gehören jene Werte, jene Weltbilder, jenes Verhalten und jene Umgebungsmerkmale, die bestimmen oder zeigen, wie die Mitglieder der Organisation mit nuklearer Sicherheit umgehen (Quelle ENSI)
Signatur (digitale)	Digitale Unterschrift mit verbindlichem Charakter.
Six Sigma	Six Sigma ist eine Qualitätsmanagementmethode zur Prozessverbesserung, Fehlerreduzierung und Effizienzsteigerung, die auf statistischen Analysen basiert. Ziel ist es, die Abweichungen in Prozessen zu minimieren und eine hohe Qualitätsstandardisierung zu erreichen.
Security Information and Event Management (SIEM)	SIEM Systeme werden eingesetzt, um sicherheitsrelevante Ereignisse zu identifizieren, zu bewerten und den Administrator daraufhin zu alarmieren.
Smart metering	Intelligente Messsysteme, die über eine bidirektionale Kommunikation ihre Messdaten übertragen und Steueraufgaben übernehmen können.
Smart Card	Plastik-Karte mit einem Chip, der Daten speichern kann, die über die Eingabe eines Codes (PIN) freigegeben werden können.
Spam	Unerwünschte Massen-E-Mails, die als Kettenbrief oder Werbung für dubiose oder spezielle Produkte oder Dienste verschickt werden. Mit dem Spamfilter kann man sich dagegen schützen und einen grossen Teil des Spam aus der regulären Post herausfiltern.
Steuerung (SPS)	Eine speicherprogrammierbare Steuerung ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert wird. (Quelle Wikipedia)



Begriff	Beschreibung
Spyware	Eine Art von Malware, welche eingesetzt wird, um Computeranwender auszuspionieren. Dabei werden das Verhalten, vor allem im Internet, beobachtet oder sogar die Eingaben auf der Tastatur mitgelesen (Passwortklau!). Als Schutz davor sollte regelmässig ein Spyware- Scanner eingesetzt werden.
Stakeholder	Stakeholder sind Personen oder Gruppen, die von den Aktivitäten einer Organisation betroffen sind oder Einfluss darauf haben.
Stationsbus	Bussystem in einem Unterwerk (UW) zwischen der UW-Leitstelle und den Sensoren im Stromfeld.
Stationsleittechnik	Gesamtsteuerung in einem Unterwerk bestehend aus Leitstelle, Sensoren und Aktionen. Ist das Bindeglied zwischen dem Prozess und der Netzleit-ebene.
Strom VV	Die "Stromversorgungsverordnung" (Strom VV) regelt in der Schweiz die Rahmenbedingungen für den Zugang zum Stromnetz und die Verrechnung von Netznutzungsentgelten.
Stromzähler	Stromzähler für die Messung der elektrischen Arbeit (Summierung von Wirkleistung).
Switch	Gerät, das Computer oder Netzwerke miteinander verbindet. Wird in lokalen Netzwerken (LAN) eingesetzt.
Threat Intelligence	Threat Intelligence bezeichnet das Sammeln, Analysieren und Verstehen von Informationen über Cyberbedrohungen, um proaktiv auf Sicherheitsrisiken zu reagieren und Schutzmassnahmen zu verbessern.
Total Quality Management (TQM)	Total Quality Management (TQM) ist eine umfassende Qualitätsmanagementmethode, die darauf abzielt, Qualität in allen Unternehmensprozessen zu integrieren und kontinuierlich zu verbessern.
Trojanisches Pferd	Gefährliches Malware-Programm, welches meist unerkannt und unerlaubt auf dem eigenen Computer gespeichert und ausgeführt wird. Es meldet sich meist bei einem Angreifer (Cracker) und erlaubt die totale Kontrolle des Computers durch den Angreifer. Als Mindestschutz sollte ein Virens Scanner eingesetzt werden.
Tunneling	Tunnel bzw. Tunneling bezeichnet in einem Netzwerk die Konvertierung und Übertragung eines Kommunikationsprotokolls, das für den Transport in ein anderes Kommunikationsprotokoll eingebettet wird.
Update	Aktualisierungsroutine, welche fehlerhafte Programme (z.B.: Betriebssysteme) repariert. Siehe auch Patch.
URL	Adresse einer Seite im Internet, z.B. <a href="http://www.vse.ch">www.vse.ch</a>
USB-Stick	Auch «Memory Stick» genannt. Speichermedium, das am USB-Anschluss des Computers angeschlossen wird. Wird aufgrund seiner kleinen Ausmasse und grossen Speicherkapazität auch von Datendieben genutzt.
USV	Steht für unterbrechungsfreie Stromversorgung. Gerät, das zwischen Stromversorgung und Verbraucher angeordnet wird und bei Stromausfall als Stützbatterie für den Verbraucher wirkt sowie als Filter den Verbraucher vor Spannungsschwankungen schützt.
Utility	Energieversorgungsunternehmen
Verfügbarkeit	Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können. (Quelle BSI)
Verschlüsselung	Verschlüsselung (auch Chiffrierung) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch „Chiffre“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.
Vertraulichkeit	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschliesslich Befugten in der zulässigen Weise zugänglich sein. (Quelle BSI)
Virens Scanner	Programm zum Auffinden und Entfernen von Computerviren und anderen Computerschädlingen. Siehe auch Anti-Virus Software und Malware.



Begriff	Beschreibung
Virtual LANs (VLAN)	Virtuelle lokale Netze werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden.
Virtual Private Network (VPN)	Virtual Private Network ist ein virtuelles privates (in sich geschlossenes) Kommunikationsnetz, das ein bestehendes Kommunikationsnetz als Transportmedium verwendet.
Virus	Meist schädliches Programm (Malware), das Daten zerstört oder die Nutzung des Computers verhindert. Kann durch jede Form der Datenübertragung (Internet, Diskette, CD-ROM, USB-Stick, E-Mail, etc.) verbreitet werden und verlangt zur Aktivierung eine Handlung des Benutzers. Als Schutz sollte ein Virens Scanner eingesetzt und regelmässig aktualisiert und aktiviert werden.
VPN	(Virtual Private Network) Technologie, die durch den Einsatz von Verschlüsselung und Zugangskontrollen (Login) die sichere Nutzung von öffentlichen Netzwerken (z.B. Internet) für private Zwecke ermöglicht.
Wide Area Network (WAN)	Wide Area Network ist ein Rechnernetz, das sich im Unterschied zu einem LAN über einen sehr grossen geographischen Bereich erstreckt.
Wurm / Worm	Schädliches Programm (Malware), das sich ohne Zutun von Dritten und unter Ausnutzung von Schwachstellen oder fehlerhaften Programmen über Netzwerke ausbreitet und diese und die daran angeschlossenen Rechner vorübergehend blockiert. Oft enthalten Würmer auch Befehle, welche Daten zerstören. Als Mindestschutz sollte ein Virens Scanner eingesetzt werden.
Zähler	Siehe Stromzähler
Zombie	Unter der Kontrolle eines Dritten (z.B. Cracker) stehender Computer, der ein Trojanisches Pferd beherbergt und in der Regel für Angriffe auf andere Computer innerhalb des Internet verwendet wird





## Anhang B: Abkürzungsverzeichnis

Abkürzung	Beschreibung
AB-EBV	Ausführungsbestimmungen zur Eisenbahnverordnung
BABS	Bundesamt für Bevölkerungsschutz
BACS	Bundesamt für Cybersicherheit
BDEW	Bundesverband der Energie- und Wasserwirtschaft (Deutschland)
BFE	Bundesamt für Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
BWL	Bundesamt für wirtschaftliche Landesversorgung
CERT	Computer Emergency Response Team
CIRT	Cyber Incident Response Team
CISO	Chief Information Security Officers
CPSO	Chief Physical Safety Officer
CRO	Chief Risk Officer
CSIRT	Computer Security Incident Response Team
CSSE	Certified SCADA Security Engineer
DMZ	Demilitarisierte Zone
DPO	Data Protection Officer oder Compliance- und Datenschutzbeauftragte
EDÖB	Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten
EVU	Energieversorgungsunternehmen
HMI	Human Maschine Interface
HoP	House of Policy
ICS	Industrial Control Systems
ICT	Information and communication technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IKT	Informations- und Kommunikationstechnik
IPS	Intrusion Prevention System
IMS	Integrierte Management System
IR	Incident Response
ISB	Informationssicherheitsbeauftragten
ISC	Information Security Coordinator
ISP	Informationssicherheitspolitik
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO	Information Security Officer
ISS	Informationssicherheitsstrategie
IT	Information Technology
KVM	Keyboard, Video und Maus
LAN	Local Area Network
MAC Address	Media Access Control Address
MMI	Man Maschine Interface
MMS	Mensch-Maschine-Schnittstelle
MPLS	Multiprotokoll Label Switching



Abkürzung	Beschreibung
MPLS-TP	Multiprotokoll Label Switching - Transport Profile
NAC	Network Access Control
NAT	Network Address Translation
NIST	National Institute of Standards and Technology (USA)
OT	Operational Technology
PDH	Plesiochronous Digital Hierarchy
PIA	Partner Informations Austausch
PLC	Programmable logic control
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SDH	Synchronous Digital Hierarchy
SIEM	Security information and event management
SLA	Service Level Agreement, Dienstleistungsvereinbarung
SN	Schweizerische Normen
SOC	Security Operations Center
SPS	Speicherprogrammierbare Steuerung
UFLS	Unterfrequenzabhängiger Lastabwurf
VLAN	Virtual LANs
VPN	Virtual Private Network
VSE	Verband Schweizerischer Elektrizitätsunternehmen
WAN	Wide Area Network



## Anhang C: Gesetzliche Grundlagen: Verpflichtende Gesetze und Verordnungen

- (1) Folgende Zusammenfassung ergibt einen Überblick über die geltenden gesetzlichen Grundlagen in Form von Gesetzes- und Verordnungsartikeln, welche in Zusammenhang mit der Steigerung der IKT-Resilienz bei den Energieversorgern im Bereich Strom angewendet werden müssen:

### C.0 Nationale Ebene

#### Obligationenrecht (SR 220)

Art.	Artikel / Details
754	<p><sup>1</sup> Die Mitglieder des Verwaltungsrates und alle mit der Geschäftsführung oder mit der Liquidation befassten Personen sind sowohl der Gesellschaft als den einzelnen Aktionären und Gesellschaftsgläubigern für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.</p> <p><sup>2</sup> Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.</p>

#### Bundesverfassung der Schweizerischen Eidgenossenschaft (BV; SR 101)

Art.	Artikel / Details
102	<p>Landesversorgung*</p> <p><sup>1</sup> Der Bund stellt die Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen sicher für den Fall machtpolitischer oder kriegerischer Bedrohungen sowie in schweren Mangellagen, denen die Wirtschaft nicht selbst zu begegnen vermag. Er trifft vorsorgliche Massnahmen.</p> <p><sup>2</sup> Er kann nötigenfalls vom Grundsatz der Wirtschaftsfreiheit abweichen.</p>

#### Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz LVG; SR 531)

Art.	Artikel / Details
4	<p>Lebenswichtige Güter und Dienstleistungen</p> <p><sup>1</sup> Lebenswichtig sind Güter und Dienstleistungen, die unmittelbar oder im Rahmen wirtschaftlicher Prozesse zur Überwindung schwerer Mangellagen notwendig sind.</p> <p><sup>2</sup> Lebenswichtige Güter sind insbesondere:</p> <ol style="list-style-type: none"><li>Energieträger sowie alle dazu benötigten Produktions- und Betriebsmittel;</li><li>Nahrungs-, Futter- und Heilmittel sowie Saat- und Pflanzgut;</li><li>andere unentbehrliche Güter des täglichen Bedarfs;</li><li>Roh- und Hilfsstoffe für die Landwirtschaft, die Industrie und das Gewerbe.</li></ol> <p><sup>3</sup> Lebenswichtige Dienstleistungen sind insbesondere:</p> <ol style="list-style-type: none"><li>Transport und Logistik;</li><li>Information und Kommunikation;</li><li>die Übertragung und Verteilung von Energieträgern und Energie;</li><li>die Gewährleistung des Zahlungsverkehrs;</li><li>die Lagerhaltung von Gütern und die Speicherung von Energie.</li></ol> <p><sup>4</sup> Zu den lebenswichtigen Dienstleistungen gehören auch die dafür benötigten Betriebsmittel und Ressourcen.</p>
31	<p>Vorschriften über lebenswichtige Güter</p> <p><sup>1</sup> Im Fall einer unmittelbar drohenden oder bereits bestehenden schweren Mangellage kann der Bundesrat zeitlich begrenzte wirtschaftliche Interventionsmassnahmen ergreifen, um die Versorgung mit lebenswichtigen Gütern sicherzustellen.</p> <p><sup>2</sup> Er kann Vorschriften erlassen über:</p> <ol style="list-style-type: none"><li>die Beschaffung, Zuteilung, Verwendung und den Verbrauch;</li><li>die Einschränkung des Angebots;</li><li>die Verarbeitung und die Anpassung der Produktion;</li><li>die Nutzung, Rückgewinnung und Wiederverwertung von Rohstoffen;</li><li>die Verstärkung der Lagerhaltung;</li><li>die Freigabe von Pflichtlagern und anderen Vorräten;</li><li>die Lieferpflicht;</li><li>die Förderung von Importen;</li><li>die Beschränkung von Ausfuhren.</li></ol> <p><sup>3</sup> Er kann, soweit erforderlich, Rechtsgeschäfte auf Kosten des Bundes abschliessen.</p>



Art.	Artikel / Details
32	<p>Vorschriften über lebenswichtige Dienstleistungen</p> <p><sup>1</sup> Im Fall einer unmittelbar drohenden oder bereits bestehenden schweren Mangellage kann der Bundesrat zeitlich begrenzte wirtschaftliche Interventionsmassnahmen ergreifen, um die Versorgung mit lebenswichtigen Dienstleistungen sicherzustellen.</p> <p><sup>2</sup> Er kann Vorschriften erlassen über:</p> <ol style="list-style-type: none"> <li>die Sicherung, den Betrieb, die Benützung und Indienststellung von Infrastrukturen der Energieversorgungs-, Informations-, Kommunikations- und Transportlogistikunternehmen sowie von Transportmitteln;</li> <li>die Ausdehnung, die Einschränkung oder das Verbot einzelner Dienstleistungen;</li> <li>die Pflicht zur Dienstleistung.</li> </ol> <p><sup>3</sup> Er kann, soweit erforderlich, Rechtsgeschäfte auf Kosten des Bundes abschliessen</p>

#### Verordnung über die wirtschaftliche Landesversorgung (VWLV; SR 531.11)

Art.	Artikel / Details
7	<p>Aufgaben der Fachbereiche</p> <p><sup>1</sup> Die Fachbereiche sind zuständig für:</p> <ol style="list-style-type: none"> <li>das Einbringen und Nutzen von Fachwissen und Erfahrungen aus der Wirtschaft sowie wirtschaftlichen Beziehungen für die wirtschaftliche Landesversorgung;</li> <li>die Vermittlung von Fachwissen;</li> <li>die periodische Lagebeurteilung;</li> <li>die Vorbereitung und den Vollzug von Vorschriften und Massnahmen der</li> <li>Organisation der wirtschaftlichen Landesversorgung.</li> </ol> <p><sup>2</sup> Sie beobachten und analysieren laufend die Entwicklung der wirtschaftlichen Landesversorgung.</p> <p><sup>3</sup> Für die folgenden Fachbereiche gelten die nachstehenden Zuständigkeiten:</p> <ol style="list-style-type: none"> <li>Ernährung: Nahrungsmittel und landwirtschaftliche Produktionsmittel;</li> <li>Energie: fossile Brenn- und Treibstoffe, Elektrizität, Energieholz und Trinkwasser;</li> <li>Heilmittel: Heilmittel für die Human- und Veterinärmedizin;</li> <li>Logistik: Land-, Wasser- und Lufttransporte sowie Logistiksysteme;</li> <li>Industrie: industrielle Hilfsstoffe, namentlich Verpackungsmaterialien;</li> <li>Informations- und Kommunikationstechnologie: Datenübertragung, -sicherheit und -verfügbarkeit.</li> </ol>
11	<p>Vorbereitungsmassnahmen der Fachbereiche</p> <p><sup>1</sup> Die Fachbereiche bereiten Interventionsmassnahmen für die Verteilung, den Verbrauch, die Verwendung und die Herstellung von lebenswichtigen Gütern sowie die Erbringung von lebenswichtigen Dienstleistungen vor; sie erstellen dafür die erforderliche Bereitschaft. Sie koordinieren ihre Tätigkeiten mit den Bundesstellen nach Artikel 8 Absatz 1, die Versorgungsaufgaben wahrnehmen.</p> <p><sup>2</sup> Sie sorgen dafür, dass die für die Erfüllung ihrer Aufgaben erforderlichen Ressourcen und Arbeitskräfte verfügbar sind.</p> <p><sup>3</sup> Sie können ihre Interessen in internationalen Organisationen vertreten</p>

#### Verordnung über die Organisation zur Sicherstellung der wirtschaftlichen Landesversorgung im Bereich der Elektrizitätswirtschaft (VOEW; SR 531.35)

Art.	Artikel / Details
1	<p>Aufgaben des VSE</p> <p><sup>1</sup> Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) trifft für den Fall einer schweren Mangellage in den Bereichen Produktion, Beschaffung, Transport, Verteilung und Verbrauch von Elektrizität die notwendigen Vorbereitungsmassnahmen.</p> <p><sup>2</sup> Er berücksichtigt dabei die regionalen und technischen Gegebenheiten, insbesondere die Stellung der nationalen Netzgesellschaft und der Eidgenössischen Elektrizitätskommission (ElCom).</p> <p><sup>3</sup> Er koordiniert die Aufgaben seiner Mitglieder.</p> <p><sup>4</sup> Bildet der VSE zur Sicherstellung der Versorgung des Landes mit Elektrizität eine besondere Organisation, so können sich Nichtmitglieder des VSE dieser Organisation freiwillig unterstellen.</p>
1a	<p>Monitoringsystem: Betrieb und Zugriff</p> <p><sup>1</sup> Die nationale Netzgesellschaft betreibt ein Monitoringsystem zur Beobachtung der Versorgungslage und von deren Entwicklung im Bereich der Elektrizitätswirtschaft.</p> <p><sup>2</sup> Sie gewährt dem Fachbereich Energie im Abrufverfahren Zugriff auf das Monitoringsystem und erstattet ihm periodisch Bericht über die aktuelle Versorgungslage.</p>
1b	<p>Monitoringsystem: Datenbearbeitung</p> <p><sup>1</sup> Das Monitoringsystem enthält insbesondere Daten über die Produktion und den Verbrauch elektrischer Energie, die Import- und Exportkapazitäten sowie die Eigenversorgungsfähigkeit der Schweiz.</p>



Art.	Artikel / Details
	<p><sup>2</sup> Die Daten stehen dem Fachbereich Energie ab dem Zeitpunkt der Erfassung während zwanzig Jahren zur Verfügung.</p> <p><sup>3</sup> Die nationale Netzgesellschaft stellt mit organisatorischen und technischen Massnahmen sicher, dass die Datenbearbeitung automatisch protokolliert und unbefugte Datenbearbeitung verhindert wird. Sie hält die Massnahmen in einem Datenbearbeitungsreglement fest.</p> <p><sup>4</sup> Die Weitergabe von Daten ist nicht zulässig. Ausgenommen ist die Weitergabe durch den Fachbereich Energie an die ElCom, an das Bundesamt für Energie, an weitere Behörden des Bundes oder eines Kantons sowie an den VSE oder an seine Organisation zur Sicherstellung der Versorgung des Landes mit Elektrizität (Art. 1 Abs. 4), wenn diese Stellen die Daten zur Erfüllung ihres gesetzlichen Auftrags benötigen.</p> <p><sup>5</sup> Die Empfänger der Daten stellen mit organisatorischen und technischen Massnahmen sicher, dass die Daten ausschliesslich für den angegebenen Zweck verwendet werden.</p> <p><sup>6</sup> Die nationale Netzgesellschaft, der Fachbereich Energie und der VSE unterstehen hinsichtlich der Beobachtung der Elektrizitätsversorgungslage sowie der damit zusammenhängenden Informationen der Verschwiegenheitspflicht (Art. 63 LVG). Sie dürfen die Daten aus dem Monitoringsystem ausschliesslich für die Zwecke der wirtschaftlichen Landesversorgung verwenden.</p>
2	<p>Aufgaben des Fachbereichs Energie</p> <p><sup>1</sup> Der Fachbereich Energie bestimmt Art und Umfang der Vorbereitungsmassnahmen und legt die Anforderungen an das Monitoringsystem fest.</p> <p><sup>2</sup> Er überwacht die Vorbereitungsarbeiten des VSE sowie den Betrieb des Monitoringsystems und ist befugt, dem VSE und der nationalen Netzgesellschaft diesbezüglich Weisungen zu erteilen.</p>

### Energiegesetz (EnG; SR 730.0)

Art.	Artikel / Details
7	<p><sup>1</sup> Eine sichere Energieversorgung umfasst die jederzeitige Verfügbarkeit von ausreichend Energie, ein breitgefächertes Angebot sowie technisch sichere und leistungsfähige Versorgungs- und Speichersysteme. Zu einer sicheren Energieversorgung gehört auch der Schutz der kritischen Infrastrukturen einschliesslich der zugehörigen Informations- und Kommunikationstechnik.</p>

### Elektrizitätsgesetz (EleG; SR 734.0)

Art.	Artikel / Details
15d	<p><sup>1</sup> Die Versorgung mit elektrischer Energie ist von nationalem Interesse.</p>

### Bundesgesetz über die Stromversorgung (Stromversorgungsgesetz StromVG; SR 734.7)

Art.	Artikel / Details
6	<p>Lieferpflicht und Tarifgestaltung für feste Endverbraucher</p> <p><sup>1</sup> Die Betreiber der Verteilnetze treffen die erforderlichen Massnahmen, damit sie in ihrem Netzgebiet den festen Endverbrauchern und den Endverbrauchern, die auf den Netzzugang verzichten, jederzeit die gewünschte Menge an Elektrizität mit der erforderlichen Qualität und zu angemessenen Tarifen liefern können.</p>

### Stromversorgungsverordnung (StromVV; SR 734.71)

Art.	Artikel / Details
5	<p><sup>6</sup> Das Bundesamt für Energie (BFE) kann technische und administrative Mindestanforderungen an ein sicheres, leistungsfähiges und effizientes Netz festlegen und internationale technische und administrative Bestimmungen und Normen sowie Empfehlungen anerkannter Fachorganisationen für verbindlich erklären.</p>
5a	<p><sup>1</sup> Zur Sicherstellung eines angemessenen Schutzes von Anlagen vor Cyberbedrohungen, insbesondere mittels Schutzes der Informations- und Kommunikationstechnologien (IKT), sind die Empfehlungen des Minimalstandards zur Verbesserung der IKT-Resilienz von Mai 2023 (IKT-Minimalstandard) gemäss dem jeweiligen Schutzniveau nach Anhang 1a verbindlich für:</p> <ol style="list-style-type: none"> <li>die Netzbetreiber</li> <li>die Erzeuger, mit Ausnahme der Kernkraftwerksbetreiber, und die Speicherbetreiber, sofern sie Anlagen mit einer Leistung von insgesamt mindestens 100 MW betreiben, die sie über ein einziges System fernsteuern können.</li> <li>die Dienstleister, die dauerhaft fernsteuern können: <ol style="list-style-type: none"> <li>Anlagen von Netzbetreibern; oder</li> <li>Anlagen von Erzeugern, mit Ausnahme der Kernkraftwerksbetreiber, oder Speicherbetreibern, sofern sie dadurch über ein einziges System Zugriff haben auf eine Leistung von mindestens 100 MW.</li> </ol> </li> </ol> <p><sup>2</sup> Nicht verbindlich sind die weiteren im IKT-Minimalstandard genannten Regelwerke.</p>





Art.	Artikel / Details
	<sup>3</sup> Das Erreichen des jeweiligen Schutzniveaus ist der ECom auf entsprechendes Verlangen nachzuweisen.

## Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz ISG; SR 128)

Art.	Artikel / Details
5	<p>Begriffe</p> <p>In diesem Gesetz bedeuten:</p> <p>c. kritische Infrastrukturen: Trinkwasser- und Energieversorgung, Informations-, Kommunikations- und Transportinfrastrukturen sowie weitere Prozesse, Systeme und Einrichtungen, die essentiell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind.</p>
74	<p>Aufgaben des Bundes</p> <p><sup>1</sup> Der Bund unterstützt die Betreiberinnen von kritischen Infrastrukturen, um zu gewährleisten, dass Netz- und Systemunterbrechungen sowie Missbräuche selten, von kurzer Dauer und beherrschbar sind und das Schadensausmass gering ist.</p> <p><sup>2</sup> Die Unterstützung im Bereich der Informationssicherheit umfasst:</p> <ol style="list-style-type: none"> <li>die frühzeitige Identifizierung und Bewertung von Bedrohungen, Gefahren,</li> <li>Schwachstellen und Sicherheitslücken;</li> <li>die Erkennung von Vorfällen;</li> <li>die Erhaltung und Wiederherstellung der Informationssicherheit nach einem</li> <li>Vorfall;</li> <li>die Nachbearbeitung von Vorfällen.</li> </ol> <p><sup>3</sup> Der Bund führt einen nationalen Frühwarndienst und eine Anlaufstelle für präventive und reaktive Massnahmen im Bereich der technischen Informationssicherheit.</p> <p><sup>4</sup> Er sorgt dafür, dass die Betreiberinnen von kritischen Infrastrukturen mit den zuständigen Stellen des Bundes sowie gegenseitig Informationen sicher austauschen können.</p> <p><sup>5</sup> Der Bundesrat bezeichnet die für diese Aufgaben zuständigen Stellen des Bundes.</p>
76	<p>Zusammenarbeit im Inland</p> <p><sup>1</sup> Die Stellen nach Artikel 74 Absatz 5 können den Betreiberinnen von kritischen Infrastrukturen Personendaten nach Artikel 75 bekanntgeben, sofern dies zur Gewährleistung der Informationssicherheit zweckmässig ist.</p> <p><sup>2</sup> Sie können den Anbieterinnen und Betreiberinnen von Informatik- und Kommunikationsdiensten Personendaten nach Artikel 75 bekanntgeben, sofern dies zur Gewährleistung der Informationssicherheit von kritischen Infrastrukturen erforderlich ist.</p> <p><sup>3</sup> Die Betreiberinnen von kritischen Infrastrukturen sowie die Anbieterinnen und Betreiberinnen von Informatik- und Kommunikationsdiensten können den Stellen nach Artikel 74 Absatz 5 Daten, einschliesslich Personendaten, die sich auf einen bestimmten Vorfall beziehen, bekanntgeben. Die Stellen nach Artikel 74 Absatz 5 dürfen diese Daten nur mit ausdrücklicher Einwilligung der Datenlieferantinnen zu Strafverfolgungszwecken weitergeben.</p>
77	<p>Internationale Zusammenarbeit</p> <p><sup>1</sup> Die Stellen nach Artikel 74 Absatz 5 können mit ausländischen und internationalen Stellen, die für den Schutz kritischer Infrastrukturen zuständig sind, Daten nach Artikel 75 austauschen, wenn sie diese Daten für die Erfüllung von Aufgaben benötigen, die den Aufgaben nach Artikel 74 entsprechen.</p> <p><sup>2</sup> Der Datenaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe Verwendung gewährleisten.</p> <p><sup>3</sup> Werden die Daten für ein rechtliches Verfahren im Ausland benötigt, so gelten die Bestimmungen über die Amts- und Rechtshilfe</p>
78	<p>Informationssystem zur Unterstützung von kritischen Infrastrukturen</p> <p><sup>1</sup> Die Stellen nach Artikel 74 Absatz 5 betreiben ein Informationssystem, um den sicheren Austausch von Informationen mit den Betreiberinnen von kritischen Infrastrukturen zu gewährleisten.</p> <p><sup>2</sup> Das Informationssystem enthält folgende Informationen:</p> <ol style="list-style-type: none"> <li>Beschreibungen und Einschätzungen von Bedrohungen und Gefahren;</li> <li>Anweisungen zur technischen Erkennung und Behebung von Vorfällen;</li> <li>Vorfallanalysen und Sicherheitsempfehlungen;</li> <li>Analysen betreffend Schwachstellen von Informatikmitteln;</li> <li>Korrespondenz.</li> </ol> <p><sup>3</sup> Die Informationen nach Absatz 2 können auch Personendaten nach Artikel 75 enthalten</p>

## Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR235.1)



Art.	Artikel / Details
	<p>Link zum neuen Datenschutzgesetz:</p> <p><a href="https://www.fedlex.admin.ch/eli/oc/2022/491/de">https://www.fedlex.admin.ch/eli/oc/2022/491/de</a></p>



**Gesetzliche Bestimmungen und Verordnungen vom Bund und den Bundesstellen sind verpflichtend und müssen zwingend eingehalten werden.**

### Internes Kontrollsystem OR 728a, 728b

Aufgabe der Revisionsstelle ist zu prüfen, ob ein internes Kontrollsystem existiert und ob der Bericht Angaben über eine Risikobeurteilung enthalten. Unabhängig davon, welcher Revisionsform eine Gesellschaft unterliegt, ist der Verwaltungsrat verpflichtet, im Anhang der Jahresrechnung Angaben über die Durchführung einer Risikoeinschätzung zu machen. Die Revisionsstelle muss formell prüfen und bestätigen, dass eine Risikoeinschätzung vorgenommen wurde. Inhaltliche Aussagen bezüglich Risikobeurteilung werden ausschliesslich vom Verwaltungsrat erwartet.

