Änderungen bitte im Änderungsmodus (Tracking) verfassen.
Geänderte Versionen bitte per Mail senden an: vds10100-feedback [at] vds-nis2.de

Feedback welcome!

ToDo’s, Diskussionen und mehr – so geht’s!

Sie sind herzlich dazu eingeladen, uns Feedback zu geben. Wo gibt es Fehler? Was meinen Sie zu noch strittigen Strukturen und Maßnahmen? Gibt es Formulierungen, die kürzer, besser oder passender gefasst werden können? Nutzen Sie den Überarbeitungsmodus Ihres Textprogramms und geben Sie uns Feedback!
Hinweis: In diesem Dokument sind die Texte in Tabellenform organisiert. In der mittleren Spalte finden sich häufiger die Schlüsselwörter „ToDo“ und „Diskussion“. Besonders an diesen Stellen benötigen wir Ihr Feedback!

Vorbemerkung

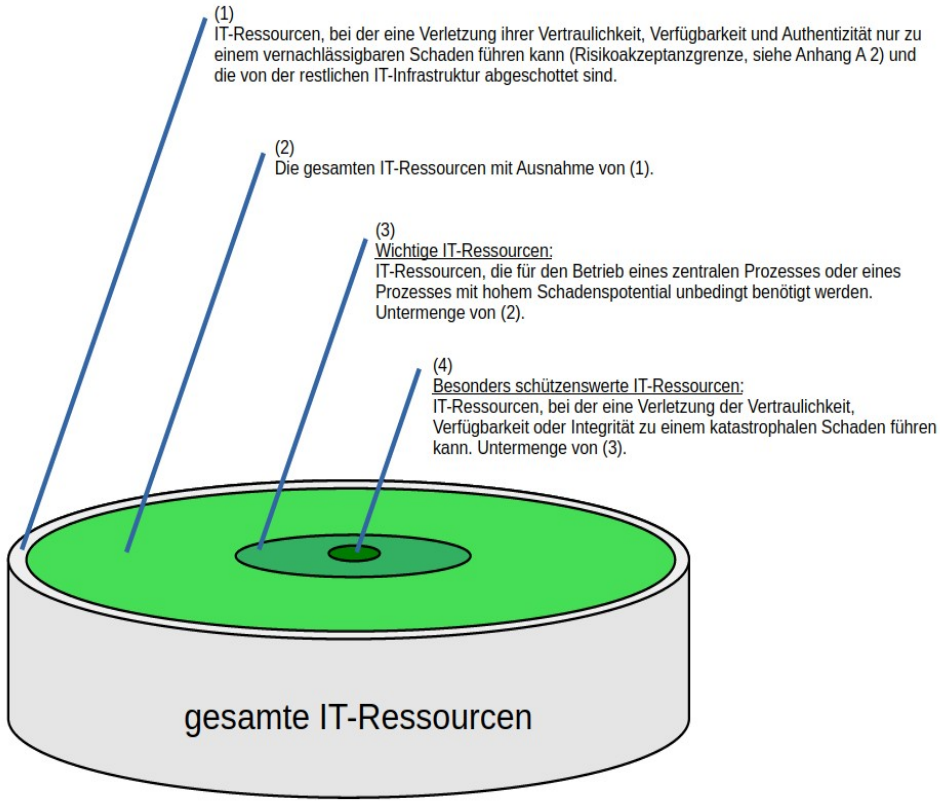
Der Aufwand für die Umsetzung gängiger Regelwerke wird z. B. dadurch begrenzt, dass ihr Geltungsbereich festgelegt werden kann. Das ist im Rahmen der Umsetzung von NIS-2 nicht möglich; die betroffenen Organisationen sind verpflichtet, ihre „informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen“ durch entsprechende „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen“ abzusichern (§ 30 Abs. 1 Satz 1). Die Erklärung im Entwurf des NIS2UmsuCG stellt klar, dass „der Begriff „Erbringung ihrer Dienste“ (…) weit gefasst (ist) und insbesondere nicht mit der Erbringung (kritischer) Versorgungsdienstleistungen zu verwechseln (ist). Vielmehr sind die hier gemeinten Dienste sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch Büro-IT oder andere IT-Systeme, die durch die Einrichtung betrieben werden.“ Wir reagieren auf diese Vorgabe, indem in Abschnitt 1.2 der VdS 10100 (Anwendungs- und Geltungsbereich) festgelegt ist, dass die Richtlinien für die gesamte Organisation umzusetzen sind.