Art.	Artikel / Details
728a	<p>2. Aufgaben der Revisionsstelle</p> <p>a. Gegenstand und Umfang der Prüfung</p> <p>1 Die Revisionsstelle prüft, ob:</p> <ol style="list-style-type: none"> <li>1. die Jahresrechnung und gegebenenfalls die Konzernrechnung den gesetzlichen Vorschriften, den Statuten und dem gewählten Regelwerk entsprechen;</li> <li>2. der Antrag des Verwaltungsrats an die Generalversammlung über die Verwendung des Bilanzgewinnes den gesetzlichen Vorschriften und den Statuten entspricht;</li> <li>3. ein internes Kontrollsystem existiert;</li> <li>4.610 bei Gesellschaften, deren Aktien an einer Börse kotiert sind, der Vergütungsbericht den gesetzlichen Vorschriften und den Statuten entspricht.</li> </ol> <p>2 Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfangs der Prüfung das interne Kontrollsystem.</p> <p>3 Die Geschäftsführung des Verwaltungsrats ist nicht Gegenstand der Prüfung durch die Revisionsstelle.</p>
728b	<p>b. Revisionsbericht</p> <p>1 Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das interne Kontrollsystem sowie die Durchführung und das Ergebnis der Revision.</p> <p>2 Die Revisionsstelle erstattet der Generalversammlung schriftlich einen zusammenfassenden Bericht über das Ergebnis der Revision. Dieser Bericht enthält:</p> <ol style="list-style-type: none"> <li>1. eine Stellungnahme zum Ergebnis der Prüfung;</li> <li>2. Angaben zur Unabhängigkeit;</li> <li>3. Angaben zu der Person, welche die Revision geleitet hat, und zu deren fachlicher Befähigung;</li> <li>4. eine Empfehlung, ob die Jahresrechnung und die Konzernrechnung mit oder ohne Einschränkung zu genehmigen oder zurückzuweisen ist.</li> </ol> <p>3 Beide Berichte müssen von der Person unterzeichnet werden, die die Revision geleitet hat.</p>

### Lagebericht OR 961 und 961c

Art.	Artikel / Details
961	<p>A. Zusätzliche Anforderungen an den Geschäftsbericht</p> <p>Unternehmen, die von Gesetzes wegen zu einer ordentlichen Revision verpflichtet sind, müssen:</p> <ol style="list-style-type: none"> <li>1. zusätzliche Angaben im Anhang der Jahresrechnung machen;</li> <li>2. als Teil der Jahresrechnung eine Geldflussrechnung erstellen;</li> <li>3. einen Lagebericht verfassen.</li> </ol>
961c	D. Lagebericht



1 Der Lagebericht stellt den Geschäftsverlauf und die wirtschaftliche Lage des Unternehmens sowie gegebenenfalls des Konzerns am Ende des Geschäftsjahres unter Gesichtspunkten dar, die in der Jahresrechnung nicht zum Ausdruck kommen.

2 Der Lagebericht muss namentlich Aufschluss geben über:

1. die Anzahl Vollzeitstellen im Jahresdurchschnitt;
2. die Durchführung einer Risikobeurteilung;
3. die Bestellungs- und Auftragslage;
4. die Forschungs- und Entwicklungstätigkeit;
5. aussergewöhnliche Ereignisse;
6. die Zukunftsaussichten.

3 Der Lagebericht darf der Darstellung der wirtschaftlichen Lage in der Jahresrechnung nicht widersprechen.

## C.1 Internationale Ebene

Folgende Sammlung von internationalen Gesetzesvorlagen und Richtlinien sind für Unternehmen und Organisationseinheiten teilweise verpflichtend, welche nicht nur auf nationaler Ebene operieren:

- **Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates** vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194 vom 19.7.2016, S. 1
- **Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates** vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 vom 27.12.2022, S. 80



**Internationale gesetzliche Vorgaben und Richtlinien müssen teilweise von Unternehmen und Organisationseinheiten umgesetzt werden, vor Allem wenn sie sich im internationalen Geschäftsumfeld befinden.**



# Anhang D: Institutionen, Frameworks, Normen, Standards, Spezifikation und Anleitungen (Guidelines) zur Steigerung der IKT-Resilienz

(1) In diesem Kapitel werden die Institutionen, Frameworks, Normen, Standards und Spezifikation im Rahmen dieses Leitfadens zur Steigerung der IKT-Resilienz zusammenfassend beschrieben. Diese Beschreibungen geben einen groben Überblick. Um die IKT-Resilienz zu erhöhen, wird empfohlen, sich an aktuelle, etablierte und eingeführte Frameworks, Normen, Standard und Spezifikation, welche von anerkannten Organisationen und Institutionen publiziert werden, zu orientieren. Viele Normen, Standard und Spezifikation dienen als Hilfe für die Umsetzung. Oft weisen die Publikationen keine Anwendungsbeispiele auf, sie dienen lediglich zur Orientierung, Definition von Massnahmen und helfen bei der Lösungsfindung.

## D.0 Organisationen und Institutionen

(2) Folgende Tabelle listet Organisationen und Institutionen auf, welche einen wertvollen Beitrag in Form von Frameworks, Normen, Spezifikationen, Anleitungen und Hilfsmittel zur Steigerung der IKT-Resilienz leisten:

Name	Kurzbeschreibung
<b>SNV (Schweizerische Normen-Vereinigung)</b>	<p>Die SNV, oder Schweizerische Normen-Vereinigung, ist die nationale Normungsorganisation der Schweiz. Sie ist verantwortlich für die Entwicklung und Förderung von technischen Standards und Normen in der Schweiz. Die SNV hat ihren Sitz in Zürich und arbeitet eng mit internationalen Normungsorganisationen wie der internationalen Normen-Organisation (ISO) und dem Europäischen Komitee für Normung (CEN) zusammen. Die Hauptaufgaben der SNV umfassen:</p> <ol style="list-style-type: none"> <li>1. Entwicklung von Normen: Die SNV entwickelt technische Normen und Standards in einer Vielzahl von Branchen und Bereichen, darunter Maschinenbau, Elektrotechnik, Informationstechnologie, Umweltschutz und mehr. Diese Normen dienen dazu, die Qualität und Sicherheit von Produkten und Dienstleistungen zu fördern und die Interoperabilität zu unterstützen.</li> <li>2. Harmonisierung: Die SNV arbeitet daran, die nationalen Normen und Standards der Schweiz mit internationalen und europäischen Normen in Einklang zu bringen, um den freien Handel von Waren und Dienstleistungen zu erleichtern und die Einhaltung internationaler Vorschriften sicherzustellen.</li> <li>3. Schulung und Beratung: Die SNV bietet Schulungen, Workshops und Beratungsdienstleistungen für Unternehmen und Organisationen, um ihnen bei der Implementierung und Einhaltung von Normen zu helfen.</li> <li>4. Informationsverbreitung: Die SNV informiert die Öffentlichkeit über die Bedeutung von Normen und Standards sowie über aktuelle Entwicklungen in der Normung.</li> </ol> <p>Die SNV spielt eine wichtige Rolle bei der Unterstützung der schweizerischen Wirtschaft und Industrie, indem sie eine solide Grundlage für Qualität und Sicherheit bietet. Sie trägt dazu bei, die Wettbewerbsfähigkeit der Schweizer Produkte und Dienstleistungen auf internationalen Märkten zu stärken und die Sicherheit und Effizienz in verschiedenen Branchen zu fördern.</p>
<b>NIST (National Institute of Standards and Technology) USA</b>	<p>Das National Institute of Standards and Technology (NIST) in den USA ist eine Bundesbehörde, die die Entwicklung und Förderung von technischen Standards und Richtlinien in verschiedenen Disziplinen unterstützt. Dies umfasst Bereiche wie Informationssicherheit, Mess- und Prüftechnik sowie Technologiestandards, um Innovation und Interoperabilität zu fördern. NIST spielt eine zentrale Rolle bei der Stärkung der technischen Grundlagen in den USA und der Förderung bewährter Verfahren in verschiedenen Industrien.</p>
<b>CSA (Cloud Security Alliance)</b>	<p>Die Cloud Security Alliance (CSA) ist eine internationale gemeinnützige Organisation, die sich auf die Förderung bewährter Praktiken und Forschung im Bereich der Cybersicherheit und Datenschutz in Cloud-Computing-Umgebungen konzentriert. Gegründet im Jahr 2009, hat die CSA rasch an Bedeutung gewonnen und ist zu einer der führenden Stimmen in der Cloud-Sicherheitsbranche geworden.</p>
<b>CIS (Center for Internet Security)</b>	<p>Das Center for Internet Security (CIS) ist eine gemeinnützige Organisation, die sich auf die Verbesserung der Cybersicherheit und den Schutz von Informationssystemen und Daten konzentriert. Gegründet im Jahr 2000, spielt CIS eine bedeutende Rolle bei der Entwicklung von Cybersicherheitsrichtlinien, Best Practices und Sicherheitskontrollen für Organisationen, Regierungen und Einzelpersonen.</p>



Name	Kurzbeschreibung
<b>ISACA (Information Systems Audit and Control Association)</b>	ISACA (Information Systems Audit and Control Association) ist eine internationale, gemeinnützige Organisation, die sich auf die Bereiche Informationssicherheit, IT-Governance, Risikomanagement und Datenschutz spezialisiert hat. ISACA bietet Zertifizierungen wie CISA (Certified Information Systems Auditor) und CISM (Certified Information Security Manager) an, um Fachleute in diesen Bereichen auszubilden und zu zertifizieren. Die Organisation fördert bewährte Praktiken und bietet Ressourcen und Schulungen zur Verbesserung der IT- und Informationssicherheit in Unternehmen und Organisationen weltweit.
<b>ISO (Internationale Organisation für Normung)</b>	<p>Die Internationale Organisation für Normung (ISO) ist eine weltweit anerkannte Normungsorganisation, die Standards für eine breite Palette von Industrien und Disziplinen entwickelt. Die ISO wurde 1947 gegründet und hat Mitgliedsländer aus der ganzen Welt. Ihr Ziel ist es, internationale Normen zu etablieren, um die Qualität, Sicherheit, Effizienz und Interoperabilität von Produkten, Dienstleistungen und Systemen zu fördern.</p> <p>ISO-Normen decken eine Vielzahl von Bereichen ab, einschliesslich Qualitätsmanagement, Umweltschutz, Informationssicherheit, Gesundheitswesen, Technologie, Sicherheit und vieles mehr. Diese Normen bieten weltweit anerkannte Richtlinien und Best Practices, die Organisationen bei der Verbesserung ihrer Prozesse, Produkte und Dienstleistungen unterstützen.</p> <p>Die ISO entwickelt ihre Standards durch eine Zusammenarbeit von Experten, Technikern und Vertretern aus verschiedenen Ländern, um sicherzustellen, dass die Normen global akzeptiert und angewendet werden können. Die Einhaltung von ISO-Normen ist in vielen Branchen und Ländern eine Voraussetzung für die Zertifizierung und den Zugang zu internationalen Märkten.</p>
<b>IEC (International Electrotechnical Commission)</b>	<p>Die International Electrotechnical Commission (IEC) ist eine weltweit anerkannte internationale Normungsorganisation, die sich auf die Entwicklung von Normen und Standards im Bereich der Elektrotechnik und Elektronik konzentriert. Die IEC wurde 1906 gegründet und hat ihren Hauptsitz in Genf, Schweiz. Sie besteht aus Vertretern aus verschiedenen Ländern und Organisationen und hat das Ziel, technische Standards zu entwickeln, um die Interoperabilität, Sicherheit und Qualität von elektrischen und elektronischen Produkten und Systemen zu fördern.</p> <p>Die IEC entwickelt Standards in einer breiten Palette von Bereichen, darunter:</p> <ol style="list-style-type: none"> <li>1. Elektrische Energieerzeugung und Verteilung</li> <li>2. Elektromagnetische Verträglichkeit (EMV)</li> <li>3. Elektrische Sicherheit</li> <li>4. Informationstechnologie</li> <li>5. Elektrische Messungen und Prüfverfahren</li> <li>6. Elektronik und Halbleitertechnologie</li> <li>7. Umweltverträglichkeit von Elektro- und Elektronikprodukten</li> </ol> <p>IEC-Normen werden von vielen Ländern weltweit übernommen und sind in vielen Industriezweigen verbindlich oder empfehlenswert. Sie bieten klare Leitlinien zur Gewährleistung der Sicherheit, Interoperabilität und Qualität von elektrischen und elektronischen Produkten und Systemen. Die IEC spielt eine wichtige Rolle bei der Unterstützung der technologischen Entwicklung und Innovation und bei der Schaffung von Standards, die den globalen Handel und die Zusammenarbeit fördern.</p>
<b>EN (Europäische Norm)</b>	<p>EN (Europäische Norm) bezieht sich auf Normen, die in der Europäischen Union (EU) gelten. Diese Normen sind spezifisch für europäische Länder und dienen dazu, technische Anforderungen und Standards in verschiedenen Industriezweigen zu harmonisieren und zu vereinheitlichen. Sie unterstützen die Interoperabilität von Produkten und Dienstleistungen und tragen zur Gewährleistung von Qualität und Sicherheit bei.</p> <p>Hier sind einige wichtige Informationen zur EN:</p> <ol style="list-style-type: none"> <li>1. Entwicklung: EN-Normen werden von verschiedenen europäischen Normungsorganisationen entwickelt, darunter das Europäische Komitee für Normung (CEN) und das Europäische Komitee für elektrotechnische Normung (CENELEC). Diese Organisationen arbeiten eng zusammen, um technische Standards für eine Vielzahl von Sektoren und Branchen zu erstellen.</li> <li>2. Anerkennung: EN-Normen werden von den Mitgliedstaaten der EU anerkannt und gelten innerhalb des gesamten EU-Binnenmarktes. Sie sind in der Regel nicht verbindlich, es sei denn, sie werden in Gesetzen oder Vorschriften aufgegriffen, in denen die Einhaltung bestimmter Normen obligatorisch ist.</li> <li>3. Harmonisierung: EN-Normen unterstützen die Harmonisierung von technischen Vorschriften in der EU. Dies erleichtert den freien Verkehr von Waren und Dienstleistungen innerhalb des EU-Binnenmarktes und fördert den Handel.</li> <li>4. Anwendungsbereiche: EN-Normen sind in einer breiten Palette von Bereichen anwendbar, darunter Maschinenbau, Elektrotechnik, Bauwesen, Medizinprodukte, Umweltschutz, Informationstechnologie und viele andere.</li> <li>5. Europäisches Normenkennzeichen: EN-Normen werden durch ein eindeutiges europäisches Normenkennzeichen identifiziert, das den Anwendungsbereich und die Ausgabejahr angibt.</li> </ol>





Name	Kurzbeschreibung
	EN-Normen spielen eine entscheidende Rolle bei der Schaffung eines einheitlichen Standards für Produkte und Dienstleistungen in der EU und sind von grosser Bedeutung für Hersteller, Dienstleister und Unternehmen, die auf europäischen Märkten tätig sind. Sie unterstützen die Qualitätssicherung, die Sicherheit und die Konformität mit EU-Vorschriften.
<b>ISA (International Society of Automation)</b>	<p>Die International Society of Automation (ISA) ist eine globale gemeinnützige Organisation, die sich auf die Förderung von Automatisierungs- und Steuerungstechnologien konzentriert. Die ISA wurde 1945 gegründet und hat ihren Hauptsitz in den USA. Sie ist eine der weltweit führenden Organisationen, die Fachleuten in den Bereichen Automatisierung, Prozesssteuerung, Mess- und Regelungstechnik sowie Cybersicherheit in der Industrie unterstützt.</p> <p>Die ISA bietet eine breite Palette von Ressourcen, darunter Schulungen, Zertifizierungen, technische Publikationen und Standards, um Fachleuten bei der Weiterbildung und beruflichen Entwicklung zu helfen. Die Organisation spielt eine wichtige Rolle bei der Förderung von bewährten Praktiken und Technologien in den Bereichen Industrieautomatisierung, Prozesssteuerung und Instrumentierung.</p> <p>Zu den Hauptaktivitäten der ISA gehören:</p> <ol style="list-style-type: none"> <li>1. Entwickeln von Standards: Die ISA entwickelt technische Standards und Normen, die in der Industrie weitverbreitet sind und zur Interoperabilität und Sicherheit von Automatisierungssystemen beitragen.</li> <li>2. Weiterbildung und Schulung: Die ISA bietet Schulungen, Seminare und Zertifizierungen an, um Fachleuten in der Automatisierungs- und Steuerungstechnik die erforderlichen Fähigkeiten und Kenntnisse zu vermitteln.</li> <li>3. Konferenzen und Veranstaltungen: Die ISA organisiert Konferenzen, Messen und Veranstaltungen, auf denen Fachleute ihr Wissen und ihre Erfahrungen austauschen können.</li> <li>4. Veröffentlichung von Technologiezeitschriften und Fachliteratur: Die ISA veröffentlicht technische Zeitschriften und Fachbücher, um aktuelle Entwicklungen und bewährte Praktiken in der Branche zu teilen.</li> </ol> <p>Die ISA spielt eine wichtige Rolle in der Förderung von Automatisierungs- und Steuerungstechnologien, und ihre Bemühungen tragen dazu bei, die Effizienz und Sicherheit in verschiedenen Industriezweigen zu verbessern.</p>
<p>Die Zusammenhänge zwischen ISA (International Society of Automation), IEC (International Electrotechnical Commission) und EN (Europäische Normen) sind wie folgt:</p> <ol style="list-style-type: none"> <li>1. ISA und IEC: ISA und IEC sind beide internationale Organisationen, die sich auf die Entwicklung von technischen Standards und Normen konzentrieren. Während ISA sich vor allem auf die Automatisierungs- und Steuerungstechnik in der Industrie spezialisiert, deckt die IEC eine breitere Palette von elektrotechnischen und elektronischen Technologien ab. Beide Organisationen entwickeln Normen und Standards, die weltweit in verschiedenen Industriezweigen und Ländern angewendet werden können. In einigen Fällen arbeiten ISA und IEC zusammen, um gemeinsame Standards zu entwickeln, insbesondere in Bereichen, in denen die Schnittstelle zwischen Automatisierung und Elektrotechnik von Bedeutung ist.</li> <li>2. EN-Normen: EN-Normen sind europäische Normen, die in der Europäischen Union (EU) gelten. Diese Normen können von verschiedenen internationalen und nationalen Normungsorganisationen entwickelt werden, darunter auch die IEC. EN-Normen sind auf europäischer Ebene anerkannt und gelten in den Mitgliedstaaten der EU. In einigen Fällen sind EN-Normen direkte Übernahmen von IEC-Normen, wobei Anpassungen an die europäischen Anforderungen vorgenommen werden. ISA-Normen sind weniger spezifisch auf europäische Standards ausgerichtet, da die ISA eine amerikanische Organisation ist.</li> </ol> <p>Insgesamt gibt es Wechselwirkungen zwischen diesen Organisationen und ihren Normen, insbesondere in internationalen Märkten und Industrien, die auf weltweite Standards angewiesen sind. Unternehmen, die Produkte und Dienstleistungen auf internationalen Märkten anbieten, müssen die relevanten Normen und Standards berücksichtigen, um die Interoperabilität und die Einhaltung von Vorschriften sicherzustellen.</p>	
<b>ENISA (European Union Agency for Cybersecurity)</b>	<p>ENISA steht für "European Union Agency for Cybersecurity" und ist eine EU-Agentur, die für die Förderung und Stärkung der Cybersicherheit in der Europäischen Union verantwortlich ist. ENISA wurde 2004 gegründet und hat ihren Sitz in Griechenland. Die Hauptaufgaben von ENISA umfassen:</p> <ol style="list-style-type: none"> <li>1. Cybersicherheitsberatung: ENISA bietet Expertise und Unterstützung in Fragen der Cybersicherheit für EU-Institutionen, Mitgliedstaaten und andere Akteure in Europa.</li> <li>2. Forschung und Entwicklung: Die Agentur fördert die Forschung und Entwicklung von Cybersicherheitslösungen und bewährten Praktiken in der EU.</li> <li>3. Awareness und Schulung: ENISA arbeitet daran, das Bewusstsein für Cybersicherheitsfragen in der EU zu steigern und Schulungsprogramme für Fachleute und die breite Öffentlichkeit zu entwickeln.</li> <li>4. Koordinierung der Zusammenarbeit: Die Agentur fördert die Koordination und den Austausch von Informationen und bewährten Praktiken in der EU, um die Cybersicherheit zu stärken.</li> </ol>



Name	Kurzbeschreibung
	ENISA spielt eine wichtige Rolle bei der Förderung der Cybersicherheit in der EU und arbeitet eng mit den Mitgliedstaaten, der Europäischen Kommission und anderen Partnern zusammen, um die digitale Infrastruktur und Daten vor Bedrohungen zu schützen.
<b>IEEE (Institute of Electrical and Electronics Engineers)</b>	<p>Das IEEE, oder Institute of Electrical and Electronics Engineers, ist eine weltweit anerkannte professionelle Organisation, die sich auf die Förderung und Weiterentwicklung von Technologie und Wissenschaft im Bereich Elektrotechnik, Elektronik, Informationstechnologie und verwandten Disziplinen konzentriert. Das IEEE ist eine der grössten technischen Organisationen der Welt und hat Mitglieder aus verschiedenen Ländern, darunter Ingenieure, Wissenschaftler und Fachleute aus einer breiten Palette von technischen Disziplinen.</p> <p>Das IEEE spielt eine wichtige Rolle bei der Entwicklung von technischen Standards und Richtlinien in verschiedenen Bereichen, darunter drahtlose Kommunikation, Computerhardware, Netzwerktechnologien und viele andere. Diese Standards tragen zur Interoperabilität von Technologien bei und fördern Innovation und Qualität.</p> <p>Die Organisation organisiert auch Konferenzen, veröffentlicht wissenschaftliche Zeitschriften und fördert den Wissensaustausch und die berufliche Weiterentwicklung von Fachleuten. Das IEEE hat verschiedene technische Gesellschaften, die sich auf spezifische Bereiche wie Elektronik, Telekommunikation, Informatik und mehr konzentrieren.</p>
<b>BSI (Deutsches Bundesamt für Sicherheit in der Informationstechnik)</b>	<p>Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die nationale Cybersecurity-Behörde in Deutschland. Es wurde 1991 gegründet und hat seinen Sitz in Bonn. Das BSI ist für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung und die Unterstützung von Unternehmen und Bürgern in Deutschland verantwortlich.</p> <p>Die Hauptaufgaben des BSI umfassen:</p> <ol style="list-style-type: none"> <li>1. Beratung und Unterstützung: Das BSI bietet Beratung und Ressourcen zur Verbesserung der IT-Sicherheit in der Bundesverwaltung, in Unternehmen und bei Privatpersonen.</li> <li>2. Zertifizierung und Standards: Das BSI entwickelt Sicherheitsstandards und Zertifizierungsverfahren für IT-Produkte und -Systeme, um sicherzustellen, dass sie den hohen Sicherheitsanforderungen entsprechen.</li> <li>3. Incident Response: Das BSI reagiert auf Cyberangriffe und koordiniert Massnahmen zur Abwehr von Sicherheitsvorfällen.</li> <li>4. Sensibilisierung und Aufklärung: Die Behörde informiert die Öffentlichkeit über aktuelle Cyberbedrohungen und fördert das Bewusstsein für IT-Sicherheit.</li> </ol> <p>Das BSI spielt eine entscheidende Rolle bei der Gewährleistung der Cybersicherheit in Deutschland und trägt dazu bei, die digitale Infrastruktur und Daten vor Cyberangriffen und Bedrohungen zu schützen.</p>
<b>NERC (North American Electric Reliability Corporation)</b>	<p>Die North American Electric Reliability Corporation (NERC) ist eine gemeinnützige Organisation in Nordamerika, die sich auf die Gewährleistung der Zuverlässigkeit und Stabilität des elektrischen Stromnetzes in den Vereinigten Staaten, Kanada und Mexiko konzentriert. NERC ist mit der Entwicklung und Durchsetzung von Standards und Vorschriften für die Stromversorgungsbranche in Nordamerika beauftragt.</p> <p>Die wichtigsten Aufgaben und Verantwortlichkeiten von NERC umfassen:</p> <ol style="list-style-type: none"> <li>1. Entwicklung von Standards: NERC entwickelt technische Standards und Normen, die für den sicheren Betrieb des Stromnetzes in Nordamerika erforderlich sind. Diese Standards umfassen Themen wie Betrieb, Planung, Cybersicherheit und Schutz von Stromübertragungs- und -Verteilungssystemen.</li> <li>2. Überwachung und Durchsetzung: NERC überwacht und überprüft die Einhaltung der von ihr entwickelten Standards und Vorschriften durch die Stromversorgungsunternehmen. Sie setzt Sanktionen durch, wenn Unternehmen gegen diese Standards verstossen.</li> <li>3. Cybersicherheit: NERC spielt eine wichtige Rolle bei der Sicherung des Stromnetzes vor Cyberbedrohungen. Sie entwickelt und fördert Standards zur Verbesserung der Cybersicherheit in der Energieversorgungsbranche.</li> <li>4. Krisenmanagement: NERC unterstützt die Vorbereitung und Reaktion auf Notfälle und Krisensituationen, die das Stromnetz betreffen, und fördert die Zusammenarbeit zwischen den Stromversorgungsunternehmen und anderen beteiligten Parteien.</li> </ol> <p>Die Arbeit von NERC ist von entscheidender Bedeutung, da ein zuverlässiges Stromnetz für die Wirtschaft, die öffentliche Sicherheit und das tägliche Leben in Nordamerika von grosser Bedeutung ist. Die Organisation arbeitet eng mit verschiedenen Interessengruppen, darunter Regierungsbehörden, Versorgungsunternehmen, Betreiber von Übertragungsnetzen und anderen relevanten Parteien, um sicherzustellen, dass das elektrische Stromnetz den höchsten Standards für Sicherheit und Zuverlässigkeit entspricht.</p>



## D.1 Frameworks

Name	Kurzbeschreibung
<b>NIST CSF 1.1 (Cyber-Security Framework Version 1.1)</b>	<p>NIST CSF 1.1 (Cyber-Security Framework Version 1.1) ist die aktuelle Version des Cybersecurity Frameworks des National Institute of Standards and Technology (NIST) in den USA. Dieses Framework dient zur Verbesserung der Cybersecurity-Praktiken in Organisationen und Unternehmen. Version 1.1 beinhaltet erweiterte Leitlinien für die Risikominderung und die Verbesserung der Resilienz gegenüber Cyberbedrohungen.</p> <p>Das NIST CSF 1.1 basiert auf fünf Kernelementen: Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellung. Diese Elemente helfen Unternehmen und Organisationseinheiten dabei, ihre Cybersecurity-Programme zu entwickeln, zu bewerten und zu verbessern, indem sie bewährte Praktiken und Standards implementieren. Die Aktualisierung 1.1 enthält auch zusätzliche Schwerpunkte auf Datenschutz und Privatsphäre sowie die Berücksichtigung von Cyber-Risiken bei der Lieferkette.</p>
<b>NIST SP 800-Serie</b>	<p>Die NIST SP 800-Serie besteht aus einer Reihe von Spezialveröffentlichungen (Special Publications, SP) des National Institute of Standards and Technology (NIST) der Vereinigten Staaten. Diese Publikationen decken verschiedene Aspekte der Informationssicherheit und des Datenschutzes ab und bieten Leitlinien, bewährte Praktiken und Empfehlungen zur Stärkung der Sicherheit von Informationssystemen und zur Bewältigung von Sicherheitsherausforderungen. Die NIST 800-Serie ist international anerkannt und wird von Unternehmen und Organisationseinheiten auf der ganzen Welt als wertvolle Ressource zur Verbesserung der Informationssicherheit und des Datenschutzes eingesetzt. Diese Publikationen werden regelmässig aktualisiert, um den sich wandelnden Anforderungen und Bedrohungen im Bereich der Informationssicherheit gerecht zu werden, und sie dienen als wichtige Referenzdokumente für Unternehmen und Organisationseinheiten, Behörden, Unternehmen und Organisationseinheiten, die ihre Sicherheitspraktiken stärken möchten.</p>
<b>COBIT 5 (Control Objectives for Information and Related Technologies Version 5)</b>	<p>COBIT 5 ist ein Rahmenwerk für die Unternehmens- und Organisationseinheiten-IT-Governance und das Management von Informationstechnologie. Es wurde von der internationalen Organisation ISACA entwickelt und ist die fünfte Version des COBIT-Frameworks (Control Objectives for Information and Related Technologies). COBIT 5 bietet Unternehmen und Organisationseinheiten eine umfassende Methode zur Verbesserung ihrer IT-Governance und -Managementprozesse. Hier sind einige wichtige Merkmale und Ziele von COBIT 5:</p> <ol style="list-style-type: none"> <li>1. IT-Governance: COBIT 5 legt die Grundsätze und Strukturen für die effektive IT-Governance fest, um sicherzustellen, dass die IT-Strategie und -Ressourcen den geschäftlichen Zielen entsprechen.</li> <li>2. Ganzheitlicher Ansatz: COBIT 5 bietet ein ganzheitliches Modell, das IT-Management, Risikomanagement und Compliance integriert, um die IT-Servicebereitstellung zu optimieren.</li> <li>3. Prozessorientierung: Das Framework stellt Prozessmodelle und Leitlinien für die IT-Governance und -Managementprozesse bereit, um die Effizienz und Effektivität zu steigern.</li> <li>4. Wertorientierung: COBIT 5 betont die Wertschöpfung durch IT und stellt sicher, dass IT-Investitionen die geschäftlichen Ziele unterstützen.</li> <li>5. Kontinuierliche Verbesserung: Das Framework fördert die kontinuierliche Überwachung und Optimierung der IT-Governance- und Managementpraktiken.</li> </ol> <p>COBIT 5 ist in der IT-Branche weitverbreitet und wird von Unternehmen und Organisationseinheiten genutzt, um ihre IT-Strukturen zu optimieren, Compliance-Anforderungen zu erfüllen und IT-Ressourcen effektiv einzusetzen. Es bietet klare Leitlinien und Best Practices, um die Qualität und Zuverlässigkeit von IT-Diensten und -Systemen zu verbessern und die geschäftlichen Ziele zu erreichen.</p>
<b>CSA CCM (Cloud Controls Matrix)</b>	<p>Die Cloud Controls Matrix (CCM) ist ein Framework, das von der Cloud Security Alliance (CSA) entwickelt wurde. Die Cloud Security Alliance ist eine internationale Organisation, die sich auf die Förderung von bewährten Praktiken und Sicherheitsstandards in Bezug auf Cloud-Computing konzentriert. Die CCM ist ein wichtiger Bestandteil der Bemühungen der CSA zur Verbesserung der Sicherheit in der Cloud.</p> <p>Die CCM ist eine Sammlung von Sicherheitskontrollen und -praktiken, die in verschiedenen Bereichen des Cloud-Computings Anwendung finden. Diese Kontrollen und Praktiken sind in einer Matrix strukturiert, die Unternehmen und Organisationseinheiten bei der Bewertung und Verbesserung der Sicherheit ihrer Cloud-Umgebungen unterstützt. Die CCM ist in mehrere Domänen unterteilt, darunter:</p> <ol style="list-style-type: none"> <li>1. Governance und Compliance</li> <li>2. Risikomanagement</li> <li>3. Datenklassifizierung und Schutz</li> <li>4. Identity and Access Management</li> <li>5. Infrastruktur und Virtualisierung</li> <li>6. Betrieb und Incident Response</li> <li>7. Compliance und Audit</li> </ol>



Name	Kurzbeschreibung
	<p>Unternehmen und Organisationseinheiten können die CCM verwenden, um sicherzustellen, dass sie angemessene Sicherheitskontrollen in ihren Cloud-Umgebungen implementieren und die Einhaltung bewährter Praktiken sicherstellen. Die CCM kann als Leitfaden für die Evaluierung von Cloud-Service-Providern und die Definition von Anforderungen in Bezug auf Sicherheit und Datenschutz dienen.</p> <p>Insgesamt ist die Cloud Controls Matrix ein nützliches Werkzeug, um die Sicherheit in Cloud-Umgebungen zu erhöhen und das Vertrauen in die Cloud-Dienste zu stärken.</p>
<b>CIS CSC (Center for Internet Security Critical Security Controls)</b>	<p>CIS CSC steht für "Center for Internet Security Critical Security Controls." Es handelt sich um ein Rahmenwerk mit 20 grundlegenden Sicherheitskontrollen, die von der gemeinnützigen Organisation Center for Internet Security (CIS) entwickelt wurden. Diese Kontrollen sind als bewährte Praktiken und Sicherheitsstandards konzipiert und dienen dazu, die Cybersicherheit von Unternehmen und Organisationseinheiten zu stärken und Schwachstellen zu minimieren.</p> <p>Die 20 CIS CSC-Kontrollen sind in drei Hauptkategorien unterteilt:</p> <ol style="list-style-type: none"> <li>1. Basic Cyber Hygiene (Grundlegende Cyber-Hygiene): <ul style="list-style-type: none"> <li>- Inventar und Kontrolle von Hard- und Software</li> <li>- Sicherheitskonfigurationen für Hard- und Software</li> <li>- Überwachung und Sicherheitsbewertungen</li> </ul> </li> <li>2. Foundational Security Controls (Grundlegende Sicherheitskontrollen): <ul style="list-style-type: none"> <li>- Datenklassifizierung und -schutz</li> <li>- Virenschutz und Malware-Abwehr</li> <li>- Netzwerksegmentierung</li> <li>- Datensicherung und Wiederherstellung</li> <li>- Sichere Verwaltung von Aktualisierungen und Patches</li> <li>- Endpunkt-Sicherheit</li> <li>- User-Account- und Berechtigungsverwaltung</li> <li>- Multifaktor-Authentifizierung</li> <li>- Datenverkehrsbegrenzung</li> <li>- Sichere E-Mail und Web-Gateways</li> </ul> </li> <li>3. Organizational Security Controls (Organisatorische Sicherheitskontrollen): <ul style="list-style-type: none"> <li>- Security Awareness and Training (Sicherheitsbewusstsein und -schulung)</li> <li>- Incident Response and Management (Reaktion und Management von Sicherheitsvorfällen)</li> <li>- Penetration Tests and Red Team Exercises (Penetrationstests und Red-Team-Übungen)</li> <li>- Continuous Monitoring (Kontinuierliche Überwachung)</li> <li>- Security Metrics (Sicherheitsmetriken)</li> </ul> </li> </ol> <p>Die CIS CSC sind darauf ausgerichtet, Unternehmen und Organisationseinheiten dabei zu helfen, sich vor den heutigen komplexen Cyberbedrohungen zu schützen, Schwachstellen zu identifizieren und Gegenmassnahmen zu ergreifen. Sie sind ein wertvolles Instrument zur Verbesserung der Sicherheit von Informationssystemen und zur Minimierung von Risiken. Unternehmen und Organisationseinheiten können die CIS CSC nutzen, um ihre Sicherheitsstrategien zu entwickeln und ihre Sicherheitsprogramme zu optimieren.</p>
<b>NERC CIP (Cyber Security Permanent)</b>	<p>NERC CIP steht für "North American Electric Reliability Corporation Critical Infrastructure Protection," was auf deutsch "Schutz der kritischen Infrastruktur der North American Electric Reliability Corporation" bedeutet. Es handelt sich um ein umfangreiches Regelwerk und eine Reihe von Cyber-Sicherheitsstandards, die von der North American Electric Reliability Corporation (NERC) entwickelt wurden, um die Cybersicherheit in der nordamerikanischen Stromversorgungsbranche zu stärken.</p> <p>NERC CIP besteht aus mehreren Versionen, wobei die aktuelle Version 6 ist. Die Standards und Anforderungen, die in NERC CIP festgelegt sind, zielen darauf ab, das Stromnetz vor Cyberbedrohungen zu schützen und die Widerstandsfähigkeit des elektrischen Stromversorgungssystems sicherzustellen. Die CIP-Standards beinhalten Vorschriften für den Schutz von Systemen und Informationen, die für den Betrieb des Stromnetzes kritisch sind, sowie für den Schutz vor unbefugtem Zugriff und die Erkennung und Bewältigung von Sicherheitsvorfällen.</p> <p>Die NERC CIP-Anforderungen umfassen Themen wie:</p> <ol style="list-style-type: none"> <li>1. Identifizierung und Klassifizierung von kritischen Assets und Informationen.</li> <li>2. Durchführung von Risikobewertungen und -management.</li> <li>3. Physische und logische Zugangskontrollen zu kritischen Infrastrukturen.</li> <li>4. Überwachung, Meldung und Reaktion auf Cyber-Sicherheitsvorfälle.</li> <li>5. Schulung und Sensibilisierung der Mitarbeiter im Bereich Cybersicherheit.</li> <li>6. Kontinuierliche Verbesserung der Sicherheitspraktiken.</li> </ol> <p>Die NERC CIP-Standards gelten für Stromerzeuger, Übertragungsnetzbetreiber, Verteilungsnetzbetreiber und andere Einrichtungen in der Stromversorgungsbranche in den Vereinigten Staaten, Kanada und Mexiko. Sie sind darauf ausgerichtet, sicherzustellen, dass die Stromversorgung in Nordamerika vor Cyberangriffen geschützt ist, und tragen zur Gewährleistung der Zuverlässigkeit und Integrität des Stromnetzes bei.</p>





Name	Kurzbeschreibung
	Die NERC CIP-Compliance ist für Unternehmen und Organisationseinheiten in der Energiebranche von entscheidender Bedeutung, da die Nichteinhaltung dieser Standards schwerwiegende rechtliche und finanzielle Konsequenzen haben kann. Unternehmen und Organisationseinheiten müssen umfassende Massnahmen zur Cybersicherheit implementieren, um den NERC CIP-Anforderungen zu entsprechen und das Stromnetz vor Cyberbedrohungen zu schützen.
<b>ISO 27000-Serie</b>	Die ISO 27000-Serie ist eine Sammlung internationaler Normen und Leitlinien, die sich auf das Informationssicherheitsmanagement und die Informationssicherheit in Unternehmen und Organisationseinheiten konzentrieren. Die Normenreihe wird von der Internationalen Organisation für Normung (ISO) entwickelt und gepflegt und bietet einen umfassenden Rahmen für die Planung, Umsetzung und Aufrechterhaltung von Informationssicherheit in Unternehmen und Organisationseinheiten. Die ISO 27000-Serie ist von grosser Bedeutung für Unternehmen und Organisationseinheiten jeder Grösse und Branche, da sie klare Leitlinien und bewährte Praktiken zur Sicherung von Informationen und Informationssystemen bietet. Sie ist besonders relevant in einer Zeit, in der die Cybersicherheit von entscheidender Bedeutung ist und Unternehmen und Organisationseinheiten vermehrt mit Cyberbedrohungen konfrontiert sind. Die Einhaltung dieser Normen trägt dazu bei, das Vertrauen von Kunden, Partnern und Interessengruppen in die Sicherheit und Integrität von Informationen zu stärken und rechtliche und regulatorische Anforderungen zu erfüllen.
<b>IEC TC 70</b>	<p>Die IEC TC 70 steht für das "Technical Committee 70" der International Electrotechnical Commission (IEC). Dieses technische Komitee ist spezialisiert auf die Normung von Anwendungen und Technologien im Bereich der elektrischen Energieerzeugung, -übertragung, -verteilung und -nutzung. IEC TC 70 entwickelt internationale Standards und Normen, die eine breite Palette von Aspekten im Zusammenhang mit elektrischen Energieversorgungssystemen abdecken.</p> <p>IEC TC 70 behandelt eine Vielzahl von Themen und Aspekten, darunter:</p> <ol style="list-style-type: none"> <li>1. Elektrische Generatoren und Motoren: Normen für die Konstruktion und Prüfung von Generatoren und Motoren, die in Energieerzeugungsanlagen und Industrieanwendungen eingesetzt werden.</li> <li>2. Leistungstransformatoren: Normen für die Konstruktion, Prüfung und Anwendung von Leistungstransformatoren, die in Übertragungs- und Verteilungsnetzen verwendet werden.</li> <li>3. Schutz- und Steuerungssysteme: Normen für Schutzrelais, Steuerungssysteme und Automatisierungslösungen in Energieversorgungssystemen.</li> <li>4. Hochspannungsanlagen: Normen für die Konstruktion und Prüfung von Hochspannungsanlagen, einschliesslich Schaltanlagen und Schaltanlagenkomponenten.</li> <li>5. Energiemanagement und Qualitätsüberwachung: Normen, die sich mit der Überwachung der Qualität elektrischer Energie und dem Energiemanagement in Versorgungsnetzen befassen.</li> </ol> <p>IEC TC 70 spielt eine entscheidende Rolle bei der Schaffung von Standards, die die Sicherheit, Effizienz und Interoperabilität von elektrischen Energieversorgungssystemen weltweit gewährleisten. Diese Standards sind von grosser Bedeutung für die Energiebranche, da sie dazu beitragen, die Zuverlässigkeit der Energieversorgung zu gewährleisten und die Integration erneuerbarer Energiequellen und neuer Technologien in die Netze zu erleichtern.</p>
<b>BSI-Standards</b>	<p>Das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland entwickelt und veröffentlicht eine Reihe von Standards und Richtlinien im Bereich der Informationssicherheit. Diese Standards sind darauf ausgerichtet, Unternehmen und Organisationseinheiten bei der Sicherung ihrer Informationssysteme und -daten zu unterstützen. Hier sind einige der wichtigsten BSI-Standards:</p> <ol style="list-style-type: none"> <li>1. BSI IT-Grundschutz: Der BSI IT-Grundschutz ist ein umfassender Standard, der bewährte Praktiken und Empfehlungen zur Sicherung von Informationssystemen enthält. Er bietet einen Rahmen für die Identifizierung von Schutzbedarf und die Umsetzung von Sicherheitsmassnahmen.</li> <li>2. BSI-Standards 100-4 bis 100-3: Diese Standards befassen sich mit dem Risikomanagement von Informationssicherheit und bieten Leitlinien zur Identifizierung, Analyse und Bewertung von Risiken in Informationssystemen.</li> <li>3. BSI-Standards 200-1 bis 200-4: Diese Standards behandeln die Sicherung von IT-Systemen, Netzwerken und Kommunikationstechnologien. Sie bieten Empfehlungen zur Implementierung von Sicherheitsmassnahmen und zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen.</li> <li>4. BSI-Standards 300-3 und 300-4: Diese Standards befassen sich mit dem Thema Business Continuity Management (BCM) und bieten Leitlinien zur Planung und Umsetzung von Massnahmen zur Aufrechterhaltung der Geschäftskontinuität im Falle von Störungen oder Katastrophen.</li> </ol>





Name	Kurzbeschreibung
	<p>5. BSI-Standards 100-1 und 100-2: Diese Standards behandeln die Themen Awareness und Schulung im Bereich Informationssicherheit und bieten Empfehlungen zur Sensibilisierung der Mitarbeiter und zur Schulung in Sicherheitsfragen.</p> <p>6. BSI-Standards 400-1 bis 400-3: Diese Standards befassen sich mit den Aspekten der Identitäts- und Zugangsmanagement (IAM) und bieten Empfehlungen zur Verwaltung von Benutzeridentitäten und Zugriffsrechten in Informationssystemen.</p> <p>Die BSI-Standards sind wichtige Instrumente zur Verbesserung der Informationssicherheit in Deutschland und gelten als Leitfaden für Unternehmen und Organisationseinheiten in verschiedenen Sektoren. Sie dienen der Minimierung von Risiken, der Gewährleistung der Einhaltung von Vorschriften und der Stärkung der Sicherheit von Informationssystemen. Unternehmen und Organisationseinheiten sollten die BSI-Standards in ihre Sicherheitsstrategien und -praktiken integrieren, um angemessene Massnahmen zur Sicherung ihrer IT-Infrastruktur zu ergreifen.</p>

## D.2 Spezifische wichtige Standards und Normen

Name	Kurzbeschreibung
<b>NIST SP 800-53</b>	<p>NIST SP 800-53 (Special Publication 800-53) ist ein Dokument des National Institute of Standards and Technology (NIST) in den USA, das Sicherheits- und Datenschutzkontrollen für Bundesbehörden, Unternehmen und Organisationseinheiten, die mit vertraulichen Informationen arbeiten, festlegt. Dieses Dokument ist Teil des NIST Cybersecurity Frameworks und spielt eine wichtige Rolle bei der Festlegung von Sicherheitsstandards und -kontrollen für Informationssysteme und -technologien.</p> <p>Die NIST SP 800-53 enthält eine umfassende Sammlung von Sicherheitskontrollen, die in 18 Familien oder Kategorien unterteilt sind, wie zum Beispiel Zugriffskontrolle, Identitätsmanagement, Überwachung und Schutz von Kommunikationssystemen. Diese Kontrollen bieten detaillierte Anleitungen und Empfehlungen zur Absicherung von IT-Systemen und Daten, um sicherzustellen, dass sie den höchsten Sicherheitsstandards entsprechen.</p> <p>Die Verwendung von NIST SP 800-53 ist in den USA weitverbreitet und erstreckt sich über Bundesbehörden hinaus, da viele Unternehmen und Organisationseinheiten es als bewährten Standard für die Sicherheit ihrer Informationssysteme anerkennen. Es bietet einen klaren und strukturierten Rahmen für die Entwicklung, Implementierung und Überwachung von Sicherheitskontrollen und trägt dazu bei, die Informationssicherheit und Datenschutz in einer sich ständig weiterentwickelnden Bedrohungslandschaft zu gewährleisten.</p>
<b>IEC 62351 (Informationssicherheit in der Netz- und Stationsleittechnik)</b>	<p>IEC 62351 ist eine Normenreihe, die sich mit dem Thema "Informationssicherheit in der Netz- und Stationsleittechnik" befasst. Diese Normenreihe wurde von der International Electrotechnical Commission (IEC) entwickelt und ist darauf ausgerichtet, die Sicherheit und Integrität von Informationssystemen in der Energieversorgungsbranche, insbesondere in den Bereichen Netz- und Stationsleittechnik, zu gewährleisten.</p> <p>Die IEC 62351-Normenreihe besteht aus verschiedenen Teilen, die spezifische Aspekte der Informationssicherheit in Energieversorgungssystemen abdecken.</p> <p>Die IEC 62351-Normenreihe zielt darauf ab, die Informationssicherheit in kritischen Infrastrukturen im Energiesektor zu stärken und vor Cyberbedrohungen zu schützen. Dies ist von entscheidender Bedeutung, da eine Störung oder ein Angriff auf Energieversorgungssysteme erhebliche Auswirkungen auf die Gesellschaft und die Wirtschaft haben kann. Die Normen bieten Leitlinien und bewährte Praktiken zur Gewährleistung der Sicherheit, Integrität und Verfügbarkeit von Informationssystemen in diesem Sektor. Unternehmen und Organisationseinheiten in der Energiebranche sollten die IEC 62351-Normenreihe berücksichtigen, um sicherzustellen, dass sie angemessene Massnahmen zur Informationssicherheit implementieren.</p>
<b>IEC 62443 (Industrielle Kommunikationsnetze - Netz- und Systemsicherheit)</b>	<p>IEC 62443 ist eine internationale Normenreihe, die sich auf die Netz- und Systemsicherheit in industriellen Kommunikationsnetzen konzentriert. Diese Normen wurden von der International Electrotechnical Commission (IEC) entwickelt und sind darauf ausgerichtet, die Cybersicherheit von Systemen und Netzwerken in der industriellen Automatisierung und Steuerungstechnik zu gewährleisten. Die Normenreihe trägt dazu bei, kritische Infrastrukturen und industrielle Prozesse vor Cyberbedrohungen zu schützen.</p> <p>IEC 62443 besteht aus mehreren Teilen, die verschiedene Aspekte der Netz- und Systemsicherheit abdecken. Sie zielt darauf ab, die Sicherheit und Integrität von industriellen Steuerungs- und Automatisierungssystemen sicherzustellen, um Störungen, Ausfälle und Sicherheitsverletzungen zu verhindern. Diese Normenreihe ist von grosser Bedeutung, da industrielle Prozesse und kritische Infrastrukturen, wie Energieerzeugung, Transport und Fertigung, stark von automatisierten Systemen abhängen. Sie bietet klare Leitlinien und bewährte Praktiken zur Sicherung dieser Systeme vor Cyberbedrohungen und unterstützt die Widerstandsfähigkeit von Industriernetzwerken. Unternehmen und Organisationseinheiten in der industriellen Automatisierung sollten IEC 62443 in ihre</p>



Name	Kurzbeschreibung
	Sicherheitsstrategien und -praktiken einbeziehen, um die Zuverlässigkeit und Sicherheit ihrer Betriebsabläufe zu gewährleisten.
<b>ISO/IEC 27001, 27002</b>	<p>ISO/IEC 27001 und ISO/IEC 27002 sind internationale Normen im Bereich der Informationssicherheit, die entwickelt wurden, um Unternehmen und Organisationseinheiten bei der Implementierung und Aufrechterhaltung eines wirksamen Informationssicherheitsmanagementsystems (ISMS) zu unterstützen. Diese Normen sind wichtig für die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in Unternehmen und Organisationseinheiten. Hier sind die wichtigsten Informationen zu diesen Normen:</p> <p>ISO/IEC 27001:</p> <ul style="list-style-type: none"> <li>- ISO/IEC 27001 ist die Hauptnorm für das Informationssicherheitsmanagementsystem. Sie legt die Anforderungen fest, die eine Organisation erfüllen muss, um ein effektives ISMS einzurichten, zu betreiben, aufrechtzuerhalten und kontinuierlich zu verbessern.</li> <li>- Die Norm enthält einen systematischen Ansatz zur Risikobewertung und -behandlung, um sicherzustellen, dass Sicherheitsrisiken identifiziert und angemessen adressiert werden.</li> <li>- Unternehmen und Organisationseinheiten, die ISO/IEC 27001 umsetzen, verfolgen einen risikobasierten Ansatz, um Sicherheitskontrollen und -Massnahmen zu identifizieren und zu implementieren, die ihren spezifischen Bedürfnissen entsprechen.</li> <li>- ISO/IEC 27001 ermöglicht die Zertifizierung, bei der unabhängige Prüfstellen die Einhaltung der Norm überprüfen und Unternehmen und Organisationseinheiten eine ISO/IEC 27001-Zertifizierung ausstellen können.</li> </ul> <p>ISO/IEC 27002:</p> <ul style="list-style-type: none"> <li>- ISO/IEC 27002, auch bekannt als "Code of Practice for Information Security Controls," ist ein begleitendes Dokument zu ISO/IEC 27001. Es bietet detaillierte Empfehlungen und Leitlinien für die Umsetzung von Informationssicherheitskontrollen.</li> <li>- Die Norm enthält eine umfassende Liste von Sicherheitskontrollen und -Massnahmen, die in verschiedenen Bereichen der Informationssicherheit eingesetzt werden können, wie Zugriffskontrolle, Verschlüsselung, Incident Management, und vieles mehr.</li> <li>- ISO/IEC 27002 bietet konkrete Massnahmen und Praktiken, die Unternehmen und Organisationseinheiten bei der Erfüllung der Anforderungen von ISO/IEC 27001 unterstützen.</li> </ul> <p>Zusammen bilden ISO/IEC 27001 und ISO/IEC 27002 eine wichtige Grundlage für die Planung und Implementierung von Informationssicherheitsmassnahmen in Unternehmen und Organisationseinheiten. Diese Normen helfen dabei, Sicherheitsrisiken zu bewerten, Sicherheitsziele festzulegen und effektive Kontrollen zur Sicherung von Informationen zu implementieren. Sie sind für Unternehmen und Organisationseinheiten jeglicher Grösse und Branche relevant und tragen zur Sicherung der Unternehmensdaten und Systeme bei. Die Zertifizierung nach ISO/IEC 27001 ist ein anerkanntes Zeichen für ein hohes Sicherheitsniveau und kann das Vertrauen von Kunden, Partnern und Interessengruppen stärken.</p>
<b>ISO/IEC 27019</b>	<p>ISO/IEC 27019 ist eine internationale Norm, die speziell für den Energiesektor entwickelt wurde und sich auf die Informationssicherheit in der Energiebranche konzentriert. Diese Norm bietet Richtlinien und Empfehlungen zur Sicherung von Informationssystemen und -daten in der Energieerzeugung, -übertragung und -verteilung.</p> <p>Hier sind die wichtigsten Merkmale und Ziele von ISO/IEC 27019:</p> <ol style="list-style-type: none"> <li>1. Anwendungsgebiet: ISO/IEC 27019 richtet sich an Unternehmen und Organisationseinheiten im Energiesektor, darunter Versorgungsunternehmen, Netzbetreiber, Energieerzeuger und andere Akteure in der Energieversorgungskette.</li> <li>2. Schutz kritischer Infrastrukturen: Die Norm ist darauf ausgerichtet, die kritischen Infrastrukturen im Energiesektor vor verschiedenen Bedrohungen, einschliesslich Cyberangriffen, zu schützen. Sie hilft, die Stabilität und Zuverlässigkeit des Stromnetzes sicherzustellen.</li> <li>3. Anwendung von ISO/IEC 27001: ISO/IEC 27019 baut auf den Grundsätzen und Anforderungen von ISO/IEC 27001 auf, der internationalen Norm für Informationssicherheitsmanagementsysteme (ISMS). Die Norm stellt sicher, dass Unternehmen und Organisationseinheiten im Energiesektor spezifische Anforderungen der Branche berücksichtigen und die besten Praktiken der Informationssicherheit einhalten.</li> <li>4. Sicherheitskontrollen und -Massnahmen: ISO/IEC 27019 enthält eine Liste von Sicherheitskontrollen und -Massnahmen, die in den Bereichen Zugriffskontrolle, Verschlüsselung, Schutz von Anlagen und Systemen, Incident Management und anderen Aspekten der Informationssicherheit relevant sind.</li> <li>5. Risikobasiertes Vorgehen: Die Norm fördert die Anwendung eines risikobasierten Ansatzes zur Identifizierung, Bewertung und Behandlung von Sicherheitsrisiken im Energiesektor.</li> </ol> <p>Die Einhaltung von ISO/IEC 27019 hilft Unternehmen und Organisationseinheiten im Energiesektor, die Sicherheit ihrer Informationssysteme zu stärken und die</p>



Name	Kurzbeschreibung
	Widerstandsfähigkeit gegenüber Cyberbedrohungen zu erhöhen. Dies ist von entscheidender Bedeutung, da die Energiewirtschaft eine kritische Infrastruktur ist, die erhebliche Auswirkungen auf die Gesellschaft und die Wirtschaft hat. Durch die Umsetzung von ISO/IEC 27019 können Unternehmen und Organisationseinheiten im Energiesektor sicherstellen, dass sie angemessene Massnahmen zur Sicherung ihrer IT-Systeme und Daten in einer sich ständig wandelnden Bedrohungslandschaft implementieren.
<b>ENISA Network Code on Cyber Security</b>	Der ENISA Network Code on Cyber Security zielt darauf ab, einen europäischen Standard für die Cybersicherheit grenzüberschreitender Stromflüsse zu schaffen. Er enthält Regeln für die Bewertung von Cyberrisiken, gemeinsame Mindestanforderungen, die Zertifizierung von Produkten und Dienstleistungen im Bereich der Cybersicherheit, die Überwachung, die Berichterstattung und das Krisenmanagement. Dieser Netzkodex enthält eine klare Definition der Aufgaben und Zuständigkeiten der verschiedenen Akteure für jede Tätigkeit.