Im Gesetzestext wird betont, dass bei der Auswahl der technischen und organisatorischen Maßnahmen „das Ausmaß der Risikoexposition die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen“ sind (§ 30 Abs. 1 Satz 2). Diese Formulierung ermöglicht es, den Aufwand für die Umsetzung von NIS-2 zu minimieren, ohne den Geltungsbereich einzuschränken.

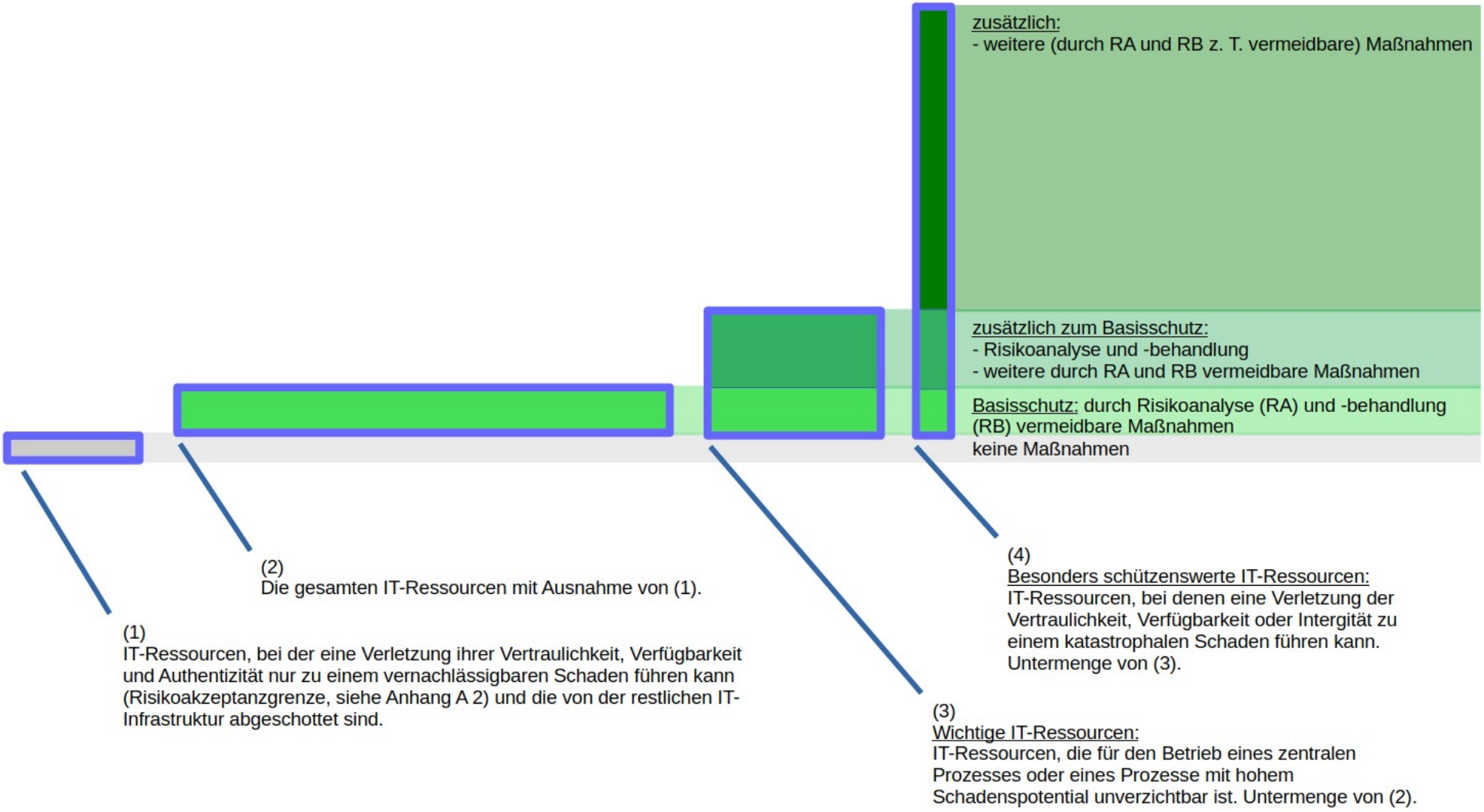
Vorgehensweise der VdS 10100

Die VdS 10100 unterteilt die IT-Ressourcen in vier Kategorien, wobei für die Einteilung allein die mögliche Schadenshöhe beim Eintritt eines Sicherheitsvorfalls (Bruch der Vertraulichkeit, Verfügbarkeit und/oder Integrität) verwendet wird:

Schutz-kategorie	Kriterien
(1) ohne Bezeichnung / „unwichtig“	IT-Ressource, bei der ein Sicherheitsvorfall nur zu einem vernachlässigbaren Schaden führen kann (Risikoakzeptanzgrenze, siehe Anhang A 2) und die von der restlichen IT-Infrastruktur abgeschottet ist.
(2) ohne Bezeichnung / „standard“ / „basis“	Die gesamten IT-Ressourcen mit Ausnahme von (1).
(3) “wichtig“	IT-Ressourcen, die für den Betrieb eines zentralen Prozesses oder eines Prozesses mit hohem Schadenspotential (siehe Abschnitt 9.1) oder für die Datensicherung unbedingt benötigt werden. Untermenge von (2).
(4) „kritisch“	IT-Ressourcen, die kritische Informationen (siehe Abschnitt 9.2) verarbeiten, speichern oder übertragen oder die für den Betrieb von kritischen IT-Ressourcen zwingend benötigt werden. Untermenge von (3).



Für die einzelnen Kategorien sind aufeinander aufbauende Sicherheitsmaßnahmen definiert, deren Umsetzungsaufwand mit der Bedeutung der IT-Ressourcen zunimmt.



Übersicht: Welche Maßnahmen für welche Schutzkategorien?

Art der Maßnahme	Beschreibung
verpflichtend	Diese Maßnahmen sind verpflichtend. Sie können nicht vermieden werden.
vermeidbar	Die Organisation kann sich gegen die (vollständige) Implementierung der Maßnahme entscheiden. In diesem Fall muss dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

Abschnitt	technische Maßnahme (Stichwort)	Schutzkategorien		
		„standard“	wichtig	kritisch
10.1 IT-Systeme → Inventarisierung	„Schutzkategorie“ des IT-Systems in Inventarisierung aufnehmen	verpflichtend	verpflichtend	verpflichtend
10.2.1 IT-Systeme → Inbetriebnahme und Änderung	Schutzkategorie des IT-Systems ermitteln	verpflichtend	verpflichtend	verpflichtend
10.3 IT-Systeme → Basisschutz	Software (vertrauenswürdige Quelle und Updates)	vermeidbar	vermeidbar	vermeidbar
	Beschränkung des Netzwerksverkehrd für verwundbare IT-Systeme	vermeidbar	vermeidbar	vermeidbar
	Protokollierung	vermeidbar	vermeidbar	vermeidbar
	Schutz vor Schadsoftware	vermeidbar	vermeidbar	vermeidbar
	Starten von fremden Medien verhindern	vermeidbar	vermeidbar	vermeidbar
	Authentifizierung	vermeidbar	vermeidbar	vermeidbar
	Zugänge und Zugriffsrechte	vermeidbar	vermeidbar	vermeidbar
10.n1 IT-Systeme → Zusätzliche Maßnahmen für wichtige IT-Systeme	individuelle Risikoanalyse und -behandlung		verpflichtend	verpflichtend
	Dokumentation		vermeidbar	vermeidbar
	Datensicherung		vermeidbar	vermeidbar
	Überwachung		vermeidbar	vermeidbar
10.5 IT-Systeme → Zusätzliche Maßnahmen für kritische IT-Systeme	keine Entwicklungen oder Tests			vermeidbar
	abschalten aller nicht benötigten Dienste			vermeidbar
	abschalten aller nicht benötigten externen Schnittstellen und Laufwerke			vermeidbar
	Änderungen in Testumgebung testen			vermeidbar
	Roll-back-Mechanismus			vermeidbar