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**



# Anhang E: VSE-Tools zur Steigerung der IKT-Resilienz

## E.0 VSE & BFE Assessment-Tool NIST CSF 1.1 ++ inkl. SoA, Maturitäten gemäss BFE und Hilfen für Umsetzung



Das BFE und der VSE haben in Zusammenarbeit mit der Arbeitsgruppe zu Erhöhung der IKT-Resilienz ein Tool entwickelt, dass die Unternehmen und Organisationseinheiten in der Strombranche bei der Erhöhung der IKT-Resilienz und der Umsetzung der nötigen Massnahmen unterstützt.



In den Schulungen des VSE wird die Anwendung des Tools genau erläutert.

### E.0.1 Ziel und Zweck

Das VSE & BFE Assessment-Tool NIST CSF 1.1++ bietet den Mitgliedern des VSE Unterstützung bei der Stärkung der IKT-Resilienz. Das Tool kann entsprechend den Vorgaben des Schutzprofils (festgelegt im Strom VV) für das jeweilige Unternehmen und die Organisationseinheiten konfiguriert werden. Dadurch sind alle Anforderungen gemäss den Schutzniveaus im Strom VV anschliessend ersichtlich.



Die ausführlichen Kommentare helfen dem Anwender mit nützlichen zusätzlichen Informationen.

### E.0.2 Register "Dokument Owner & History"

Im Abschnitt "Dokument Owner & History" werden relevante Angaben zu den Unternehmen oder Organisationseinheiten gemacht. Darüber hinaus können Informationen zur präzisen Identifizierung, Überarbeitung, Klassifizierung, Geltungsbereich und Historie des Dokuments bereitgestellt werden.

### E.0.3 Register "Assessment 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- Tabelle	Category Kategorie Kategorie	Checkpoints (Subcategory) Komponenten (Subkategorie) Maassnahmen (Subkategorie)	Priority by BFE	Rating / Bewertung / Appreciation / Stim												Informative References Informative Referenzen Informazioni			
				Grid operator area				Energy producer area				General IT area (Baseline)							
				Applicability	Present	Maturity	Target	Applicability	Present	Maturity	Target	Applicability	Present	Maturity	Target				
								Need for action				Need for action							
								Quick Wins				Quick Wins							
		ID AM-1: Develop an inventory-rating process which ensures that you have a complete inventory of all your ICT assets at all times. Erstellen Sie einen Inventurierungsprozess welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar Ihrer IKT-Betriebsmittel (Assets) vorhanden ist. Developpez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC (Assets). Definire una procedura che garantisca la costante presenza di un inventario completo dei vostri strumenti operativi TIC (asset).	High	-	0	4	0	-	0	4	0	-	0	0	0	VSE-BFE-Zusammenstellung NIST SP 800-53 Rev. 5, CIS und CSC (inkl. SoA) VSE-Leitfaden: Kapitel: VSE-Dokumente: ISA 62443-2-3:2009 4.2.3.4 ISA 62443-3-3:2009 3P.7.8 ISO/IEC 27001:2005 7.1.1.7.12 ISO/IEC 27001:2002 A.5.9 BSI-Standard 100-2 Kapitel 4.2, M.2.25 CISIT 5 BAP 01, BAP 02, BAP 05 NERC CIP-002			
		ID AM-2: Produce an inventory of all of the software platform/licenses and applications within your organization. Inventarisieren Sie alle Softwareplattformen/-Lizenzen und Applikationen innerhalb Ihrer Organisation. Inventorize toutes les plateformes, licences et applications logicielles dans votre entreprise. Inventariare tutte le piattaforme/licenze e applicazioni di software all'interno dell'organizzazione.	High	-	0	4	0	-	0	4	0	-	0	0	0	VSE-BFE-Zusammenstellung NIST SP 800-53 Rev. 5, CIS und CSC (inkl. SoA) VSE-Leitfaden: Kapitel: VSE-Dokumente: ISA 62443-2-3:2009 4.2.3.4 ISA 62443-3-3:2009 3P.7.8 ISO/IEC 27001:2005 7.1.1.7.12 ISO/IEC 27001:2002 A.5.9 A.5.2 BSI-Standard 100-2 Kapitel 4.2, M.2.25 CISIT 5 BAP 01, BAP 02, BAP 05 NERC CIP-002			
																		VSE-BFE-Zusammenstellung NIST SP 800-53 Rev. 5, CIS und CSC (inkl. SoA) VSE-Leitfaden: Kapitel:	

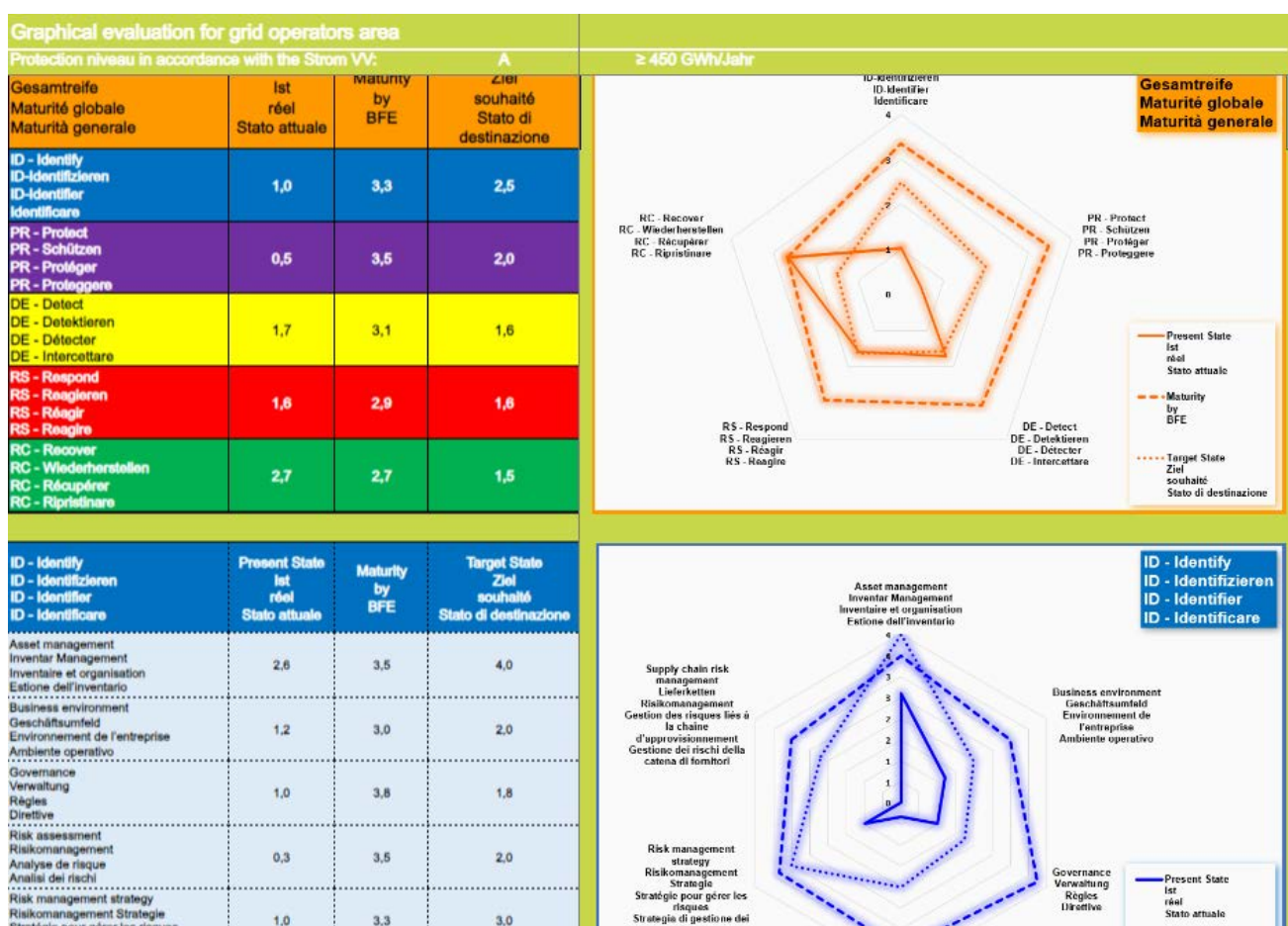
Der Aufbau und die Funktionen können wie folgt zusammengefasst werden:

- Basiert auf dem NIST Cyber Security Framework CFS 1.1 und den BWL IKT-Minimalstandard Assessment Tool
- Die Bewertung ist in drei Gebiete, welche separat behandelt werden können, aufgeteilt:
  - "Grid operator area" Gebiet des Netzbetreibers
  - "Energy producer area" Gebiet für Energieproduktion und Energiespeicherung
  - "General IT area" Gebiet für die allgemeine IT, primär die Büro- bzw. Business-Bereiche, gilt auch als Baseline für die gesamte OT/IT-Umgebung
- Der Anwender kann sein zugewiesenes Schutzniveau gemäss Strom VV wählen



- Die Prioritäten und Maturitäten gemäss Vorgaben im Strom VV sind je nach Wahl des Schutzniveaus aufgeführt
- Die Anwendbarkeit kann abgebildet werden
- Der aktuelle Stand der Maturität kann abgebildet werden (Self Assessment)
- Das Soll- bzw. Ziel-Maturitäten kann abgebildet werden
- Bei den "Kommentaren" können zu den einzelnen Checkpoints Kommentare eingetragen werden z.B. Begründung bei Nichtanwendbarkeit
- "Need for action" zeigen dem Anwender die Differenz zwischen den Vorgabe-Maturität zur IST-Maturität farblich dar. Dies soll als Hilfe für die Priorisierung der Massnahmen verstanden werden.
- "Quick Wins" zeigen dem Anwender farblich dar, wo aus Sicht der VSE Cyber Security Task Force Experten schnelle Erfolge (Massnahmen ohne grossen Aufwand mit grosser Wirkung) erzielt werden können
- Referenzen: Zeigt Verweise auf zusätzliche Dokumente oder Normen und Spezifikationen auf

#### E.0.4 Grafische Auswertung in den "Results"-Registern



Bei den grafischen Auswertungen werden die IST-, Soll- und Ziel-Maturitäten dargestellt. Diese Auswertung hilft dem Anwender einfacher zu erkennen, wo die grössten Unterschiede bei den verschiedenen Maturitäten liegen. Dabei gibt es eine Auswertung über das gesamte Framework wie auch für die einzelnen Funktionen.

#### E.0.5 Register "Assistance Information"

Im Register "Assistance Informationen" sind alle nötigen Erklärungen und Ausführungen zu den verschiedenen variablen Punkten im Register "Assessment NIS CSF 1.1 ++" aufgeführt.



**BFE & VSE (Branche)**  
**Assessment Tool ++**  
**(inkl. Need for Action**  
**und Quick Wins)**



—

Der Aufbau und die Funktionen in diesen Registern können wie folgt zusammengefasst werden:

- Basiert auf dem NIST Cyber Security Framework CFS 1.1 und den BWL IKT-Minimalstandard Assessment Tool
- Zu den Checkpoints gemäss NIST CSF 1.1 sind entsprechend die Massnahmen der NIST Special Publication 800-53 Revision 5, CSA Cloud Controls Matrix v3.0.1 und CIS Critical Security Controls v8 aufgeführt.
- Bei den NIST Special Publication 800-53 Revision 5, CSA Cloud Controls Matrix v3.0.1 und CIS Critical Security Controls v8 sind die ID, der Titel und die Beschreibung der einzelnen Massnahme ersichtlich
- Die Bewertung ist in drei Gebiete, welche separat behandelt werden können, aufgeteilt:
  - "Grid operator area" Gebiet des Netzbetreibers
  - "Energy producer area" Gebiet für Energieproduktion und Energiespeicherung
  - "General IT area" Gebiet für die allgemeine IT, primär die Büro- bzw. Business-Bereiche, gilt eigentlich als Baseline für die gesamte OT/IT-Umgebung
- Das Gebiet "Grid operator area" ist in zwei Teilgebiete dem "Grid Domain Core" mit den Sub-Teilgebieten "Grid Scada" (Leitsysteme), "Grid Load Control" (Laststeuerung), "Grid Field System" (Feldsysteme, Umspannwerke, Transformationsanlagen usw.) und dem Teilgebiet "Grid Domain Support & Management" unterteilt. Diese Teilgebiete werden im "Grid over all" automatisch zusammengefasst. Mit dieser Unterteilung erhält der Anwender eine grössere Granularität.
- Das Gebiet "Energy producer area" ist in zwei Teilgebiete dem "Energy Domain Core" mit den Sub-Teilgebieten "Energy producer SCADA" (Leitsysteme), "Energy Management System" (Energiemanagementsysteme), "Energy producer Field System" (Feldsysteme, Kraftwerke, Speicherwerke usw.) und dem Teilgebiete "Energy producer Domain Support & Management" unterteilt. Diese Teilgebiete werden im "Energy producer over all" automatisch zusammengefasst. Mit dieser Unterteilung erhält der Anwender eine grössere Granularität.
- Der Anwender kann sein zugewiesenes Schutzniveau gemäss Strom VV wählen, dabei werden automatisch die anzuwendenden Massnahmen dargestellt oder grau hinterlegt.
- Die Maturitäten auf Stufe NIST CSF 1.1 Checkpoints gemäss Vorgaben im Strom VV sind je nach Wahl des Schutzniveaus aufgeführt
- Die Anwendbarkeit kann abgebildet werden
- Der aktuelle Stand der Maturität kann abgebildet werden (Self Assessment)
- Das Soll- bzw. Ziel-Maturitäten kann abgebildet werden
- Bei den "SoA, n/a or Evidenz" können zu den einzelnen Massnahmen Kommentare eingetragen werden z.B. Begründung für eine Nichtanwendbarkeit oder Nachweise

#### **E.1.4 Register "Assistance Information"**

Im Register "Assistance Informationen" sind alle nötigen Erklärungen und Ausführungen zu den verschiedenen variablen Punkten im Register "All Functions", "IDENTIFY (ID)", "PROTECT (PR)", "DETECT (DE)", "RESPOND (RE)" und "RECOVER (RC)" aufgeführt.

## **E.2 VSE-Tool NIST CSF 1.1 HoP-Mapping**

Das "VSE-Tool NIST CSF 1.1 HoP Mapping" hilft dem Anwender bei der Erstellung der HoP-Dokumente. In diesem Tool werden die einzelnen Checkpoints aus dem NIST CSF 1.1 den entsprechenden Dokumenten im HoP zugewiesen. Dies erleichtert dem Anwender auch die Nachweisführung.

### **E.2.1 Register "Dokument Owner & History"**

Im Abschnitt "Dokument Owner & History" werden relevante Angaben zu den Unternehmen oder Organisationseinheiten gemacht. Darüber hinaus können Informationen zur präzisen Identifizierung, Überarbeitung, Klassifizierung, Geltungsbereich und Historie des Dokuments bereitgestellt werden.



### E.2.2 Register "All Function HoP"

[illegible]

Die einzelnen Checkpoints gemäss NIST CSF 1.1 können den HoP-Dokumenten zugewiesen werden.

### E.3 VSE Assessment-Tool ISO27001 Annex A incl. Controls acc.to ISO27002

Das VSE haben in Zusammenarbeit mit der Arbeitsgruppe zu Erhöhung der IKT-Resilienz ein Tool entwickelt, dass die Unternehmen und Organisationseinheiten in der Strombranche bei der Erhöhung der IKT-Resilienz und der Umsetzung der nötigen Massnahmen im Rahmen von ISO27001 Annex A vollumfänglich unterstützen soll.



In den Schulungen des VSE wird die Anwendung des Tools genau erläutert.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.

### E.3.1 Ziel und Zweck

Falls vom Anwender gewünscht, kann das VSE Assessment-Tool ISO27001 Annex A incl. Controls acc.to ISO27002 für die VSE Mitglieder Unterstützung bei der Erhöhung der IKT-Resilienz bieten. Im diesem Tool werden die einzelnen Controls von ISO 27001:2022 Annex A behandelt.



**Die ausführlichen Kommentare helfen dem Anwender mit nützlichen zusätzlichen Informationen.**

### E.3.2 Register "Dokument Owner & History"

Im Abschnitt "Dokument Owner & History" werden relevante Angaben zu den Unternehmen oder Organisationseinheiten gemacht. Darüber hinaus können Informationen zur präzisen Identifizierung, Überarbeitung, Klassifizierung, Geltungsbereich und Historie des Dokuments bereitgestellt werden.



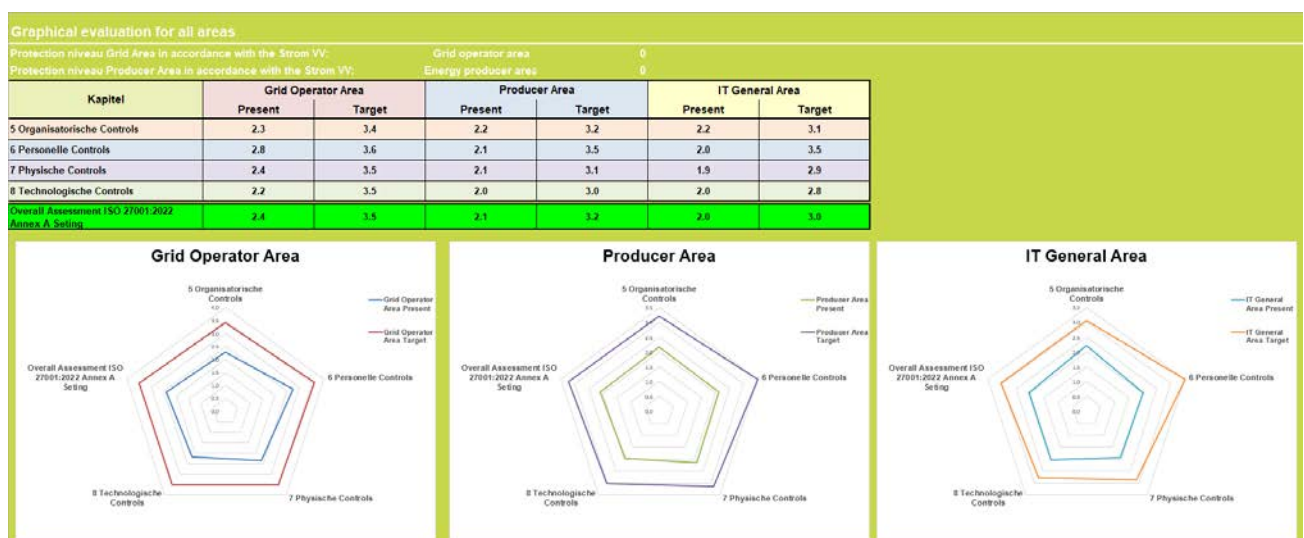
### E.3.3 Register "Assessment Tool ISO 27001"

VSE Assessment Tool ISO27001:2022 Annex A					Organisation protection niveau according to BFE:										Company: Strom AG																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			
Grid operator area: A ≥ 450 GWh/year					Energy producer area: B 10 MW and < 500 MW										Area of validity: Entire Strom AG Group with subsidiaries																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			
This document may only be used if a valid license for ISO 27001/27002 is available.					Status: In Progress																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
Kapitel	Titel	Detail	Control	Priority	Sating - Bewertung - Appreciation - Status										Proposed Zweck Object Scope	Kind Art Control Model	Target Ziel Objective OJA - Target	MST CSF 1.1 Cyber- Security Function	Last updated by / Date of last update	Last update / Date of last update	Implementation / Umsetzungsempfehlungen																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
					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								Test zur Umsetzungsempfehlung																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
A.5.1	Richtlinien für die Informationssicherheit		Informationssicherheitsrichtlinien und Sammelrichtlinien festlegen, welche die Geschäftsziele, die Geschäftsleistung, die Geschäftsreputation, die Geschäftsbeziehungen, die Geschäftsinteressen und die Geschäftsrisiken berücksichtigen und die Geschäftsinteressen und die Geschäftsrisiken berücksichtigen.	Medium	F	1	4		P	2	4		P	3	4		Stärkung der konvergenzen, Eignung, Angemessenheit und Vollständigkeit der Leitung und Unterstützung der Informationssicherheit	Verfügbarkeit	Identifizierung																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															</

Der Aufbau und die Funktionen können wie folgt zusammengefasst werden:

- Basiert auf ISO 27001:2022 Annex A und Umsetzungsempfehlungen nach ISO 27002
- Die Bewertung ist in drei Gebiete, welche separate behandelt werden können, aufgeteilt:
  - "Grid operator area" Gebiet des Netzbetreibers
  - "Energy producer area" Gebiet für Energieproduktion und Energiespeicherung
  - "General IT area" Gebiet für die allgemeine IT, primär die Büro- bzw. Business-Bereiche, gilt eigentlich als Baseline für die gesamte OT/IT-Umgebung
- Der Anwender kann sein zugewiesenes Schutzniveau gemäss Strom VV wählen
- Die durch den Anwender definierten Prioritäten können definiert werden
- Die Anwendbarkeit SoA kann abgebildet werden
- Der aktuelle Stand der Maturität kann abgebildet werden (Self Assessment)
- Das Soll- bzw. Ziel-Maturitäten kann abgebildet werden
- Bei den "Kommentaren" können zu den einzelnen Checkpoints Kommentare eingetragen werden z.B. Begründung bei Nichtanwendbarkeit
- Die Umsetzungsempfehlungen nach ISO 27002 mit Zweck, Art und Ziel werden dargestellt
- Der Bezug zu den NIST CSF 1.1 Funktionen ist ersichtlich

### E.3.4 Grafische Auswertung in den "Graphics All Area"-Register



Bei den grafischen Auswertungen werden die IST- und Ziel-Maturitäten dargestellt. Diese Auswertung hilft dem Anwender einfacher zu erkennen, wo die grössten Unterschiede bei den verschiedenen Maturitäten liegen.



### E.3.5 Register "Assistance Information"

Im Register "Assistance Informationen" sind alle nötigen Erklärungen und Ausführungen zu den verschiedenen variablen Punkten im Register "Assessment Tool ISO 27001" aufgeführt.

### E.4 VSE Assessment-Tool ISO27001 ISMS-Goals incl. HoP-Mapping

Das VSE haben in Zusammenarbeit mit der Arbeitsgruppe zu Erhöhung der IKT-Resilienz ein Tool entwickelt, dass die Unternehmen und Organisationseinheiten in der Strombranche bei der Einführung des ISMS unterstützt. Dabei werden die 52 Goals zur erfolgreichen Implementierung behandelt.



In den Schulungen des VSE wird die Anwendung des Tools genau erläutert.



Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.

#### E.4.1 Ziel und Zweck

Das VSE Assessment-Tool ISO27001 ISMS-Goals incl. HoP-Mapping bietet den Mitgliedern des VSE Unterstützung bei der Stärkung der IKT-Resilienz. Das Tool unterstützt den Anwender bei der Implementierung des ISMS im Unternehmen oder in den Organisationseinheiten. Darüber hinaus ermöglicht das Tool die Zuweisung einzelner Punkte zum HoP des IMS.



Die ausführlichen Kommentare helfen dem Anwender mit nützlichen zusätzlichen Informationen.

#### E.4.2 Register "Dokument Owner & History"

Im Abschnitt "Dokument Owner & History" werden relevante Angaben zu den Unternehmen oder Organisationseinheiten gemacht. Darüber hinaus können Informationen zur präzisen Identifizierung, Überarbeitung, Klassifizierung, Geltungsbereich und Historie des Dokuments bereitgestellt werden.

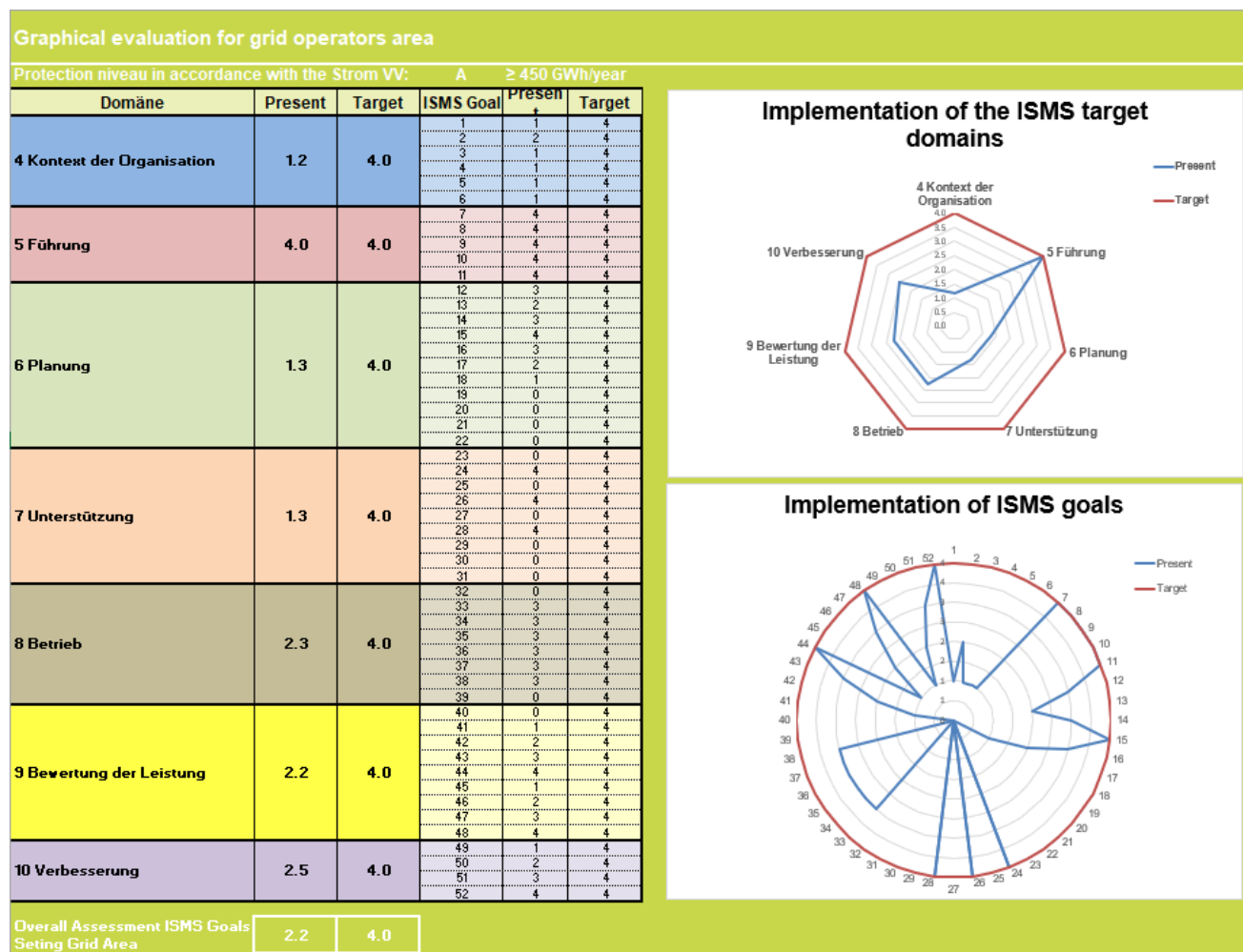
#### E.4.3 Register "Assessment ISMS Goals"

VSE Assessment Tool ISO27001 ISMS Goals				Organisation protection niveau according to BPE:				Company: Strom AG				Mapping to ISO Documents (When needs to be proved, not actual) - Choose the link																	
This tool may only be used if a valid license for ISO 27001/27002 is available. incl. VSE HoP-Mapping				Grid operator area: A 3-450 GWh/year Energy producer area: B 3-100 MW and 4-900 MW				Area of validity: Entire Strom AG Group with subsidiaries Status: In Progress																					
Sachverhalte Prozesse Strukturen Systeme		Kapital Kapital Kapital Kapital		Requisiten / Controls Anforderung / Requisites Eigenschaft / Constraints Requisit / Controls		Goal		Priority Priority Priority		Grid operator area		Energy producer area		General IT area (Baseline)		Normen / Standards													
										Present Target		Present Target		Present Target		ISO 27001 ISO 27001 ISO 27001													
4 Kontext der Organisation				1.1 Verstehen der Organisation und ihres Kontextes		Die Organisation muss externe und interne Themen bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informations-sicherheitsmanagementsystems zu erreichen. <b>ANMERKUNG:</b> Die Bestimmung dieser Aspekte April ist auf die Ermittlung der externen und internen Kontexte der Organisation, die in Absatz 4.1 der ISO 38000:2020 (Definition 4.1) definiert ist.		1 Low		1 4		2 3		1 4		6.1		IDR-2											
				1.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien		Die Organisation muss <b>ANMERKUNG:</b> Die Anforderungen der Interessierten Parteien können sich aufgrund sich verändernder Anforderungen (z.B. gesetzlicher Anforderungen) über die verfügbare Verfügbarkeit hinaus ändern. Die Organisation muss die Grenzen und die Anwendbarkeit des Informations-sicherheitsmanagementsystems bestimmen, um dessen Anwendungsbereich festzulegen.		2 Low		2 4		3 3		1 4		6.2 6.3 6.3													
				1.3 Festlegen des Anwendungsbereichs des Informations-sicherheitsmanagementsystems		Bei der Festlegung des Anwendungsbereichs muss die Organisation sicherstellen, dass der Anwendungsbereich sowohl die dokumentierte Information verfügbar sein, als auch die Organisation selbst, die die Information verarbeitet, umfasst. Der Anwendungsbereich muss die dokumentierte Information verfügbar sein.		3 High		3 4		2 3		1 4		6.3 6.3 6.3													
				1.4 Informations-sicherheitsmanagementsystem		Die Organisation muss entsprechend den Anforderungen dieses Dokuments ein Informations-sicherheitsmanagementsystem aufbauen, umsetzen, aufrechterhalten und fortlaufend verbessern, einschließlich der erforderlichen Prozesse und ihrer Verantwortlichkeiten.		4 High		4 4		2 3		1 3		6.3 6.4													
				4 Kontext der Organisation Subtotal				6 High		1 4		2 3		1 3		6.4													
								1.2 4.0		2.0 3.0		2.0 3.0		2.0 3.0															
5 Führung				5.1 Führung und Verpflichtung		a) sicherstellen, dass die Informations-sicherheitspolitik und die Informations-sicherheitsziele festgelegt sind und mit der strategischen Ausrichtung der Organisation vereinbar sind, b) sicherstellen, dass die Anforderungen des Informations-sicherheitsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden, c) sicherstellen, dass die für das Informations-sicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen, d) überlegen, wie ein wirksames Informations-sicherheitsmanagementsystem sowie die Vollständigkeit der Erfüllung der Anforderungen des Informations-sicherheitsmanagementsystems verhindert, e) sicherstellen, dass das Informations-sicherheitsmanagementsystem sein beabsichtigtes Ergebnis liefert, seine beabsichtigten Ergebnisse erfüllt, f) überlegen, wie und wie oft das Informations-sicherheitsmanagementsystem überprüft werden soll, um sicherzustellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, g) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, h) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, i) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, j) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, k) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, l) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, m) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, n) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, o) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, p) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, q) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, r) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, s) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, t) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, u) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, v) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, w) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, x) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, y) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt, z) sicherstellen, dass das Informations-sicherheitsmanagementsystem seine beabsichtigten Ergebnisse erfüllt.		7 Low		4 4		0 4		0 4		0 4		5.1 5											



- Die Bewertung ist in drei Gebiete, welche separate behandelt werden können, aufgeteilt:
  - "Grid operator area" Gebiet des Netzbetreibers
  - "Energy producer area" Gebiet für Energieproduktion und Energiespeicherung
  - "General IT area" Gebiet für die allgemeine IT, primär die Büro- bzw. Business-Bereiche, gilt eigentlich als Baseline für die gesamte OT/IT-Umgebung
- Der Anwender kann sein zugewiesenes Schutzniveau gemäss Strom VV wählen
- Der aktuelle Stand der Maturität kann abgebildet werden (Self Assessment)
- Das Soll- bzw. Ziel-Maturitäten kann abgebildet werden
- Bei den "Kommentaren" können zu den einzelnen Goals-Kommentare eingetragen werden z.B. weiterführende Informationen
- Der Bezug auf die ISO 27001 Kapitel und Referenzen sind aufgeführt
- Der Bezug zu den NIST CSF 1.1 Funktionen ist ersichtlich
- Die Zuweisung zu den IMS-HoP-Dokumenten kann gemacht werden.

#### E.4.4 Grafische Auswertung in den "Graphics ISMS Goals"-Register



Bei den grafischen Auswertungen werden die IST- und Ziel-Maturitäten dargestellt. Diese Auswertung hilft dem Anwender einfacher zu erkennen, wo die grössten Unterschiede bei den verschiedenen Maturitäten liegen. Die Auswertung ist für alle drei Register "Grid", "Producer" und "IT-General" ausgeführt.

#### E.4.5 Register "Assistance Information"

Im Register "Assistance Informationen" sind alle nötigen Erklärungen und Ausführungen zu den verschiedenen variablen Punkten im Register "Assessment ISMS Goals" aufgeführt.



## E.5 VSE-Tool ISO27001 Annex A HoP-Mapping

Das "VSE-Tool ISO27001 Annex A HoP-Mapping" hilft dem Anwender bei der Erstellung der HoP-Dokumente. In diesem Tool werden die einzelnen Checkpoints von ISO 27001:2022 Annex A den entsprechenden Dokumenten im HoP zugewiesen. Dies hilft dem Anwender anschliessend auch beim den Nachweisen.



**Tools, Frameworks, Normen, Standards, Guidelines und Publikationen benötigen sehr oft eine Lizenz zur Nutzung und Anwendung. Somit dürfen diese nur von Unternehmen und Organisationseinheiten verwendet werden, wenn eine gültige Lizenz vorliegt. Dies gilt insbesondere für SNV, ISO, ISA, EN, DIN, IEEE.**

### E.5.1 Register "Dokument Owner & History"

Im Abschnitt "Dokument Owner & History" werden relevante Angaben zu den Unternehmen oder Organisationseinheiten gemacht. Darüber hinaus können Informationen zur präzisen Identifizierung, Überarbeitung, Klassifizierung, Geltungsbereich und Historie des Dokuments bereitgestellt werden.

### E.5.2 Register "All Function HoP"

[illegible]

Die einzelnen Checkpoints gemäss ISO 27001:2022 Annex A können den HoP-Dokumenten zugewiesen werden.

## E.6 VSE-Tool IMS HoP-Dokumentenverzeichnis

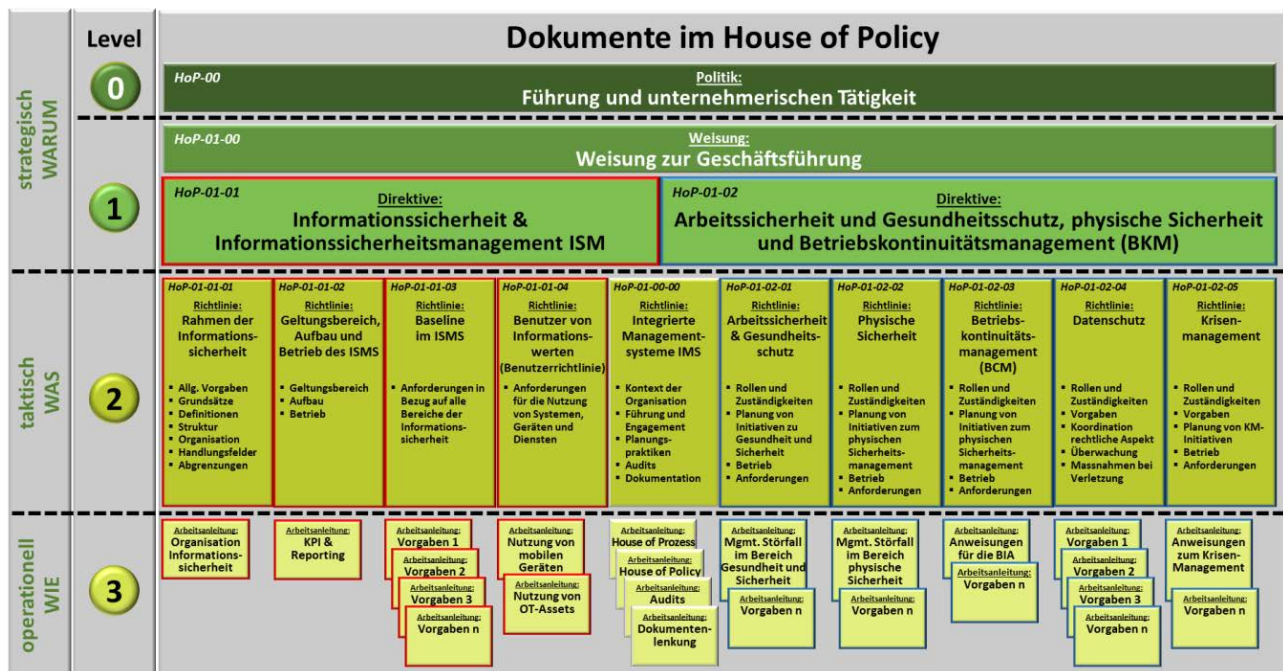
[illegible]

Im VSE-Tool IMS HoP-Dokumentenverzeichnis werden die nötigen Dokumente im IMS-HoP aufgelistet. Dabei werden alle HoP-Dokument aufgeführt, welche zu einem vollumfänglichen Betrieb eines ISMS benötigt werden. Mit diesem Toll kann der Stand der HoP-Dokumente abgebildet werden.



## Anhang F: Beschreibung der Vorgaben im House of Policy Level 0 bis 3

(1) In diesem Anhang sind die Vorgaben gemäss den House of Policy Level 0 bis 3 abgebildet:



### F.0 House of Policy auf Level 0: Politik (Verwaltungsrat / Konzernleitung)

Titel	Inhaltsbeschreibung
<b>HoP-00 Politik zur Führung und unternehmerischen Tätigkeit</b>	Die Politik zur Führung und unternehmerischen Tätigkeit ist ein prägnantes und autoritäres Dokument, das typischerweise vom Verwaltungsrat bzw. der höchsten Ebene eines Unternehmens herausgegeben wird. Es bietet spezifische Vorgaben oder Anweisungen an die Geschäftsleitung des Unternehmens auf wichtige strategische Grundsätze, Entscheidungen, Richtlinien oder Massnahmen, die mit der Vision des Vorstands und der Unternehmensführung in Einklang stehen. Diese Anweisungen konzentrieren sich in der Regel auf die Unternehmensführung, unternehmensweite Angelegenheiten, Compliance, Risikomanagement und grosse Unternehmensinitiativen. Sie dienen als Mittel zur Kommunikation der strategischen Erwartungen und Ziele des Vorstandes an das Führungsteam. Es müssen strategische Vorgaben betreffend Informationssicherheit im Unternehmen und in den Organisationseinheiten gemacht werden. Somit bekennt sich der Verwaltungsrat klar zur Informationssicherheit im Unternehmen und in den Organisationseinheiten.

### F.1 House of Policy auf Level 1: Weisungen und Direktiven (Geschäftsleitung, C-Level)

Titel	Inhaltsbeschreibung
<b>HoP-01-00 Weisung zur Geschäftsführung</b>	Die Weisung zur Geschäftsführung ist ein prägnantes und autoritäres Dokument, vom Geschäftsführer CEO eines Unternehmens herausgegeben wird. Es bietet spezifische Anleitungen oder Anweisungen an das Unternehmen und die Organisationseinheiten in Bezug auf wichtige strategische Entscheidungen, Richtlinien oder Massnahmen, die mit der Vision der höchsten Führungsebene bzw. in Einklang stehen. Sie beschreibt die Umsetzung der Vorgaben in der Politik der Geschäftsführung. Sie konzentriert sich in der Regel auf unternehmensweite Angelegenheiten, Compliance, Risikomanagement und grosse Unternehmensinitiativen. Sie dienen als Mittel zur Kommunikation der strategischen Erwartungen und Ziele des Vorstands an das Führungsteam. Es muss vom CEO eine klare Vorgabe zur Informationssicherheit im Unternehmen und in den Organisationseinheiten gemacht werden. Diese muss im Einklang mit den gesetzlichen und regulatorischen Vorgaben und der Politik der Geschäftsführung stehen.
<b>HoP-01-01 Direktive zur Informationssicherheit &amp; Informationssicherheitsmanagement ISM</b>	Die Direktive zur Informationssicherheit und zum Informationssicherheitsmanagement (ISM) legt die grundlegenden strategischen Ziele und Prinzipien für den Schutz von Informationen in einer Organisation fest. Sie definiert den Rahmen für die Umsetzung von Sicherheitsmassnahmen und die Einrichtung eines ISM-Systems. Die Direktive betont die Bedeutung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie die Notwendigkeit einer proaktiven Risikobewertung. Sie legt auch die Verantwortlichkeiten der Mitarbeiter fest und unterstreicht die kontinuierliche Verbesserung der Informationssicherheit als integralen Bestandteil der



Titel	Inhaltsbeschreibung
	Unternehmenskultur. Mindestens muss in dieser direktive der Verweisung und die Behandlung der Informationssicherheit mit den dazugehörnden Informationsmanagementsystem (IMS), das Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 und die anzuwendenden Rahmenwerke wie NIST Cyber Security Framework CSF aufgeführt werden.
<b>HoP-01-02 Direk- tive für die Ar- beitssicherheit und Gesundheits- schutz, physische Sicherheit und Be- triebskontinuitäts- management (BKM)</b>	Die Direktive für Arbeitssicherheit und Gesundheitsschutz, physische Sicherheit und Betriebskontinuitätsmanagement (BCM) etabliert klare Vorgaben zur Gewährleistung eines sicheren und ge- sunden Arbeitsumfelds sowie zur physischen Sicherheit unserer Organisation. Das Hauptziel besteht darin, die Gesundheit und Sicherheit aller Mitarbeiter zu schützen und die Fortführung betrieblicher Abläufe sicherzustellen. Die Geschäftsleitung übernimmt die Verantwortung für die Festlegung von Standards und Richtlinien, um sicherzustellen, dass alle Arbeitnehmer in einem sicheren und gesunden Umfeld arbeiten. Dies schliesst die Identifizierung, Bewertung und Mini- mierung von Gefahren und Risiken am Arbeitsplatz ein. Im Bereich der physischen Sicherheit werden klare Anweisungen bezüglich des Schutzes von Ressourcen, Einrichtungen und sensiblen Informationen gegeben. Massnahmen zur Zugangskontrolle, Überwachung und Notfallvorsorge werden festgelegt, um unbefugten Zugang und potenzielle Bedrohungen zu minimieren. Das Be- triebskontinuitätsmanagement (BCM) ist integraler Bestandteil dieser Direktive. Es legt Prozesse und Verfahren fest, um sicherzustellen, dass im Falle von Störungen oder Katastrophen die be- trieblichen Abläufe so schnell wie möglich wiederhergestellt werden können. Dies umfasst auch die regelmässige Überprüfung und Aktualisierung von Notfallplänen sowie Schulungen für Mitar- beiter, um eine effektive Reaktion im Ernstfall zu gewährleisten. Die Einhaltung dieser Direktive ist für alle Mitarbeiter verbindlich, und die Geschäftsleitung behält sich das Recht vor, bei Nicht- einhaltung angemessene disziplinarische Massnahmen zu ergreifen.
<b>HoP-01-03 Direk- tive für das Risiko- management</b>	Die Direktive für das Risikomanagement bildet das grundlegende Dokument, das die strategischen Ziele, Prinzipien und den Rahmen für den Umgang mit Risiken im Unternehmen und in den Orga- nisationseinheiten festlegt. Sie gibt die Leitlinien vor, wie Risiken identifiziert, bewertet und behan- delt werden sollen, um die Geschäftsziele zu schützen, die Compliance zu gewährleisten und eine effektive Risikokultur zu etablieren.

## F.2 House of Policy auf Level 2: Richtlinien und Guidelines (CISO, CRO, DPO)

Titel	Beschreibung
<b>HoP-01-00-00 Richtlinie Inte- grierte Manage- ment Systeme IMS</b>	Die Richtlinie für Integrierte Management Systeme (IMS) definiert die strategischen Ziele und Grundsätze für die Implementierung und den Betrieb eines IMS in einer Organisation. Sie legt den Rahmen für die Integration verschiedener Managementsysteme fest, einschliesslich Qualität, Umwelt, Gesundheit und Sicherheit, und bietet klare Leitlinien zur Harmonisierung von Prozessen und Verfahren. Die Richtlinie zielt darauf ab, die Effizienz zu steigern, Syner- gien zu schaffen und die Gesamtleistung des Unternehmens und der Organisationseinheiten zu verbessern.
<b>HoP-01-01-01 Richtlinie Bereich Informationssi- cherheit &amp; Infor- mationssicherheit smanagement ISM: Rahmen der Infor- mationssicherheit</b>	Die Richtlinie zur Definition des Rahmens zur Informationssicherheit skizziert grundlegende Vorgaben, Prinzipien, Handlungsfelder und Standards, um einen klaren und kohärenten Rah- men für die Informationssicherheit im Unternehmen und in den Organisationseinheiten zu schaffen. Ihr Hauptziel besteht darin, klare Leitlinien zu etablieren, die den Umfang und die Grundlagen für die Entwicklung und Implementierung des Information Security Management Systems (ISMS) vorgeben. Die Richtlinie betont die Wichtigkeit einer umfassenden Kon- textanalyse, bei der die geschäftlichen Ziele, externen Einflüsse und die Art der verarbeiteten Informationen berücksichtigt werden. Auf dieser Basis erfolgt die Festlegung des Anwen- dungsbereichs des ISMS und die Identifikation der relevanten rechtlichen, regulatorischen und geschäftlichen Anforderungen. Es werden klare Verantwortlichkeiten für die Umsetzung und Aufrechterhaltung des ISMS auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Zuweisung von Rollen und Verantwortlichkeiten für die Informationssicherheit ein, um sicherzustellen, dass alle relevanten Stakeholder angemessen eingebunden sind. Die Einhaltung dieser Richtlinie ist für alle Mitarbeiter verbindlich, und die Geschäftsleitung behält sich das Recht vor, bei Nichteinhaltung angemessene Massnahmen zu ergreifen.
<b>HoP-01-01-02: Richtlinie Bereich Informationssi- cherheit: Gel- tungsbereich, Aufbau und Orga- nisation des ISMS</b>	Die Richtlinie für den Geltungsbereich, Aufbau und die Organisation des Information Security Management Systems (ISMS) legt grundlegende Prinzipien und Standards fest, um einen klaren Rahmen für die Implementierung und Strukturierung des ISMS in unserer Organisation zu schaffen. Ihr Hauptziel besteht darin, klare Leitlinien zu etablieren, die den Umfang des ISMS, seine Struktur und die Verantwortlichkeiten für die Informationssicherheit definieren. Die Richtlinie betont die Bedeutung einer gründlichen Analyse des organisatorischen Kontex- tes, um den Anwendungsbereich des ISMS genau zu bestimmen. Dies beinhaltet die Identi- fikation von internen und externen Faktoren, die die Informationssicherheit beeinflussen könnten, sowie die Festlegung der Geschäftsbereiche, auf die sich das ISMS konzentriert. Es werden klare Verantwortlichkeiten und Rollen für den Aufbau und die Aufrechterhaltung des ISMS auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Festlegung von Sicherheitsbeauftragten und die Zuweisung spezifischer Aufgaben im Zusammenhang mit der Informationssicherheit ein.