Abschnitt	technische Maßnahme (Stichwort)	Schutzkategorien		
		„standard“	wichtig	kritisch
	vorhalten von Ersatzsystemen oder -verfahren			vermeidbar
	sicherstellen, dass kritische Individualsoftware auch in Zukunft verwendet und angepasst werden kann			vermeidbar
11.4 Netzwerke und Verbindungen → Basisschutz	Dauerhaft nicht genutzte Netzwerkanschlüsse deaktivieren	vermeidbar	vermeidbar	vermeidbar
	Segmentierung	vermeidbar	vermeidbar	vermeidbar
	Fernzugang absichern	vermeidbar	vermeidbar	vermeidbar
	Kopplung von Netzwerken absichern	vermeidbar	vermeidbar	vermeidbar
11.5 Netzwerke und Verbindungen → Zusätzliche Maßnahmen für wichtige Verbindungen	Risikoanalyse und -behandlung		verpflichtend	verpflichtend
12.2 Mobile Datenträger → Schutz der Informationen	Risikoanalyse für den Einsatz von Kryptografie	verpflichtend	verpflichtend	verpflichtend
12.3 Mobile Datenträger → Zusätzliche Maßnahmen für wichtige mobile Datenträger	Risikoanalyse und -behandlung		verpflichtend	verpflichtend
13.1 Umgebung → Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen	Schutz vor Beschädigung und unberechtigtem Zutritt	verpflichtend	verpflichtend	verpflichtend
13.2 Umgebung → Datenleitungen	Schutz vor Beschädigung	verpflichtend	verpflichtend	verpflichtend
13.3 Umgebung → Zusätzliche Maßnahmen für wichtigen IT-Systeme	Risikoanalyse und -behandlung der Bedrohungen ungeeignete Umgebungsbedingungen, negative Umwelteinflüsse, unzuverlässige Stromversorgung, Beschädigung und Verlust, unautorisierter Zutritt, Ausspähen vertraulicher Informationen		verpflichtend	verpflichtend
14.2 IT-Outsourcing und Cloud Computing → Vorbereitung	Ermitteln der betrieblichen, gesetzlichen und vertraglichen Bestimmungen, insbesondere in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität der ausgelagerten IT-Ressourcen.	verpflichtend	verpflichtend	verpflichtend
14.3 IT-Outsourcing und Cloud Computing → Vertragsgestaltung	Vertrag mit Anbieter gem. 14.2 schließen.	verpflichtend	verpflichtend	verpflichtend
14.4 IT-Outsourcing und Cloud Computing → Zusätzliche Maßnahmen für wichtige IT-Ressourcen	erhöhte Anforderungen an den zu schließenden Vertrag		noch unklar	noch unklar
15.1 Zugänge und Zugriffsrechte → Verwaltung	Zugänge und Zugriffsrechte strukturiert verwalten	verpflichtend	verpflichtend	verpflichtend

Abschnitt	technische Maßnahme (Stichwort)	Schutzkategorien		
		„standard“	wichtig	kritisch
15.2 Zugänge und Zugriffsrechte → Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen	Alle Zugänge und Zugriffsrechte müssen jährlich erfasst und überprüft werden, ob sie gem. 15.1 verwaltet wurden.			verpflichtend
16.5 Datensicherung → Basisschutz	Absichern der IT-Systeme für die Datensicherung und -wiederherstellung	vermeidbar	vermeidbar	vermeidbar
	Datensicherung der Speicherorte	vermeidbar	vermeidbar	vermeidbar
	Datensicherung der Server	vermeidbar	vermeidbar	vermeidbar
	Datensicherung der aktiven Netzwerkkomponenten	vermeidbar	vermeidbar	vermeidbar
	Datensicherung der mobilen IT-Systeme	vermeidbar	vermeidbar	vermeidbar
16.6 Datensicherung → Zusätzliche Maßnahmen für wichtige IT-Systeme	Risikoanalyse: Folgen eines Datenverlusts analysieren und MTD bestimmen		verpflichtend	verpflichtend
	Zusätzliche Anforderungen an die Verfahren (MTA und MTD)		verpflichtend	verpflichtend
17.4 Sicherheitsvorfälle → Zusätzliche Maßnahmen für wichtig IT-Systeme	Wiederanlaufpläne		verpflichtend	verpflichtend
	Abhängigkeiten erfassen		verpflichtend	verpflichtend
18.2 Wichtige Lieferanten	Basisschutz IT-Systeme, Netzwerke, Datensicherung, Wiederanlaufpläne		vermeidbar	vermeidbar
18.3 Kritische Lieferanten	ISMS			vermeidbar