Titel	Beschreibung
<b>HoP-01-01-03</b> <b>Richtlinie Bereich Informationssicherheitsmanagement ISM: Baseline im ISMS</b>	<p>Die Richtlinie Baseline Informationssicherheit im Information Security Management System (ISMS) Baseline skizziert klare und grundlegende Standards, die als Ausgangspunkt für die Implementierung und Aufrechterhaltung unseres ISMS dienen. Das Hauptziel besteht darin, einen einheitlichen und stabilen Rahmen für die Informationssicherheit in der gesamten Organisation zu schaffen. Die Richtlinie betont die Bedeutung der Identifizierung und Implementierung von Baseline-Sicherheitskontrollen, die als Mindestanforderungen gelten, um ein angemessenes Mass an Informationssicherheit zu gewährleisten. Dabei werden grundlegende Prinzipien wie Vertraulichkeit, Integrität und Verfügbarkeit von Informationen berücksichtigt. Die Baseline dient als Referenzpunkt für alle Bereiche der Organisation und legt klare Anforderungen für den Umgang mit sensiblen Informationen fest. Dies schliesst den Zugriff auf Daten, den Schutz vor Malware, die Sicherung von Netzwerken und die Verwaltung von Zugriffsrechten ein. Die Richtlinie unterstreicht auch die Notwendigkeit regelmässiger Überprüfungen und Aktualisierungen der Baseline, um sicherzustellen, dass sie den sich ändernden Bedrohungen und Anforderungen an die Informationssicherheit gerecht wird. Die Kommunikation und Schulung der Mitarbeiter über die Baseline-Standards sind ebenfalls wesentliche Bestandteile, um ein gemeinsames Verständnis und Bewusstsein für Sicherheitsanforderungen zu schaffen.</p>
<b>HoP-01-01-04:</b> <b>Richtlinie Bereich Informationssicherheit: Benutzer von Informationswerten</b>	<p>Die Richtlinie für Nutzer und Benutzer im Rahmen eines Information Security Management Systems (ISMS) legt klare Leitlinien und Verhaltensstandards für alle Mitarbeiter fest, um einen sicheren Umgang mit Informationen zu gewährleisten. Ihr Hauptziel besteht darin, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu schützen und gleichzeitig das Bewusstsein der Mitarbeiter für Sicherheitsaspekte zu fördern. Die Richtlinie betont die individuelle Verantwortung jedes Benutzers im Schutz sensibler Informationen und legt klare Erwartungen hinsichtlich der Einhaltung sicherheitsrelevanter Richtlinien und Verfahren fest. Die sichere Handhabung von Benutzerkonten, Passwörtern und Zugriffsberechtigungen ist dabei ein zentraler Bestandteil. Es wird darauf hingewiesen, dass Mitarbeiter vertrauliche Zugangsdaten sorgfältig behandeln müssen und keine unbefugten Informationen preisgeben dürfen. Gleichzeitig werden Schulungsmassnahmen eingeführt, um sicherzustellen, dass die Mitarbeiter über die neuesten Sicherheitspraktiken informiert sind und in der Lage sind, Phishing-Angriffe zu erkennen.</p>
<b>HoP-01-02-01:</b> <b>Richtlinie Bereich AGSB: Arbeitssicherheit &amp; Gesundheitsschutz</b>	<p>Die Richtlinie für Arbeitssicherheit und Gesundheitsschutz legt die grundlegenden Prinzipien und Standards fest, um ein sicheres und gesundes Arbeitsumfeld in unserer Organisation zu gewährleisten. Das Hauptziel dieser Richtlinie besteht darin, klare Anweisungen und Leitlinien zu geben, um potentielle Risiken am Arbeitsplatz zu minimieren und die Gesundheit sowie das Wohlbefinden der Mitarbeiter zu schützen. Die Richtlinie betont die Wichtigkeit einer kontinuierlichen Identifikation und Bewertung von Arbeitsplatzrisiken sowie der Implementierung von präventiven Massnahmen. Dabei wird darauf abgezielt, Arbeitsunfälle zu verhindern, die Gesundheit der Mitarbeiter zu fördern und die Einhaltung relevanter Vorschriften sicherzustellen. Es werden klare Verantwortlichkeiten für die Umsetzung von Sicherheitsstandards auf allen Ebenen der Organisation definiert. Die Organisation setzt klare Erwartungen hinsichtlich der Schulung der Mitarbeiter, um ein Bewusstsein für Sicherheitsrisiken zu schaffen und deren aktive Mitwirkung an Sicherheitsmassnahmen zu fördern.</p>
<b>HoP-01-02-02:</b> <b>Richtlinie Bereich AGSB: Physische Sicherheit</b>	<p>Die Richtlinie für physische Sicherheit legt die grundlegenden Prinzipien und Standards fest, um die physische Integrität unserer Ressourcen, Einrichtungen und sensiblen Informationen zu schützen. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um physische Bedrohungen zu minimieren und eine sichere Umgebung für unsere Mitarbeiter und Vermögenswerte zu gewährleisten. Die Richtlinie betont die Wichtigkeit einer umfassenden Risikobewertung, die die Identifikation potentieller Gefahren für physische Sicherheit einschliesst. Dabei wird darauf abgezielt, Massnahmen zu entwickeln, um Einbrüche, Diebstähle, Naturkatastrophen und andere physische Bedrohungen zu verhindern oder zu minimieren. Es werden klare Verantwortlichkeiten für die Umsetzung von physischen Sicherheitsstandards auf allen Ebenen der Organisation definiert. Dies schliesst die Zugangskontrolle, Überwachungssysteme und Notfallvorsorge ein, um sicherzustellen, dass unsere Einrichtungen angemessen geschützt sind.</p>
<b>HoP-01-02-03:</b> <b>Richtlinie Bereich AGSB: Betriebskontinuitätsmanagement (BCM)</b>	<p>Die Richtlinie zum Betriebskontinuitätsmanagement (BCM) etabliert die grundlegenden Prinzipien und Standards, um sicherzustellen, dass unsere Organisation in der Lage ist, auch unter widrigen Bedingungen ihre kritischen Geschäftsprozesse aufrechtzuerhalten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um Störungen und Unterbrechungen unserer betrieblichen Abläufe zu minimieren und im Notfall eine rasche Wiederherstellung zu ermöglichen. Die Richtlinie betont die Wichtigkeit einer umfassenden Risikobewertung, um potenzielle Bedrohungen und Schwachstellen zu identifizieren, die die Betriebskontinuität beeinträchtigen könnten. Dabei wird darauf abgezielt, Strategien und Massnahmen zu entwickeln, um diese Risiken zu minimieren und einen kontinuierlichen Geschäftsbetrieb sicherzustellen. Es werden klare Verantwortlichkeiten für die Umsetzung von BCM-Standards auf allen Ebenen der Organisation definiert. Dies schliesst die Entwicklung von Notfallplänen, Schulungen der Mitarbeiter und regelmässige Notfallübungen ein, um sicherzustellen, dass das Personal effektiv auf verschiedene Szenarien reagieren kann.</p>
<b>HoP-01-02-04:</b>	<p>Die Datenschutzrichtlinie legt die grundlegenden Prinzipien und Standards fest, um sicherzustellen, dass personenbezogene Daten in unserer Organisation gemäss den</p>





Titel	Beschreibung
<b>Richtlinie Bereich AGSB: Datenschutz</b>	Datenschutzbestimmungen geschützt werden. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten zu gewährleisten und gleichzeitig die Rechte und Privatsphäre der betroffenen Personen zu respektieren. Die Richtlinie betont die Wichtigkeit einer sorgfältigen Verarbeitung personenbezogener Daten, beginnend mit ihrer Erhebung bis hin zur Speicherung und Löschung. Dabei wird darauf abgezielt, sicherzustellen, dass nur autorisierte Personen Zugriff auf diese Daten haben und dass angemessene Sicherheitsmassnahmen implementiert sind, um unbefugten Zugriff oder Datenverlust zu verhindern. Es werden klare Verantwortlichkeiten für die Umsetzung von Datenschutzstandards auf allen Ebenen der Organisation definiert. Dies schliesst die Schulung der Mitarbeiter ein, um ein Bewusstsein für Datenschutzpraktiken zu schaffen, und die Bereitstellung von Mechanismen, um die Einhaltung von Datenschutzrechten der betroffenen Personen sicherzustellen. Die Richtlinie muss auch das Management von Vorfällen mit personenbezogenen Daten beschreiben und legt klare Prinzipien und Standards fest, um sicherzustellen, dass alle möglichen Vorfälle im Zusammenhang mit personenbezogenen Daten innerhalb unserer Organisation effektiv und angemessen behandelt werden. Ihr Ziel besteht auch darin, klare Leitlinien zu schaffen, um auf Datenschutzverletzungen oder Sicherheitsvorfälle umgehend zu reagieren, die Vertraulichkeit und Integrität personenbezogener Daten zu bewahren und rechtliche Anforderungen zu erfüllen. Die Richtlinie betont die Wichtigkeit einer raschen Identifikation, Meldung und Analyse von Datenschutzvorfällen. Dabei wird darauf abgezielt, potenzielle Auswirkungen auf betroffene Personen und die Organisation zu minimieren und gleichzeitig die Transparenz in Bezug auf Sicherheitsvorfälle zu gewährleisten. Es werden klare Verantwortlichkeiten für das Incident Management auf allen Ebenen der Organisation definiert. Dies umfasst die Einrichtung eines Incident-Response-Teams, das für die koordinierte Bewältigung von Datenschutzvorfällen verantwortlich ist. Gleichzeitig legt die Richtlinie Massnahmen fest, um betroffene Personen, Aufsichtsbehörden und andere relevante Parteien zeitnah zu informieren.
<b>HoP-01-02-05: Richtlinie Bereich AGSB: Notfallmanagement</b>	Die Richtlinie für Notfallmanagement skizziert die grundlegenden Prinzipien und Standards, um einen strukturierten und effektiven Ansatz zur Bewältigung von Krisensituationen in unserer Organisation sicherzustellen. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um eine umgehende und koordinierte Reaktion auf unvorhergesehene Ereignisse zu gewährleisten, die die Geschäftskontinuität und den Ruf der Organisation beeinträchtigen könnten. Die Richtlinie betont die Notwendigkeit einer proaktiven Risikoanalyse, um potenzielle Krisenszenarien zu identifizieren. Dabei wird darauf abgezielt, klare Verantwortlichkeiten für das Notfallmanagement festzulegen und die Ressourcen zu identifizieren, die im Krisenfall mobilisiert werden können. Es werden klare Kommunikationsstrukturen und -verantwortlichkeiten definiert, um sicherzustellen, dass alle relevanten Parteien angemessen informiert sind. Gleichzeitig wird die Einrichtung eines Notfallmanagement-Teams betont, das für die Koordinierung und Umsetzung der Krisenreaktion verantwortlich ist. Die Einhaltung dieser Richtlinie ist für alle Mitarbeiter verbindlich, und die Geschäftsleitung behält sich das Recht vor, bei Nichteinhaltung angemessene Massnahmen zu ergreifen.

### F.3 House of Policy auf Level 3: Arbeitsanleitungen und Instructions (ISO, ISC und Cyber Security Team)

Titel	Beschreibung
<b>HoP-01-00-00-01 Arbeitsanleitung zu Bereich IMS: House of Prozess</b>	<p>Die Arbeitsanleitung für den Bereich Integrierte Management Systeme (IMS) im Kontext des "House of Process" bietet eine umfassende Anleitung für die Prozessgestaltung und -optimierung innerhalb eines IMS. Das "House of Process" ist ein Konzept, das die verschiedenen Aspekte der Prozesslandschaft in einer Organisation strukturiert und integriert.</p> <p>Im Geltungsbereich dieser Arbeitsanleitung wird klar definiert, welche Prozesse, Abteilungen und Aktivitäten innerhalb des IMS berücksichtigt werden. Dies schafft eine klare Ausgangsbasis für die Prozessoptimierung. Der Aufbau des "House of Process" wird im Detail erläutert, einschliesslich der Hierarchie der Prozesse, Unterprozesse und Aktivitäten. Hierbei werden Schnittstellen zwischen den einzelnen Prozessbereichen identifiziert und beschrieben.</p> <p>Die Arbeitsanleitung gibt klare Anweisungen zur Gestaltung der Prozesse innerhalb des "House of Process". Dies umfasst die Definition von Prozesszielen, die Festlegung von Verantwortlichkeiten und Befugnissen, sowie die Implementierung von Massnahmen zur Prozessüberwachung und -steuerung. Auch die Integration von Qualitätsstandards und die Anwendung von Best Practices werden in der Anleitung berücksichtigt.</p> <p>Ein wesentlicher Bestandteil der Arbeitsanleitung ist die Anleitung zur kontinuierlichen Verbesserung der Prozesse. Dies beinhaltet die regelmässige Überprüfung und Aktualisierung der Prozesslandschaft, um auf sich ändernde Anforderungen und Geschäftsbedingungen reagieren zu können. Die Anleitung enthält auch klare Schritte für Audits und Überprüfungen, um die Effektivität der Prozesse sicherzustellen.</p> <p>Insgesamt bietet die Arbeitsanleitung für den Bereich IMS: House of Process eine umfassende Orientierung für die erfolgreiche Gestaltung, Umsetzung und kontinuierliche Verbesserung von Prozessen innerhalb eines Integrierten Management Systems.</p>



Titel	Beschreibung
<b>HoP-01-00-00-02</b> <b>Arbeitsanleitung</b> <b>zu Bereich IMS:</b> <b>House of Policy</b>	<p>Die Arbeitsanleitung für den Bereich IMS: House of Policy bietet eine umfassende Orientierung für die Gestaltung, Implementierung und Aufrechterhaltung von Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen innerhalb eines Integrierten Management Systems (IMS). Hierbei bezieht sich der "House of Policy" auf die Struktur und Verwaltung von Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen in einer Organisation.</p> <p>Die Arbeitsanleitung beginnt mit der klaren Definition des Geltungsbereichs, um festzulegen, welche Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen innerhalb des IMS berücksichtigt werden. Dies schafft eine klare Ausgangsbasis für die Erstellung und Verwaltung von Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen. Die Struktur des "House of Policy" wird im Detail erläutert. Dies umfasst die Hierarchie der Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen, die Identifizierung von Schlüssel-Politiken, -Direktiven, -Richtlinien, -Guidelines und -Arbeitsanleitungen sowie deren Zusammenhang und Abhängigkeiten. Die Anleitung gibt klare Anweisungen zur Kategorisierung und Organisation von Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen, um eine übersichtliche und effektive Verwaltung sicherzustellen. Die Arbeitsanleitung gibt detaillierte Schritte zur Erstellung von Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen vor. Dies beinhaltet die Festlegung von klaren Zielen, Verantwortlichkeiten, Anwendungsbereichen und Umsetzungsdetails. Auch die Integration von rechtlichen Anforderungen, Normen und Best Practices wird berücksichtigt. Die Anleitung enthält klare Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen zur Implementierung von Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen in der Organisation. Dies schliesst Schulungen, Bewusstseinsbildung und Kommunikationsstrategien ein, um sicherzustellen, dass alle relevanten Stakeholder die Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen verstehen und befolgen. Ein wesentlicher Bestandteil der Arbeitsanleitung ist die Anleitung zur regelmässigen Überprüfung und Aktualisierung der Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen. Dies gewährleistet, dass die Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen an sich ändernde Anforderungen und externe Faktoren angepasst werden können. Die Anleitung gibt klare Vorgaben für die Dokumentation und Aufbewahrung von Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen vor. Dies schliesst die Festlegung von Verantwortlichkeiten für die Pflege der Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen sowie den Zugriff und die Verfügbarkeit für relevante Parteien ein. Insgesamt bietet die Arbeitsanleitung für den Bereich IMS: House of Policy eine umfassende und praxisnahe Anleitung für die effektive Erstellung, Umsetzung und Pflege von Politiken, Direktiven, Richtlinien, Guidelines und Arbeitsanleitungen innerhalb eines Integrierten Management Systems.</p>
<b>HoP-01-00-00-03</b> <b>Arbeitsanleitung</b> <b>Bereich IMS: Do-</b> <b>kumentenlenkung</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für die Dokumentenlenkung legt die wesentlichen Schritte und Prinzipien fest, um sicherzustellen, dass alle relevanten Dokumente, die die Informationssicherheit betreffen, ordnungsgemäss erstellt, überprüft, genehmigt, aktualisiert und archiviert werden. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Integrität und Aktualität von sicherheitsrelevanten Dokumenten zu gewährleisten. Die Arbeitsanleitung betont die Notwendigkeit einer strukturierten Dokumentenlenkung, die sicherstellt, dass alle relevanten Informationen leicht zugänglich sind und dass die neuesten Versionen verwendet werden. Dies beinhaltet klare Prozesse für die Erstellung neuer Dokumente, Überprüfung durch kompetente Parteien, formale Genehmigung und die regelmässige Aktualisierung entsprechend den sich ändernden Anforderungen. Es werden klare Verantwortlichkeiten für die Umsetzung der Dokumentenlenkung auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Benennung von Verantwortlichen für die verschiedenen Phasen des Dokumentenlebenszyklus ein, um sicherzustellen, dass die festgelegten Verfahren konsequent eingehalten werden.</p>
<b>HoP-01-00-00-04</b> <b>Arbeitsanleitung</b> <b>Bereich IMS: Au-</b> <b>dings</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für Audits legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass Audits in Unternehmen und Organisationseinheiten effektiv, konsequent und zielgerichtet durchgeführt werden. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um sicherzustellen, dass alle relevanten Aspekte der Informationssicherheit regelmässig überprüft werden, um die Einhaltung von Standards und Richtlinien zu gewährleisten. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Audit-Richtlinie für Informationssicherheit. Dabei werden klare Prozesse für die Planung von Audits, die Identifizierung von zu überprüfenden Sicherheitskontrollen, die Durchführung von Audits sowie die Berichterstattung und Nachverfolgung von Ergebnissen definiert. Es werden klare Verantwortlichkeiten für die Umsetzung der Audit-Richtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Audit-Verantwortlichen, internen Auditoren und Ansprechpartnern in den jeweiligen Geschäftsbereichen ein. Schulungsmassnahmen sind ebenfalls vorgesehen, um sicherzustellen, dass Mitarbeiter die Bedeutung von Audits verstehen und bei Bedarf kooperativ mit den Prüfteams zusammenarbeiten.</p>
<b>HoP-01-01-01-01</b> <b>Arbeitsanleitung</b> <b>Bereich ISM: Infor-</b> <b>mationssicherheit</b> <b>Organisation</b>	<p>Die Arbeitsanleitung für den Bereich Informationssicherheit: Organisationstruktur beschreibt detailliert die strukturellen Aspekte, die notwendig sind, um eine effektive Informationssicherheit in einem Unternehmen und den Organisationseinheiten zu gewährleisten. Die Arbeitsanleitung beginnt mit der Festlegung des Geltungsbereichs, um zu definieren, welche Bereiche und Prozesse von den Sicherheitsmassnahmen abgedeckt werden. Dabei wird auch die Zielsetzung klar formuliert, um sicherzustellen, dass die Organisation ihre spezifischen Sicherheitsziele erreicht. Ein zentraler Bestandteil ist die Definition der Verantwortlichkeiten und Rollen im Kontext der Informationssicherheit. Das umfasst die Benennung von Sicherheitsverantwortlichen, Sicherheitsbeauftragten und anderen relevanten Rollen, um klare Zuständigkeiten zu schaffen. Die Anleitung legt</p>



Titel	Beschreibung
	<p>dar, wie die Aufgaben und Verantwortlichkeiten für Informationssicherheit in die bestehende Organisationsstruktur integriert werden. Dies beinhaltet die Zusammenarbeit mit anderen Abteilungen und die Schaffung einer klaren Hierarchie für Sicherheitsangelegenheiten. Die Anleitung beschreibt die Berichtswege und Kommunikationskanäle für sicherheitsrelevante Informationen innerhalb der Organisation. Dies sorgt für eine effektive Kommunikation zwischen den Sicherheitsverantwortlichen und anderen Mitarbeitern. Die Anleitung betont die Notwendigkeit von Schulungen und Sensibilisierungsmassnahmen bei Änderungen von Mitarbeiterrollen oder -verantwortlichkeiten. Dies ist besonders wichtig, um sicherzustellen, dass neue Aufgaben im Einklang mit den Sicherheitsrichtlinien wahrgenommen werden. Die Anleitung legt fest, wie Sicherheitsrichtlinien innerhalb des Unternehmens und der Organisationseinheiten durchgesetzt werden sollen. Dies kann die Integration von Sicherheitsrichtlinien in bestehende Arbeitsprozesse und -verfahren sowie die Implementierung von Kontrollmechanismen umfassen. Regelmässige Evaluierungen der Organisationsstruktur für Informationssicherheit sind vorgesehen. Dies ermöglicht eine kontinuierliche Anpassung an sich ändernde Bedrohungen und Anforderungen und stellt sicher, dass die Organisationsstruktur stets effektiv bleibt. Die Arbeitsanleitung für den Bereich Informationssicherheit: Organisationsstruktur fungiert als Leitfaden, um sicherzustellen, dass die organisatorischen Aspekte der Informationssicherheit klar definiert, integriert und durchgesetzt werden.</p>
<b>HoP-01-01-02-01</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b> <b>Key Performance</b> <b>Indicators (KPI)</b> <b>und Reporting</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für Key Performance Indicators (KPIs) definiert die wesentlichen Schritte und Prinzipien, um effektive Leistungskennzahlen zu entwickeln, zu implementieren und zu überwachen, die die Wirksamkeit des Informationssicherheitsmanagementsystems (ISMS) messen. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um aussagekräftige KPIs zu identifizieren, die die Zielerreichung und Leistung im Bereich der Informationssicherheit widerspiegeln. Die Arbeitsanleitung betont die Bedeutung einer umfassenden Analyse, um relevante KPIs zu identifizieren, die den Fortschritt gegenüber den definierten Sicherheitszielen und -standards quantifizieren können. Dies beinhaltet die Festlegung von klaren und messbaren Indikatoren, die die Leistung im Kontext der Informationssicherheit widerspiegeln. Es werden klare Verantwortlichkeiten für die Umsetzung und Überwachung der KPIs auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Zuweisung von Aufgaben an relevante Sicherheitsverantwortliche und die Festlegung von Prozessen für die regelmässige Bewertung und Aktualisierung der KPIs ein.</p>
<b>HoP-01-01-03-01</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b> <b>Grundschutz Infor-</b> <b>mationssicherheit</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für den Grundschutz, insbesondere in Bezug auf die Datensicherheit, legt grundlegende Schritte und Prinzipien fest, um eine angemessene Sicherung von Daten in den Unternehmen und Organisationseinheiten zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen und gleichzeitig die gesetzlichen Anforderungen und Compliance-Vorgaben zu erfüllen. Die Arbeitsanleitung betont die Bedeutung einer umfassenden Risikoanalyse im Hinblick auf Datensicherheit, um potenzielle Bedrohungen und Schwachstellen zu identifizieren. Dabei werden klare Prozesse für die Klassifizierung von Daten, den Zugriffsschutz, die Verschlüsselung und die regelmässige Überprüfung von Sicherheitsmassnahmen festgelegt. Es werden klare Verantwortlichkeiten für die Umsetzung der Datensicherheitsrichtlinien auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Schulung der Mitarbeiter ein, um ein Bewusstsein für den verantwortungsbewussten Umgang mit Daten zu schaffen, sowie die Implementierung von Mechanismen zur kontinuierlichen Überwachung und Verbesserung der Datensicherheitsmassnahmen.</p>
<b>HoP-01-01-03-02</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b> <b>IT-OT-Risiko-Ma-</b> <b>nagement</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für die Anwendung des IT-OT-Risiko-Managements legt die wesentlichen Schritte und Prinzipien fest, um sicherzustellen, dass Risiken im Zusammenhang mit der Integration von Informationstechnologie (IT) und Betriebstechnologie (OT) wirksam identifiziert, bewertet und gesteuert werden. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Sicherheit und Stabilität der kritischen Betriebsinfrastrukturen zu gewährleisten. Die Arbeitsanleitung betont die Notwendigkeit einer umfassenden Risikoanalyse, die die spezifischen Herausforderungen der Konvergenz von IT und OT berücksichtigt. Dabei werden klare Prozesse für die Identifikation von Risiken, die Bewertung ihrer Auswirkungen auf Geschäftsprozesse und die Entwicklung geeigneter Massnahmen zur Risikominderung festgelegt. Es werden klare Verantwortlichkeiten für die Umsetzung des IT-OT-Risiko-Managements auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Einrichtung eines Teams oder Ausschusses ein, dass für die koordinierte Umsetzung und Überwachung der Risikobehandlung verantwortlich ist.</p>
<b>HoP-01-01-03-03</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b> <b>Asset Manage-</b> <b>ment und Informa-</b> <b>tionsklassifizierung</b> <b>g</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für das Asset Management und die Informationsklassifizierung legt grundlegende Schritte und Prinzipien fest, um eine effektive Verwaltung von Vermögenswerten und die Klassifizierung von Informationen in Unternehmen und Organisationseinheiten sicherzustellen. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und Vermögenswerten zu gewährleisten. Die Arbeitsanleitung betont die Wichtigkeit einer systematischen Bestandsaufnahme und Verwaltung von Vermögenswerten, einschliesslich Hardware, Software und Informationen. Dabei werden klare Prozesse für die Identifikation, Klassifizierung und Überwachung von Vermögenswerten festgelegt, um sicherzustellen, dass diese angemessen geschützt sind. Des Weiteren wird auf die Bedeutung der Informationsklassifizierung hingewiesen, die es ermöglicht, Informationen entsprechend ihrem Wert und ihrer Sensitivität zu kategorisieren. Hierbei werden</p>



Titel	Beschreibung
	klare Richtlinien für die Klassifizierung, den Zugriff und die Handhabung von Informationen definiert, um sicherzustellen, dass angemessene Sicherheitsmassnahmen implementiert werden. Es werden klare Verantwortlichkeiten für die Umsetzung des Asset Managements und der Informationsklassifizierung auf verschiedenen Ebenen der Organisation definiert. Dies schliesst Schulungen für Mitarbeiter ein, um ein Bewusstsein für die Bedeutung der Asset-Verwaltung und Informationsklassifizierung zu schaffen, sowie Mechanismen zur kontinuierlichen Überwachung und Verbesserung dieser Prozesse.
<b>HoP-01-01-03-04 Arbeitsanleitung Bereich ISMS: Schulung und Sensibilisierung</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Schulung und Sensibilisierung legt grundlegende Schritte und Prinzipien fest, um sicherzustellen, dass Mitarbeiter in Unternehmen und Organisationseinheiten angemessen auf die Herausforderungen der Informationssicherheit vorbereitet sind. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um ein Bewusstsein für Sicherheitsrisiken zu schaffen, das notwendige Wissen zu vermitteln und sicherzustellen, dass Mitarbeiter verantwortungsbewusst mit Informationen umgehen. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Schulungsstrategie, die auf die spezifischen Bedürfnisse der Organisation zugeschnitten ist. Dies beinhaltet Schulungen zu Themen wie sicheres Passwortmanagement, Phishing-Prävention, Datenschutzbestimmungen und anderen relevanten Sicherheitsaspekten. Des Weiteren werden klare Verantwortlichkeiten für die Umsetzung von Schulungsmassnahmen auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Identifikation von Schlüsselpersonen für Schulungen, die Planung von Schulungsprogrammen und die regelmässige Überprüfung der Schulungseffektivität ein.
<b>HoP-01-01-03-05 Arbeitsanleitung Bereich ISMS: Physische Sicherheit der IKT-Assets</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für die physische Sicherheit der Informations- und Kommunikationstechnologie (IKT)-Assets legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass die physische Umgebung, in der IKT-Geräte und -Systeme betrieben werden, angemessen geschützt ist. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Verfügbarkeit, Integrität und Vertraulichkeit von IKT-Assets zu gewährleisten und gleichzeitig physische Risiken zu minimieren. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Risikoanalyse im Bereich physischer Sicherheit, die mögliche Bedrohungen wie unbefugten Zugriff, Diebstahl oder Naturkatastrophen berücksichtigt. Dabei werden klare Prozesse für den Zugang zu Räumlichkeiten, den Schutz von IKT-Geräten vor unbefugtem Zugriff und die Sicherstellung der Umgebung, in der sie betrieben werden, definiert. Es werden klare Verantwortlichkeiten für die Umsetzung der physischen Sicherheitsrichtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Sicherheitsbeauftragten, die Überwachung von Sicherheitsmassnahmen und die Schulung der Mitarbeiter in Bezug auf physische Sicherheitsrichtlinien ein.
<b>HoP-01-01-03-06 Arbeitsanleitung Bereich ISMS: Zugriffskontrolle</b>	Die Arbeitsanleitung im Bereich ISMS (Information Security Management System) für Zugriffskontrolle legt den Fokus auf die effektive Verwaltung und Überwachung des Zugriffs auf Informationen und Systeme in einer Organisation. Die Anleitung beginnt mit einer klaren Definition des Geltungsbereichs, um zu bestimmen, welche Bereiche und Ressourcen durch die Zugriffskontrolle abgedeckt werden. Die Zielsetzung wird präzise formuliert, um sicherzustellen, dass die Zugriffskontrolle die spezifischen Sicherheitsziele der Organisation unterstützt. Ein wesentlicher Schritt ist die Identifikation von Zugriffsanforderungen, wobei festgelegt wird, welche Benutzergruppen auf welche Informationen und Systeme zugreifen dürfen. Dies bildet die Grundlage für die Festlegung von Zugriffsrichtlinien. Die Anleitung beschreibt detailliert, wie Zugriffsrichtlinien entwickelt werden, einschliesslich der Definition von Berechtigungen, Rollen und Verantwortlichkeiten. Hierbei werden Sicherheitsprinzipien berücksichtigt, um den Prinzipien der Vertraulichkeit, Integrität und Verfügbarkeit gerecht zu werden. Die konkrete Umsetzung der Zugriffskontrollen wird beschrieben, wobei verschiedene Technologien und Mechanismen, wie z. B. Authentifizierung und Autorisierung, berücksichtigt werden. Hierbei wird darauf geachtet, dass die Zugriffskontrollen sowohl wirksam als auch benutzerfreundlich sind. Die Anleitung legt fest, wie die Zugriffskontrollen überwacht und durch regelmässige Audits überprüft werden. Dies gewährleistet die Einhaltung der Zugriffsrichtlinien und ermöglicht die Identifikation von Abweichungen oder potenziellen Sicherheitsrisiken. Massnahmen zur Schulung und Sensibilisierung der Mitarbeiter für die Zugriffskontrolle werden beschrieben. Dies beinhaltet Schulungsprogramme, um sicherzustellen, dass alle Benutzer ein angemessenes Verständnis für sichere Zugriffspraktiken entwickeln. Die Anleitung sieht vor, wie auf Sicherheitsvorfälle im Zusammenhang mit Zugriffskontrollen reagiert werden soll. Dies schliesst Massnahmen zur sofortigen Reaktion auf unautorisierte Zugriffe oder Sicherheitsverletzungen mit ein. Die Dokumentation der implementierten Zugriffskontrollen sowie die Erstellung von Berichten über den aktuellen Status sind ebenfalls integraler Bestandteil der Arbeitsanleitung. Dies gewährleistet Transparenz und ermöglicht eine kontinuierliche Verbesserung. Die Anleitung betont die Notwendigkeit, alle relevanten Stakeholder, einschliesslich IT-Personal, Management und Benutzer, in den Prozess einzubeziehen, um eine ganzheitliche und effektive Umsetzung der Zugriffskontrolle zu gewährleisten. Die Arbeitsanleitung für den Bereich ISMS: Zugriffskontrolle dient als umfassender Leitfaden, um sicherzustellen, dass die Zugriffskontrollen klar definiert, implementiert und kontinuierlich verbessert werden.
<b>HoP-01-01-03-07 Arbeitsanleitung Bereich ISMS:</b>	Die Arbeitsanleitung für den Bereich ISMS (Information Security Management System) im Kontext der Multi-Faktor-Authentifizierung (MFA) konzentriert sich darauf, wie die Organisation dieses fortschrittliche Sicherheitskonzept implementieren kann. Die Anleitung beginnt mit der klaren Definition des Geltungsbereichs, um festzulegen, welche Bereiche und Systeme von der MFA abgedeckt werden. Die Zielsetzung wird präzise formuliert, um sicherzustellen, dass die MFA die





Titel	Beschreibung
<b>Multi Faktor Authentisierung</b>	spezifischen Sicherheitsziele der Organisation unterstützt, insbesondere in Bezug auf Authentifizierung und Zugriffskontrolle. Es wird erläutert, wie die Organisation kritische Bereiche identifizieren kann, in denen die MFA besonders wichtig ist. Dies könnte sensible Datenbanken, administrative Zugänge oder andere Schlüsselbereiche umfassen. Die Anleitung beschreibt die Auswahl und Implementierung verschiedener Authentifizierungsfaktoren, die in der MFA verwendet werden sollen. Dazu gehören typischerweise Wissensfaktoren (Passwörter), Besitzfaktoren (Smartcards, Token) und biometrische Faktoren (Fingerabdrücke, Gesichtserkennung). Es wird erläutert, wie die MFA nahtlos in bestehende Systeme und Authentifizierungsmethoden integriert werden kann, um Störungen zu minimieren und eine reibungslose Umstellung zu ermöglichen. Die Anleitung betont die Bedeutung einer benutzerfreundlichen Implementierung der MFA, um die Akzeptanz der Mitarbeiter zu fördern. Schulungen und Sensibilisierungsmassnahmen werden möglicherweise vorgeschlagen, um sicherzustellen, dass die Benutzer die neuen Authentifizierungsmethoden richtig verstehen und nutzen können. Massnahmen zur Überwachung der MFA-Implementierung werden beschrieben, um sicherzustellen, dass alle Authentifizierungsfaktoren ordnungsgemäss funktionieren und potentielle Sicherheitsvorfälle sofort erkannt werden können. Die Anleitung sieht vor, wie auf Sicherheitsvorfälle im Zusammenhang mit der MFA reagiert werden soll. Dies kann die sofortige Sperrung von Zugängen und die Wiederherstellung von Konten nach einem Kompromiss umfassen. Es wird festgelegt, wie die MFA-Implementierung dokumentiert und überwacht wird. Regelmässige Berichte über den Status und mögliche Verbesserungen werden als wichtige Elemente der kontinuierlichen Verbesserung hervorgehoben. Die Anleitung betont die Notwendigkeit, alle relevanten Stakeholder, einschliesslich IT-Personal, Management und Benutzer, in den Prozess der MFA-Implementierung einzubeziehen, um eine umfassende und effektive Umsetzung sicherzustellen. Die Arbeitsanleitung für den Bereich ISMS: Multi-Faktor-Authentisierung dient als umfassender Leitfaden, um sicherzustellen, dass die MFA klar definiert, implementiert und kontinuierlich verbessert wird.
<b>HoP-01-01-03-08 Arbeitsanleitung Bereich ISMS: Management von privilegierten Zugriffsrechten</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für das Management von privilegierten Zugriffsrechten legt grundlegende Prinzipien und Schritte fest, um einen sicheren Umgang mit besonders privilegierten Zugriffsberechtigungen in Unternehmen und Organisationseinheiten zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu schützen, während gleichzeitig der Zugang zu privilegierten Benutzerkonten streng kontrolliert wird. Die Arbeitsanleitung betont die Notwendigkeit einer sorgfältigen Verwaltung privilegierter Zugriffsrechte, um das Risiko von Missbrauch oder unbefugter Nutzung zu minimieren. Dabei werden klare Prozesse für die Vergabe, Überprüfung und Überwachung privilegierter Zugriffsrechte festgelegt, um sicherzustellen, dass diese nur an autorisierte Personen vergeben werden und dass ihre Nutzung angemessen überwacht wird. Es werden klare Verantwortlichkeiten für die Umsetzung des Managements von privilegierten Zugriffsrechten auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Identifikation von Administratoren und Sicherheitsverantwortlichen ein, die für die Verwaltung privilegierter Zugriffsrechte verantwortlich sind, sowie Schulungsmassnahmen, um sicherzustellen, dass die Verantwortlichen die Sicherheitsrichtlinien verstehen und befolgen.
<b>HoP-01-01-03-09 Arbeitsanleitung Bereich ISMS: Systeme (Server und Client)</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Systeme, sowohl Server als auch Client, legt grundlegende Prinzipien und Schritte fest, um die Sicherheit und den Schutz von IT-Systemen in Unternehmen und Organisationseinheiten zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu sichern, die auf diesen Systemen verarbeitet werden. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Sicherheitsrichtlinie für Server und Client-Systeme. Dabei werden klare Prozesse für die Konfiguration, den Betrieb und die Überwachung dieser Systeme definiert, um potentielle Schwachstellen zu minimieren und die Einhaltung sicherheitsrelevanter Standards sicherzustellen. Es werden klare Verantwortlichkeiten für die Umsetzung der Sicherheitsrichtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Systemadministratoren und Verantwortlichen für die Systempflege ein, sowie die Schulung der Mitarbeiter, um sicherzustellen, dass sie bewusst mit den Sicherheitsrichtlinien umgehen.
<b>HoP-01-01-03-10 Arbeitsanleitung Bereich ISMS: Leittechnikkomponenten</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Leittechnikkomponenten legt grundlegende Prinzipien und Schritte fest, um die Sicherheit und den Schutz von Leittechniksystemen in Unternehmen und Organisationseinheiten zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in Leittechnikkomponenten zu sichern. Die Arbeitsanleitung betont die Notwendigkeit einer spezifischen Sicherheitsrichtlinie für Leittechniksysteme. Dabei werden klare Prozesse für die Konfiguration, den Betrieb und die Überwachung dieser Systeme definiert, um potentielle Risiken und Schwachstellen zu minimieren und die Einhaltung sicherheitsrelevanter Standards sicherzustellen. Es werden klare Verantwortlichkeiten für die Umsetzung der Sicherheitsrichtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Systemadministratoren und Verantwortlichen für die Pflege von Leittechnikkomponenten ein, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter bewusst mit den Sicherheitsrichtlinien umgehen.
<b>HoP-01-01-03-11 Arbeitsanleitung Bereich ISMS:</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Betriebssysteme und Applikationen legt grundlegende Prinzipien und Schritte fest, um die Sicherheit und den Schutz von IT-Systemen in Unternehmen und Organisationseinheiten zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen auf





Titel	Beschreibung
<b>Betriebssysteme und Applikationen</b>	Betriebssystemen und Applikationen sicherzustellen. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Sicherheitsrichtlinie für Betriebssysteme und Applikationen. Dabei werden klare Prozesse für die Installation, Konfiguration, den Betrieb und die regelmässige Aktualisierung dieser Systeme definiert, um potentielle Schwachstellen zu minimieren und die Einhaltung sicherheitsrelevanter Standards zu gewährleisten. Es werden klare Verantwortlichkeiten für die Umsetzung der Sicherheitsrichtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Systemadministratoren und Verantwortlichen für die Pflege von Betriebssystemen und Applikationen ein, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter bewusst mit den Sicherheitsrichtlinien umgehen.
<b>HoP-01-01-03-12 Arbeitsanleitung Bereich ISMS: Verschlüsselung</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Verschlüsselung legt grundlegende Prinzipien und Schritte fest, um einen sicheren Umgang mit sensiblen Daten in Unternehmen und Organisationseinheiten zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit von Informationen durch den Einsatz von Verschlüsselungstechnologien zu gewährleisten. Die Arbeitsanleitung betont die Notwendigkeit einer umfassenden Verschlüsselungsrichtlinie, die verschiedene Aspekte abdeckt, von der Identifikation von zu verschlüsselnden Daten bis hin zur Auswahl und Implementierung geeigneter Verschlüsselungsalgorithmen und einer Schlüsselverwaltung. Es werden klare Prozesse für die Verschlüsselung von Daten auf verschiedenen Ebenen der Organisation definiert, um sicherzustellen, dass alle relevanten Informationen angemessen geschützt sind. Dabei werden auch Schulungen für Mitarbeiter zur sicheren Handhabung verschlüsselter Daten berücksichtigt. Die Verantwortlichkeiten für die Umsetzung der Verschlüsselungsrichtlinien werden klar festgelegt, einschliesslich der Identifikation von Administratoren und Sicherheitsverantwortlichen, die für die Implementierung und Überwachung der Verschlüsselungstechnologien verantwortlich sind.
<b>HoP-01-01-03-13 Arbeitsanleitung Bereich ISMS: Netzwerke</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Netzwerke legt grundlegende Prinzipien und Schritte fest, um die Sicherheit und den Schutz von IT-Netzwerken in Unternehmen und Organisationseinheiten zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen während der Übertragung über Netzwerke sicherzustellen. Die Arbeitsanleitung betont die Notwendigkeit einer umfassenden Netzwerksicherheitsrichtlinie, die verschiedene Aspekte der Netzwerkarchitektur und -nutzung abdeckt. Dabei werden klare Prozesse für die Konfiguration, Überwachung und den Schutz von Netzwerken vor potentiellen Bedrohungen definiert, um die Einhaltung sicherheitsrelevanter Standards zu gewährleisten. Es werden klare Verantwortlichkeiten für die Umsetzung der Netzwerksicherheitsrichtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Netzwerkadministratoren und Sicherheitsverantwortlichen ein, die für die Implementierung und Überwachung von Sicherheitsmassnahmen auf Netzwerkebene verantwortlich sind.
<b>HoP-01-01-03-14 Arbeitsanleitung Bereich ISMS: Backup &amp; Backup- Checkliste</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Backup und die dazugehörige Backup-Checkliste legt grundlegende Prinzipien und Schritte fest, um die Sicherheit und Verfügbarkeit von Daten in Unternehmen und Organisationseinheiten zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien für die regelmässige Sicherung von Daten sowie die Überprüfung und Wiederherstellung von Backups zu schaffen. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Backup-Richtlinie, die verschiedene Aspekte abdeckt, von der Identifikation kritischer Daten bis hin zur Festlegung von Sicherungsintervallen und -methoden. Dabei werden klare Prozesse für die Durchführung von Backups und die Überprüfung ihrer Integrität definiert, um sicherzustellen, dass im Falle von Datenverlust oder Systemausfällen eine effektive Wiederherstellung möglich ist. Die dazugehörige Backup-Checkliste bietet einen strukturierten Leitfaden für die Umsetzung der Backup-Richtlinien. Diese umfasst die regelmässige Überprüfung von Backup-Protokollen, die Sicherstellung der Vollständigkeit und Aktualität von Backups sowie die Planung von Wiederherstellungstests, um die Effektivität des Backup-Systems zu gewährleisten. Es werden klare Verantwortlichkeiten für die Umsetzung der Backup-Richtlinien und die Durchführung von Backup-Checks auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Backup-Administratoren und Sicherheitsverantwortlichen ein, die für die Planung, Durchführung und Überwachung von Backup- und Wiederherstellungsaktivitäten verantwortlich sind.
<b>HoP-01-01-03-15 Arbeitsanleitung Bereich ISMS: Medienbereini- gung</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Medienbereinigung legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass Informationen auf physischen Medien in Unternehmen und Organisationseinheiten sicher und endgültig gelöscht werden können. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit von Daten zu schützen und sicherzustellen, dass Medien ordnungsgemäss und unwiederbringlich gelöscht werden, bevor sie ausserhalb der Organisation gelangen. Die Arbeitsanleitung betont die Notwendigkeit einer umfassenden Medienbereinigungsrichtlinie, die verschiedene Arten von physischen Medien abdeckt, von Festplatten bis zu USB-Laufwerken. Dabei werden klare Prozesse für die sichere Löschung von Daten definiert, um sicherzustellen, dass keine vertraulichen Informationen auf den Medien verbleiben. Es werden klare Verantwortlichkeiten für die Umsetzung der Medienbereinigungsrichtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Verantwortlichen für die physische Sicherheit und Datenlöschung ein, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter bewusst mit den Sicherheitsrichtlinien im Zusammenhang mit der Medienbereinigung umgehen.



Titel	Beschreibung
<b>HoP-01-01-03-16</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b> <b>LOG-Management</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für das LOG-Management legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass Protokolldaten in Unternehmen und Organisationseinheiten effektiv erfasst, überwacht und verwaltet werden. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Integrität und Verfügbarkeit von Protokolldaten sicherzustellen und gleichzeitig potenzielle Sicherheitsvorfälle frühzeitig zu identifizieren. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden LOG-Management-Richtlinie, die verschiedene Aspekte abdeckt, von der Definition der zu protokollierenden Ereignissen bis hin zur sicheren Speicherung und Überwachung von Protokolldaten. Dabei werden klare Prozesse für die Erfassung, Analyse und Archivierung von Protokolldaten definiert, um sicherzustellen, dass sie sowohl den gesetzlichen Anforderungen als auch den internen Sicherheitsstandards entsprechen. Es werden klare Verantwortlichkeiten für die Umsetzung der LOG-Management-Richtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Administratoren und Sicherheitsverantwortlichen ein, die für die Konfiguration und Überwachung von Protokollierungssystemen verantwortlich sind, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter die Bedeutung von Protokolldaten verstehen und angemessen mit ihnen umgehen.</p>
<b>HoP-01-01-03-17</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b> <b>Malware- und Schwachstellenmanagement</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für das Malware- und Schwachstellenmanagement legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass Unternehmen und Organisationseinheiten effektive Massnahmen gegen Malware und potenzielle Schwachstellen in IT-Systemen implementiert. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Integrität und Verfügbarkeit von Daten zu schützen und gleichzeitig das Risiko von Malware-Infektionen und Sicherheitslücken zu minimieren. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Richtlinie für das Malware- und Schwachstellenmanagement. Dabei werden klare Prozesse für die regelmässige Überwachung von IT-Systemen auf Schwachstellen und die Implementierung von Schutzmassnahmen gegen Malware definiert. Dies schliesst auch Mechanismen für die schnelle Identifizierung, Isolierung und Entfernung von Malware-Infektionen ein. Es werden klare Verantwortlichkeiten für die Umsetzung der Malware- und Schwachstellenmanagement-Richtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies beinhaltet die Identifikation von IT-Sicherheitsverantwortlichen und Administratoren, die für die Überwachung und Aktualisierung von Schutzmechanismen zuständig sind, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter die Risiken von Malware verstehen und sich sicherheitsbewusst verhalten. Die Einhaltung dieser Arbeitsanleitung ist für alle Mitarbeiter verbindlich, und die Geschäftsleitung behält sich das Recht vor, bei Nichteinhaltung angemessene Massnahmen zu ergreifen. Durch die kontinuierliche Überprüfung und Anpassung der Arbeitsanleitung im Bereich Informationssicherheit für Malware- und Schwachstellenmanagement wird sichergestellt, dass sie stets den aktuellen Standards und Anforderungen im Bereich der Informationssicherheit entspricht und so einen effektiven Schutz vor potenziellen Bedrohungen gewährleistet.</p>
<b>HoP-01-01-03-18</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b> <b>Management von Bereich Informationssicherheitsvorfällen (Incident Management)</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für das Management von Sicherheitsvorfällen, auch als Incident Management bekannt, legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass Unternehmen und Organisationseinheiten effektiv und koordiniert auf Sicherheitsvorfälle reagiert. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um Sicherheitsvorfälle schnell zu erkennen, angemessen zu bewerten und darauf zu reagieren, um die Auswirkungen zu minimieren. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Incident-Management-Richtlinie, die verschiedene Arten von Sicherheitsvorfällen abdeckt, von Datenlecks bis zu Cyberangriffen. Dabei werden klare Prozesse für die Identifizierung, Meldung, Untersuchung und Eskalation von Sicherheitsvorfällen definiert, um eine effektive Reaktion zu gewährleisten. Es werden klare Verantwortlichkeiten für die Umsetzung der Incident-Management-Richtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Incident-Response-Teams und Verantwortlichen für die Koordinierung von Massnahmen ein, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter die Bedeutung von sofortigen und präzisen Reaktionen auf Sicherheitsvorfälle verstehen.</p>
<b>HoP-01-01-03-19</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b> <b>Betriebskontinuitätsmanagement (BCM)</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für das Betriebskontinuitätsmanagement (BCM) legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass Unternehmen und Organisationseinheiten widerstandsfähig gegenüber Unterbrechungen ist und im Falle von Störungen oder Katastrophen ihre Geschäftstätigkeiten effektiv fortsetzen kann. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Geschäftskontinuität zu gewährleisten und die Auswirkungen von Unterbrechungen auf ein Minimum zu reduzieren. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden BCM-Richtlinie, die verschiedene Aspekte abdeckt, von der Identifizierung geschäftskritischer Prozesse bis hin zur Entwicklung von Notfallplänen und Wiederherstellungsstrategien. Dabei werden klare Prozesse für die Analyse von Risiken, die Implementierung von Schutzmassnahmen und die regelmässige Überprüfung und Aktualisierung von BCM-Plänen definiert. Es werden klare Verantwortlichkeiten für die Umsetzung der BCM-Richtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von BCM-Verantwortlichen und Notfallteams ein, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter die Notwendigkeit und Verfahren im Zusammenhang mit BCM verstehen.</p>
<b>HoP-01-01-03-20</b> <b>Arbeitsanleitung</b> <b>Bereich ISMS:</b>	<p>Die Arbeitsanleitung für den Bereich ISMS (Information Security Management System) im Kontext des Notfallmanagements ist darauf ausgerichtet, wie das Unternehmen und Organisationseinheiten effektiv auf Sicherheitsvorfälle und Krisensituationen reagieren kann. Die Anleitung beginnt mit</p>



Titel	Beschreibung
<b>Notfallmanagement</b>	<p>einer klaren Definition des Geltungsbereichs, um festzulegen, welche Arten von Sicherheitsvorfällen und Notfällen abgedeckt werden sollen. Die Zielsetzung wird präzise formuliert, um sicherzustellen, dass das Notfallmanagement die spezifischen Sicherheitsziele der Organisation unterstützt. Es wird erläutert, wie eine umfassende Risikobewertung durchgeführt wird, um potenzielle Sicherheitsvorfälle und Notfallszenarien zu identifizieren. Dies könnte Bedrohungen wie Cyberangriffe, Naturkatastrophen oder menschliches Versagen umfassen. Die Anleitung beschreibt den Prozess der Notfallplanung, einschliesslich der Erstellung von klaren Handlungsanweisungen und Verantwortlichkeiten für verschiedene Teams und Mitarbeiter während eines Notfalls. Es wird betont, wie wichtig es ist, verschiedene Szenarien zu berücksichtigen und flexible Pläne zu entwickeln. Massnahmen zur effektiven Kommunikation und Alarmierung werden dargestellt, um sicherzustellen, dass alle relevanten Parteien, einschliesslich Mitarbeiter, Führungskräfte und externe Stakeholder, rechtzeitig informiert werden. Dies kann die Verwendung verschiedener Kommunikationskanäle und -mittel umfassen. Es wird erläutert, wie Teams im Falle eines Notfalls effektiv reagieren sollten. Dies beinhaltet klare Schritte zur Eskalation, Zusammenarbeit mit externen Behörden und die Implementierung von Sofortmassnahmen zur Schadensbegrenzung. Die Anleitung umfasst den Prozess der Wiederherstellung nach einem Notfall, einschliesslich der schrittweisen Rückkehr zu normalen Betriebsabläufen. Es wird betont, wie wichtig eine umfassende Nachbereitung ist, um Lehren aus dem Vorfall zu ziehen und zukünftige Notfallpläne zu verbessern. Es werden Massnahmen zur regelmässigen Durchführung von Notfallübungen und Schulungen für Mitarbeiter vorgeschlagen, um sicherzustellen, dass das Notfallmanagement effektiv und effizient umgesetzt werden kann. Es wird festgelegt, wie das Notfallmanagement dokumentiert und überwacht wird. Regelmässige Berichte über den Status, die Wirksamkeit von Massnahmen und mögliche Verbesserungen werden als wichtige Elemente der kontinuierlichen Verbesserung hervorgehoben. Die Anleitung betont die Notwendigkeit, alle relevanten Stakeholder, einschliesslich IT-Personal, Management und Notfallteams, in den Prozess des Notfallmanagements einzubeziehen, um eine umfassende und effektive Umsetzung sicherzustellen. Die Arbeitsanleitung für den Bereich ISMS: Notfallmanagement dient als umfassender Leitfaden, um sicherzustellen, dass das Unternehmen und die Organisationseinheiten gut vorbereitet ist, auf Notfälle zu reagieren, und dass das Notfallmanagement klar definiert, implementiert und kontinuierlich verbessert wird.</p>
<b>HoP-01-01-03-21 Arbeitsanleitung Bereich ISMS: Sicherheitsmassnahmen für Dienstleister</b>	<p>Die Arbeitsanleitung für den Bereich ISMS (Information Security Management System) bezüglich Sicherheitsmassnahmen für Dienstleister ist darauf ausgerichtet, sicherzustellen, dass externe Partner und Dienstleister angemessen in die Sicherheitsstrategie des Unternehmens und der Organisationseinheiten integriert werden. Die Anleitung beginnt mit der klaren Definition des Geltungsbereichs, um festzulegen, welche Dienstleister und Partner abgedeckt sind. Die Zielsetzung ist darauf ausgerichtet, sicherzustellen, dass die Sicherheitsmassnahmen für Dienstleister den Sicherheitsstandards der Organisation entsprechen. Es wird erläutert, wie eine umfassende Risikobewertung für Dienstleister durchgeführt wird, um potenzielle Sicherheitsrisiken und Bedrohungen zu identifizieren, die sich aus deren Tätigkeiten ergeben könnten. Die Anleitung beschreibt die Integration von Sicherheitsanforderungen in Verträge und Vereinbarungen mit Dienstleistern. Dabei wird betont, wie wichtig es ist, sicherzustellen, dass die Dienstleister die relevanten Compliance-Standards und Sicherheitsrichtlinien einhalten. Massnahmen zur laufenden Überwachung der Sicherheitsleistung von Dienstleistern werden dargestellt. Dies kann die regelmässige Durchführung von Audits, Sicherheitsprüfungen und Leistungsbewertungen umfassen. Es wird erläutert, wie klare Sicherheitsvorgaben für Dienstleister erstellt und kommuniziert werden. Die Schulung von Dienstleistern in Bezug auf Sicherheitsrichtlinien und -verfahren wird als integraler Bestandteil hervorgehoben. Die Anleitung umfasst Massnahmen zur Sicherstellung, dass Dienstleister in Notfallsituationen angemessen reagieren können. Dies schliesst die Definition von Notfallplänen, Kommunikationsverfahren und koordinierten Reaktionsmechanismen ein. Es wird festgelegt, wie die Dienstleister regelmässig über ihre Sicherheitsleistung berichten und transparente Einblicke in ihre Sicherheitsmassnahmen gewähren sollten. Dies fördert eine offene Kommunikation und Zusammenarbeit. Die Anleitung betont die Notwendigkeit einer engen Zusammenarbeit mit Dienstleistern im Falle von Sicherheitsvorfällen. Dies umfasst klare Prozesse für die Meldung von Vorfällen, Eskalationsverfahren und die gemeinsame Bewältigung von Sicherheitsbedrohungen. Die Anleitung schliesst mit dem Fokus auf kontinuierliche Verbesserung und Anpassung der Sicherheitsmassnahmen für Dienstleister ab. Dies umfasst regelmässige Überprüfungen, Feedback-Schleifen und die Integration neuer Sicherheitsstandards. Die Arbeitsanleitung für den Bereich ISMS: Sicherheitsmassnahmen für Dienstleister stellt sicher, dass Dienstleister angemessen in die Sicherheitsstrategie integriert werden und dazu beitragen, die Gesamtsicherheit des Unternehmens und der Organisationseinheiten zu gewährleisten.</p>
<b>HoP-01-01-03-22 Arbeitsanleitung Bereich ISMS: Lieferanten Management</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für das Lieferantenmanagement legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass Unternehmen und Organisationseinheiten in Bezug auf ihre Lieferanten und Partner angemessene Sicherheitsstandards aufrechterhalten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um das Sicherheitsrisiko, das von externen Partnern ausgeht, zu minimieren und die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Lieferantenmanagement-Richtlinie, die verschiedene Aspekte abdeckt, von der Auswahl und Überprüfung von Lieferanten bis zur Festlegung von Sicherheitsanforderungen und Überwachungsmechanismen. Dabei werden klare Prozesse für die Risikobewertung, Vertragsgestaltung</p>





Titel	Beschreibung
	und regelmässige Überprüfung der Sicherheitspraktiken der Lieferanten definiert. Es werden klare Verantwortlichkeiten für die Umsetzung der Lieferantenmanagement-Richtlinien auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Verantwortlichen für die Auswahl, Überwachung und Beendigung von Lieferantenbeziehungen ein, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter die Bedeutung der Sicherheit bei der Zusammenarbeit mit externen Partnern verstehen.
<b>HoP-01-01-03-23 Arbeitsanleitung Bereich ISMS: Informationssicherheit im Personalbereich</b>	<p>Die Arbeitsanleitung im Bereich Informationssicherheit für die Sicherheit im Personalbereich legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass die Mitarbeiter der Unternehmen und Organisationseinheiten angemessen qualifiziert, geschult, sensibilisiert und sicherheitsbewusst handeln. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um menschliche Faktoren als potenzielle Sicherheitsrisiken zu minimieren und eine sichere Arbeitsumgebung zu fördern.</p> <p>Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Personalrichtlinie für Informationssicherheit. Dabei werden klare Prozesse für die Schulung der Mitarbeiter in sicherheitsrelevanten Angelegenheiten, die Sensibilisierung für mögliche Bedrohungen und die Förderung eines Sicherheitsbewusstseins am Arbeitsplatz definiert. Es werden klare Verantwortlichkeiten für die Umsetzung der Sicherheitsrichtlinien im Personalbereich auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Sicherheitsbeauftragten und Schulungsverantwortlichen ein, sowie Massnahmen zur regelmässigen Bewertung und Aktualisierung der Sicherheits-schulungen.</p>
<b>HoP-01-01-03-24 Arbeitsanleitung Bereich ISMS: Informationssicherheit in Projekten</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für Projekte legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass Informationssicherheitsaspekte angemessen in die Planung, Umsetzung und Bewertung von Projekten der Unternehmen und Organisationseinheiten integriert werden. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um sicherzustellen, dass Projekte von Anfang an sicherheitsbewusst gestaltet und umgesetzt werden. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Richtlinie für Informationssicherheit in Projekten. Dabei werden klare Prozesse für die Identifizierung von Sicherheitsanforderungen, die Durchführung von Risikobewertungen und die Integration von Sicherheitskontrollen in alle Phasen des Projektzyklus definiert. Es werden klare Verantwortlichkeiten für die Umsetzung der Richtlinien für Informationssicherheit in Projekten auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Sicherheitsverantwortlichen und Projektmanagern ein, die für die Integration von Informationssicherheitspraktiken in ihren Projekten verantwortlich sind, sowie Schulungsmassnahmen, um sicherzustellen, dass Projektteams die Bedeutung von Informationssicherheit verstehen.
<b>HoP-01-01-03-25 Arbeitsanleitung Bereich ISMS: Nutzung von Cloud-Services</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für die Nutzung von Cloud-Services legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass die Integration von Cloud-Diensten in Unternehmen und Organisationseinheiten sicher und konform mit den Informationssicherheitsstandards erfolgt. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten in der Cloud zu gewährleisten. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Richtlinie für die Nutzung von Cloud-Services. Dabei werden klare Prozesse für die Auswahl von Cloud-Dienstleistern, die Bewertung von Sicherheitsstandards, die Implementierung von Sicherheitskontrollen und die regelmässige Überprüfung der Cloud-Sicherheit definiert. Es werden klare Verantwortlichkeiten für die Umsetzung der Richtlinien für die Nutzung von Cloud-Services auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von Cloud-Verantwortlichen und IT-Administratoren ein, die für die Konfiguration und Überwachung von Cloud-Sicherheitsmassnahmen verantwortlich sind, sowie Schulungsmassnahmen, um sicherzustellen, dass Mitarbeiter die sicherheitsrelevanten Aspekte bei der Nutzung von Cloud-Services verstehen.
<b>HoP-01-01-03-26 Arbeitsanleitung Bereich ISMS: Verwendung von maschinellem Lernen und künstlicher Intelligenz</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für die Verwendung von maschinellem Lernen und künstlicher Intelligenz (KI) legt grundlegende Prinzipien und Schritte fest, um sicherzustellen, dass der Einsatz von KI-Technologien in Unternehmen und Organisationseinheiten sicher, ethisch und konform mit den Informationssicherheitsstandards erfolgt. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Integrität von KI-Systemen zu gewährleisten, Datenschutzaspekte zu berücksichtigen und mögliche Sicherheitsrisiken zu minimieren. Die Arbeitsanleitung betont die Wichtigkeit einer umfassenden Richtlinie für die Verwendung von maschinellem Lernen und KI. Dabei werden klare Prozesse für die Auswahl und Implementierung von KI-Technologien, die Bewertung von Datenschutzrisiken, die regelmässige Überprüfung der Algorithmen und die Schulung von Mitarbeitern im Umgang mit KI-Systemen definiert. Es werden klare Verantwortlichkeiten für die Umsetzung der Richtlinien für die Verwendung von maschinellem Lernen und KI auf verschiedenen Ebenen der Organisation festgelegt. Dies schliesst die Identifikation von KI-Verantwortlichen, Datenschutzbeauftragten und IT-Experten ein, die für die Sicherheit und ethische Anwendung von KI-Technologien verantwortlich sind.
<b>HoP-01-01-04-01 Arbeitsanleitung Bereich Benutzer von Informationswerten:</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für die Nutzung von mobilen Geräten legt die wesentlichen Schritte und Prinzipien fest, um sicherzustellen, dass mobile Geräte in der Organisation sicher und verantwortungsbewusst verwendet werden. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen, die über mobile Geräte zugänglich sind. Die Arbeitsanleitung betont die Notwendigkeit einer klaren Sicherheitsrichtlinie für mobile Geräte, die sowohl Unternehmens- und



Titel	Beschreibung
<b>Nutzung von mobilen Geräten</b>	Organisationseinheitenrichtlinien als auch gesetzliche Anforderungen berücksichtigt. Dabei werden Aspekte wie Zugriffskontrolle, Datensicherheit, Verlust oder Diebstahl von Geräten und die Nutzung von öffentlichen Netzwerken berücksichtigt. Es werden klare Verantwortlichkeiten für die Umsetzung der Sicherheitsrichtlinie für mobile Geräte auf verschiedenen Ebenen der Organisation definiert. Dies schliesst die Schulung der Mitarbeiter ein, um ein Bewusstsein für die Sicherheitsrisiken im Zusammenhang mit mobilen Geräten zu schaffen, sowie die Implementierung von Mechanismen zur Überwachung und Durchsetzung der Sicherheitsrichtlinien.
<b>HoP-01-01-04-02 Arbeitsanleitung Bereich Benutzer von Informations- werten: Nutzung von OT- Assets</b>	Die Arbeitsanleitung im Bereich Informationssicherheit für die Nutzung von Operational Technology (OT)-Assets legt die grundlegenden Schritte und Prinzipien fest, um eine sichere und verantwortungsbewusste Verwendung von OT-Geräten und -Systemen in unserer Organisation zu gewährleisten. Ihr Hauptziel besteht darin, klare Leitlinien zu schaffen, um die Integrität, Verfügbarkeit und Vertraulichkeit von OT-Assets zu schützen und gleichzeitig die betriebliche Kontinuität sicherzustellen. Die Arbeitsanleitung betont die Notwendigkeit einer umfassenden Risikoanalyse, die die spezifischen Anforderungen und Besonderheiten von OT-Assets berücksichtigt. Dabei werden klare Prozesse für die Identifikation von Risiken, die Bewertung ihrer Auswirkungen auf betriebliche Abläufe und die Umsetzung von angemessenen Sicherheitsmassnahmen festgelegt. Es werden klare Verantwortlichkeiten für die Umsetzung der Sicherheitsrichtlinien für OT-Assets auf verschiedenen Ebenen der Organisation definiert. Dies beinhaltet die Schulung von Mitarbeitern, um ein Bewusstsein für die besonderen Sicherheitsanforderungen von OT-Systemen zu schaffen, sowie die Implementierung von Mechanismen zur kontinuierlichen Überwachung und Anpassung der Sicherheitsmassnahmen.





## Anhang G: Weiterführende Literatur

Titel	Jahr	Herausgeber & Beschreibung
<b>Massnahmen zum Schutz von industriellen Kontrollsystemen (IKS)</b>	2013	Hrsg.: Melde- und Analysestelle Informationssicherung MELANI Diese Anleitung beschreibt basierend auf US-amerikanischen Unterlagen vom <i>Department of Homeland Security, Industrial Control Systems - Cyber Emergency Response Team (IKS-CERT)</i> sowie dem <i>National Institute of Standards and Technology (NIST)</i> knapp und pragmatisch auf 8 Seiten die wichtigsten 11 Massnahmen, die IKS-Betreiber gewährleisten müssen.
<b>Risiko- und Verwundbarkeitsanalyse des Teilssektors Stromversorgung</b>	2016	Hrsg.: Bundesamt für wirtschaftliche Landesversorgung (BWL) Die Risiko- und Verwundbarkeitsanalyse ist basierend auf der Nationalen Cyber-Strategie (NCS) und der Strategie zum Schutz kritischer Infrastrukturen (SKI) entwickelt worden. Ziel ist die Analyse der Verwundbarkeit gegenüber Ausfällen oder Störungen der IKT im kritischen Teilssektor „Stromversorgung“.
<b>Leitfaden Schutz kritischer Infrastrukturen (Leitfaden SKI)</b>	2015	Hrsg.: Bundesamt für Bevölkerungsschutz (BABS) Der Leitfaden stellt ein Instrument zur Überprüfung und gegebenenfalls Verbesserung der Resilienz der kritischen Infrastrukturen dar. Insbesondere ist er in Hinblick auf die Anwendung in kritischen Teilssektoren (z.B. Stromversorgung) durch Betreiber, Branchenverbänden (wie VSE) und Fachbehörden konzipiert. Im Wesentlichen beschreibt der Leitfaden ein mögliches Risikomanagement-Vorgehen: Analyse (Ressourcen-Identifikation, Verwundbarkeiten, Risiken), Bewertung, Massnahmen sowie deren Sicherstellung (Umsetzung, Überprüfung, Verbesserung). Das Vorgehen kann durchaus bzw. sollte gar in bestehende Managementprozesse integriert oder darauf aufbauend ausgeführt werden.
<b>Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI)</b>	2012	Hrsg.: Bundesamt für Bevölkerungsschutz (BABS) Die Strategie umschreibt den Geltungsbereich, bezeichnet die kritischen Infrastrukturen (u.a. Stromversorgung mit sehr grosser Kritikalität) und hält die übergeordneten Grundsätze beim Schutz kritischer Infrastrukturen fest. Die nationale SKI-Strategie richtet sich an alle Stellen, die im Umfeld des Schutzes kritischer Infrastrukturen Verantwortlichkeiten aufweisen, insbesondere an die jeweils zuständigen Behörden, die politischen Entscheidungsträger und die Betreiber von kritischen Infrastrukturen (z.B. Energieversorgungsunternehmen EVU).
<b>Nationale Cyberstrategie (NCS)</b>	2023	Hrsg.: Nationales Zentrum für Cybersicherheit (NCSC) Die Schweizerische Nationale Cyberstrategie (NCS) ist ein strategisches Rahmenwerk, das die Ziele und Massnahmen der Schweiz im Umgang mit Cyberbedrohungen festlegt. Sie zielt darauf ab, die Cybersicherheit des Landes zu stärken, die Resilienz gegenüber Cyberangriffen zu erhöhen und die digitale Souveränität zu wahren. Die NCS legt Schwerpunkte auf die Zusammenarbeit zwischen Regierung, Wirtschaft, Wissenschaft und Zivilgesellschaft, um eine koordinierte Reaktion auf Cyberbedrohungen zu ermöglichen. Zu den Kernbereichen gehören die Stärkung der Cyberabwehr, die Förderung von Cyberkompetenzen und -innovationen sowie die internationale Zusammenarbeit im Bereich der Cybersicherheit. Die Umsetzung der NCS erfolgt durch verschiedene staatliche Stellen und Partner, um eine umfassende Sicherheitsarchitektur zu gewährleisten.
<b>VSE IKT Continuity</b>	2011	Hrsg.: Verband Schweizerischer Elektrizitätsunternehmen (VSE) Ist ein Schlüsseldokument des Branchenverbandes mit Umsetzungsempfehlungen zur Gewährleistung der ständigen Disponibilität der Informatik- und der Kommunikationstechnologie zwecks Sicherstellung der Versorgung.
<b>VSE Handbuch Grundschutz für «Operational Technology» in der Stromversorgung</b>	2018	Hrsg.: Verband Schweizerischer Elektrizitätsunternehmen (VSE) Massnahmen und Hilfsmittel für die Reduktion von Cyber-Risiken in der kritischen Infrastruktur der Stromversorgung auf ein akzeptables Mass durch die Implementierung einer sogenannten «Defense-in -Depth»-Strategie.
<b>BDEW und oe: White Paper und Ausführungshinweise: Anforderungen an sichere Steuerungs- und</b>	2024	Hrsg.: Bundesverband der Energie- und Wasserwirtschaft (BDEW) und Österreichs E-Wirtschaft (oe) Die beiden Dokumente beschreiben technische und betriebliche Sicherheitsmassnahmen für neu zu beschaffende bzw. neu



Titel	Jahr	Herausgeber & Beschreibung
<b>Telekommunikationssysteme</b>		einzuführende IT-gestützte Steuerungs- und Telekommunikationssysteme im Prozessbereich von Energieversorgungsunternehmen. Ziel ist die positive Beeinflussung der Produktentwicklung und die Vermittlung eines gemeinsamen Verständnisses. Adressaten sind potenzielle Auftragnehmer sowie unternehmensinterne Planer und Betreiber. Referenzen auf die internationalen Standards ISO 27002 und 27019 dienen lediglich als Hinweis, verbindlich umzusetzen sind immer nur die explizit aufgeführten Forderungen der vorliegenden Dokumente. Die Systematik unterscheidet sich denn auch etwas von den ISO-Standards.
<b>IT-Sicherheitskatalog gemäss §11 Absatz 1a Energiewirtschaftsgesetz</b>	2015	Hrsg.: Bundesnetzagentur (BNetzA) Deutsche Energieversorger müssen per Gesetz (EnWG 2011 in §11) bis spätestens 31. Januar 2018 einen angemessenen Schutz ihrer IKT-Systeme, die für einen sicheren Netzbetrieb notwendig sind, nachweisen und die an sie gestellten Anforderungen gegenüber der Bundesnetzagentur (BNetzA) durch ein Zertifikat belegen. Dazu veröffentlichte die BNetzA in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) den IT-Sicherheitskatalog. Kernforderung des Sicherheitskatalogs ist die Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäss DIN ISO/IEC 27001. Die Anforderungen des Sicherheitskatalogs sind von allen Netzbetreibern unabhängig von Grösse oder Anzahl angeschlossener Kunden zu erfüllen. Der Katalog enthält konkrete Anforderungen an Netzbetreiber, die unter Verweis auf die internationalen Standards umzusetzen sind.
<b>ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements</b>	2022	Hrsg.: International Standard Organization (ISO) / International Electrotechnical Commission (IEC) Detailliert die Anforderungen an ein Information Security Management System (ISMS). Die ISO 27k Serie umfasst eine Reihe von <i>Information Security Standards</i> , wovon folgende hier von Interesse sind:  27000:2018 Übersicht und Vokabular (:2018 indiziert Jahr der Herausgabe) 27001:2022 Anforderungen: Grundlagen mit Kontrollen und Kontrollzielen im Anhang 27002:2022 Leitfaden für Kontrollen 27003:2017 Anleitung zur Implementation 27005:2022 Risiko Management 27019:2017 Technischer Bericht mit Ergänzungen spezifisch für Prozesskontrollen in der Elektrizitätsversorgung  Die ISO 27000 Security Standards sind mittlerweile die am meisten verbreiteten und dürften sich in den kommenden Jahren als die massgebenden erweisen. Schon heute liegt richtig, wer ISO Security Standards befolgt. Im Gegensatz zu anderen Standards, wie IT-Grundschutz, NERC, ANSI/ISA oder NIST, sind sie nicht so sehr detailliert, dementsprechend flexibel anwendbar und können über eine längere Zeitspanne kontinuierlich verbessert und erweitert werden.
<b>ISO/IEC 27002:2022 Information technology — Security techniques — Code of practice for information security controls</b>		
<b>ISO/IEC TR 27019:2017 Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry</b>		
<b>NERC CIP – Critical Infrastructure Protection</b>	2006 ff	Hrsg.: North American Electric Reliability Corporation (NERC) Die NERC Critical Infrastructure Protection Standards sind derzeit in Version 5 und teilweise Version 6. Es sind die einzigen Standards in den USA, die nicht freiwillig, sondern zwingend durch die „Bulk Electric Systems“ (BES) bzw. deren Betreiber umgesetzt werden müssen. Es wird verlangt, dass die BES mindestens eine Security Policy definieren und implementieren, die vier Bereiche umfasst: Security Awareness, physische Sicherheit, Remote Access und Incident Response. Dabei reicht es nicht, Policies bloss zu dokumentieren, sondern Prozesse, Prozeduren und Kontrollen müssen implementiert und auch in einem Audit geprüft werden.
<b>Guide to Industrial Control Systems (IKS) Security SP 800-82 Rev.3</b>	2023	Hrsg.: National Institute of Standards and Technology (NIST) Dieser Leitfaden gibt eine umfassende Einführung in IKS, Topologien und Architekturen, identifiziert Bedrohungen und Verwundbarkeiten und gibt Empfehlungen zu Gegenmassnahmen und Risikominderung. Zudem werden IKS-spezifische Kontrollen basierend auf dem NIST 800-53 Framework präsentiert.
<b>ISA/IEC 62443</b>	2009 ff	Hrsg.: International Society of Automation (ISA) / International Electrotechnical Commission (IEC)



Titel	Jahr	Herausgeber & Beschreibung
<b>Industrial Communication Networks – Network and System Security</b>		Serie von insgesamt 13 <i>Industrial Automation and Control System</i> (IKS) Security Standards und technischen Berichten. Diese Normen sind allgemein anwendbar im Bereich industrieller Automation und nicht stromversorgungs-spezifisch. Sie basieren auf den ISO 27000 Standards und erweitern diese mit Unterschieden und Spezifika industrieller Automation. Speziell zu erwähnen ist die Behandlung von Netzwerk- und Zonenarchitektur, die sich in anderen Standards kaum oder nicht so detailliert findet.
<b>IEC 62351 Power Systems Management and Associated Information Exchange – Data and Communications Security</b>	2007 ff	Hrsg.: International Electrotechnical Commission (IEC) Dies ist ein stromversorgungsspezifischer Standard und ergänzt den IEC 62443 mit Unterschieden und Erweiterungen aus der Stromerzeugung, Übertragung und Verteilung. Er reiht sich mit weiteren Standards wie IEC 61850 zur Automation von Unterwerken sowie 60870 zu IEC 61850 zur Automation von Unterwerken sowie 60870 zu IEC 61850 zur Automation von Unterwerken sowie 60870 zu IEC 61850 zur Automation von Unterwerken sowie 60870 zu IEC 61850 zur Automation von Unterwerken ein. Die IEC 62351 Standards (mittlerweile 13 Teile) sind technisch detailliert und können schwer mit konzeptionellen Sicherheitsstandards verglichen werden.
<b>IEEE 1686 IEEE Standard for Intelligent Electronic Devices Cyber-Security Capabilities</b>	2022	Hrsg.: Institute of Electrical and Electronics Engineers (IEEE) Funktionen und Konfigurationen, die in intelligenten elektronischen Geräten (IEDs) zwecks OT-Sicherheit kritischer Infrastruktur zur Verfügung gestellt werden sollen, sind in dieser Norm definiert. Sicherheit in Bezug auf Zugriff, Betrieb, Konfiguration, Firmware-Revision und Datenabruf von einem IED sowie Datenverschlüsselung von und zu IEDs werden adressiert. Kommunikationen zum Zwecke des Stromschutzes (Teleprotektion) oder zum Schutz von Leben, Leib und Umwelt werden in dieser Norm nicht behandelt. Der Standard baut gewissermaßen auf NERC-CIP (Critical Infrastructure Protection) auf und ergänzt diese auf IED-Stufe, so dass elektronische Geräte nicht NERC-CIP Anforderungen unterlaufen.
<b>Recommended Practice: Improving Industrial Control System Cyber-Security with Defense-in-Depth Strategies</b>	2016	Hrsg.: Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (IKS-CERT) Eine erweiterte und erneuerte Ausgabe einer früheren Veröffentlichung aus dem Jahre 2006. Umfassende Einführung in die Defense-in-depth Security Strategie für industrielle Kontrollsysteme.
<b>BSI IT-Grundschutz</b>		Hrsg.: Bundesamt für Sicherheit in der Informationstechnik (BSI) Der IT-Grundschutz beschreibt mit Hilfe der BSI-Standards 100-1 bis 100-3 eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Informations-Sicherheits-Management-Systems (ISMS). Die IT-Grundschutz-Kataloge bzw. das IT-Grundschutz-Kompendium beschreiben die Umsetzung der damit einhergehenden Massnahmen und Ziele. Das damit aufgebaute ISMS erfüllt die Anforderungen von ISO 27001 und verfügt über ein Äquivalent zu den Handlungsempfehlungen von ISO 27002.
<b>BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz (V1.2 2014)</b>	2014 ff	Sicherheit kann nach den vom BSI entwickelten Vorgehensweisen des IT-Grundschutzes, aber auch nach Standards der ISO 27000-Familie eingeführt und kontrolliert werden. Beide Möglichkeiten sind von ihrem Ansatz her kompatibel. Mit beiden wird ein ISMS aufgebaut und betrieben, und Risiken im Bereich der Informationssicherheit ermittelt und durch geeignete Massnahmen auf ein akzeptables Mass reduziert werden. Ein wesentlicher Bestandteil eines ISMS nach ISO 27001 ist die Risikoanalyse und –Bewertung, wohingegen eine Risikoanalyse beim BSI-Grundschutz nur in besonderen Fällen erforderlich ist. In den BSI-Grundschutzkatalogen wird die detaillierte Vorgehensweise zur Minimierung von Risiken beschrieben. Demnach lassen die ISO-Standards mehr Interpretation offen und sind flexibler, geben aber auch entsprechend weniger detailliert Anleitung und Unterstützung. Für den IT-Grundschutz-Ansatz gilt demnach entsprechend das Gegenteil und bietet, wie der Name aussagt, einen „Grundschutz“. Der Aufwand für eine ISO-basierte Zertifizierung ist geringer.
<b>BSI Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz</b>		
<b>BSI IKS Security –Kompendium</b>	2013	Hrsg.: Bundesamt für Sicherheit in der Informationstechnik (BSI) Das Kompendium stellt ein Grundlagenwerk dar und soll einen einfachen Zugang zur IKS IT Security ermöglichen. Erläutert werden die notwendigen IKS-Grundlagen, Abläufe, relevante Standards und ein konkreter Zusammenhang zum IT-Grundschutz, wobei auch



Titel	Jahr	Herausgeber & Beschreibung
		Unterschiede und Lücken etablierter Standards und insbesondere des IT-Grundschutzes im Bereich IKS-Security aufgezeigt werden.
<b>BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)</b>	2017	Hrsg.: Bundesamt für Sicherheit in der Informationstechnik (BSI) Der Standard beschreibt ISMS-relevante Methoden, Aufgaben und Aktivitäten, welche ein erfolgreiches ISMS ausmachen und welche Aufgaben auf die Führungsebene zukommen. Bei der Umsetzung der Empfehlungen hilft die Methodik des IT-Grundschutzes, die eine Schritt-für-Schritt-Anleitung für die Entwicklung eines ISMS in der Praxis gibt und konkrete Massnahmen für alle Aspekte der Informationssicherheit nennt. Der Standard 200-1 richtet sich an Verantwortliche für den IT-Betrieb, Sicherheitsbeauftragte, -experten und -berater, welche mit dem Management für Informationssicherheit beauftragt sind.
<b>BSI-Standard 200-2 IT-Grundschutz Vorgehensweise</b>	2017	Hrsg.: Bundesamt für Sicherheit in der Informationstechnik (BSI) Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis und mit Hilfe der Grundschutzkataloge aufgebaut und betrieben werden kann. Es wird sehr ausführlich darauf eingegangen, wie ein Sicherheitskonzept in der Praxis erstellt wird, wie angemessene Sicherheitsmassnahmen ausgewählt werden und was bei der Umsetzung zu beachten ist.
<b>BSI-Standard 200-3 Risikoanalyse</b>	2017	Hrsg.: Bundesamt für Sicherheit in der Informationstechnik (BSI) Dieses Dokument beschreibt eine Methodik zur Durchführung von Risikoanalysen, die ein bestehendes IT Grundschutz Sicherheitskonzept ergänzen. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen als Hilfsmittel verwendet. Ein wesentlicher Unterschied zu den meisten anderen Risikoanalysemethoden ist das gänzliche Weglassen von Eintrittswahrscheinlichkeiten von Schadensereignissen.
<b>BSI-Standard 100-4 Notfallorganisation</b>	2008	Hrsg.: Bundesamt für Sicherheit in der Informationstechnik (BSI) Dieses Dokument beschreibt eine Methodik zur Etablierung eines Notfallmanagements, welche auf die in Standard 100-2 beschriebenen Vorgehensweisen aufsetzt und ergänzt. Beschrieben werden sämtliche Prozesse innerhalb einer Notfallorganisation von Business Impact Analyse über Krisenmanagement bis hin zu Rückführung und kontinuierlichen Prozessstätigkeiten ausserhalb von Krisensituationen.
<b>ISA 95 / IEC/ISO 62264 Enterprise Control System Integration</b>	2010 ff	Hrsg.: International Society of Automation (ISA) / International Electrotechnical Commission (IEC) Eine Normenreihe von insgesamt 5 Standards zur Integration von Unternehmens-IT und Kontroll-Leitsystemen.
<b>Energy Sector Cyber-Security Framework Implementation Guidance</b>	2015	Hrsg.: Department of Energy (DOE) Eine Anleitung des DOE zur Implementierung eines Critical Infrastructure Cyber-Security Frameworks in Anlehnung an das Framework vom NIST.
<b>Report on Cyber-Security Information Sharing in the Energy Sector</b>	2017	Hrsg.: European Union Agency for Network and Information Security (ENISA) Ziel dieses Berichtes ist es, die Entwicklung von CSIRTs ( <i>Computer Security Incident Response Team</i> ), ISACs ( <i>Information Sharing and Analysis Center</i> ) sowie relevante Initiativen zum Informationsaustausch über Cyber-Security Incidents <u>im Energiesektor</u> zu verstehen und zu erlernen. Sie konzentriert sich auf die in der NIS-Richtlinie (European Parliament and Council, 2016: Netz und Informationssicherheit) identifizierten Teilsektoren Strom, Öl und Gas.
<b>Communication network dependencies for IKS/SCADA Systems</b>	2017	Hrsg.: European Union Agency for Network and Information Security (ENISA) Dieser Bericht konzentriert sich auf die Aspekte der Kommunikationsnetze und der Interkommunikation zwischen IKS/SCADA und der Erkennung von Schwachstellen, Risiken, Bedrohungen und Sicherheitsauswirkungen, die durch cyber-physikalische Systeme verursacht werden können. Der Bericht enthält auch eine Reihe von Empfehlungen zur Minderung der identifizierten Risiken. Das wichtigste Ergebnis der vorgängigen Studie ist eine Liste von bewährten Praktiken und Richtlinien, um die Angriffsfläche von IKS/SCADA-Systemen soweit wie möglich zu begrenzen. Das Hauptziel des Dokumentes ist es, einen Einblick in die Kommunikationsnetzwerkabhängigkeiten der IKS/SCADA-Systeme zu geben sowie kritische Sicherheitsressourcen und realistische Angriffsszenarien und Bedrohungen gegen diese Kommunikationsnetze zu identifizieren.



Titel	Jahr	Herausgeber & Beschreibung
<b>VDI/VDE 2182</b> <b>Informationssicherheit in</b> <b>der industriellen Automati-</b> <b>sierung</b>	2011 - 2020	<p>Hrsg.: Verein Deutscher Ingenieure (VDI) / Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE)</p> <p>Diese Richtlinie beschreibt, wie die Informationssicherheit von automatisierten Maschinen und Anlagen durch die Umsetzung von konkreten Schutzmassnahmen erreicht werden kann. Dazu werden Aspekte der eingesetzten Automatisierungsgeräte, -systeme und -anwendungen betrachtet. Auf der Basis einer zwischen Herstellern von Automatisierungsgeräten und -systemen und deren Nutzern (z.B. Maschinenbauern, Integratoren, Betreibern) abgestimmten gemeinsamen Begriffsdefinition wird eine einheitliche, praktikable Vorgehensweise beschrieben, wie Informationssicherheit im gesamten Lebenszyklus von Automatisierungsgeräten, -systemen und -anwendungen gewährleistet werden kann. Der Lebenszyklus berücksichtigt die Phasen der Entwicklung, Integration, des Betriebs, der Migration und Ausserbetriebsetzung. Die Richtlinie definiert ein einfaches Vorgehensmodell zur Bearbeitung und Darstellung der Informationssicherheit. Das Modell besteht aus mehreren Prozessschritten.</p>