VdS 10100, Version 0.5.8 vom 24.09.2024

0 VdS-Richtlinien für die Informationsverarbeitung

Strukturierte Informationssicherheit gemäß NIS-2

Inhaltsverzeichnis

Anforderungen

Kommentar / ToDo	VdS 10100
übernehmen	Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

1 Allgemeines

Kommentar / ToDo	VdS 10100
ToDo für 0.6: Muss neu verfasst werden.	
Angepasst.	Die vorliegenden Richtlinien legen Mindestanforderungen fest und beschreiben Maßnahmen für die Umsetzung einer strukturierten Informationssicherheit gemäß der EU-Richtlinie NIS-2.

1.1 Anwendungshinweise

Kommentar / ToDo	VdS 10100
0.4.3-Verbesserungsvorschlag/Diskussion: „bei der objektive Nachweise für die Umsetzung der Maßnahmen geprüft werden „ hinzugefügt.	Die vorliegenden Richtlinien sind Grundlage für eine Zertifizierung durch VdS Schadenverhütung, bei der objektive Nachweise für die Umsetzung der Maßnahmen geprüft werden.
übernehmen 0.4.2 – ToDo: Prüfen ob die entsprechenden VdS-Richtlinien für die VdS 10100 gültig sind bzw. die gleiche Rolle wie für die VdS 10k besitzen.	Die Umsetzung der geforderten Maßnahmen bedingt Fachwissen und Erfahrung auf den Gebieten der Informationssicherheit und der Managementsysteme. Sind diese Kenntnisse nicht in ausreichendem Maß vorhanden, empfiehlt sich die Inanspruchnahme qualifizierter Dienstleister die ein Anerkennungsverfahren gemäß VdS 3477 bzw. VdS 10003 durchlaufen haben.
übernehmen	Verpflichtende Maßnahmen sind durch die Schlüsselworte MUSS/MÜSSEN, DARF NICHT/DÜRFEN NICHT/DÜRFEN KEINE gekennzeichnet, empfohlene Maßnahmen durch die Schlüsselworte SOLLTE/SOLLTEN, SOLLTE NICHT/SOLLTEN NICHT, KANN/KÖNNEN, DARF/DÜRFEN.
übernehmen	*Diese Richtlinien SOLLTEN in bestehende Managementsysteme, insbesondere in das Qualitätsmanagement und in das Risikomanagement integriert werden, um potentielle Synergieeffekte zu nutzen.*
ToDo für 0.6: Formulierung überarbeiten: - Die Erkenntnisse und Strukturen der VdS 10010 unterstützen die Umsetzung der VdS 10100.	Sie stützen sich auf die Strukturen und Maßnahmen der VdS 10000, deren Umsetzung empfohlen jedoch nicht notwendigerweise Voraussetzung für das erfolgreiche Implementieren dieser Richtlinien sind.

	Diese Richtlinie referenziert auf die VdS-Richtlinie 10000 (VdS 10000), sie KANN jedoch auch auf Basis anderer ISMS umgesetzt werden, sofern die entsprechenden Anforderungen dadurch erfüllt werden.
	Um Wiederholungen zu vermeiden wird wenn angebracht im Text dieser Richtlinie auf die entsprechenden Abschnitte der VdS 10000 verwiesen.
übernehmen	Aus Gründen der leichteren Lesbarkeit wird in diesen Richtlinien auf eine geschlechtsspezifische Differenzierung, wie z. B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form verwendet. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten.

1.2 Anwendungs- und Geltungsbereich

Kommentar / ToDo	VdS 10100
angepasst	Diese Richtlinie ist für Organisationen anwendbar, die als „wichtige“ oder „besonders wichtige“ Einrichtungen im Sinne des BSIG gelten oder gelten könnten.
ergänzt/neu	Sie ist nicht für Betreiber kritischer Anlagen im Sinne des BSIG geeignet.
Gem. NIS-2 muss der Anwendungsbereich die gesamte Organisation umfassen.	Die Richtlinie MUSS auf die gesamte Informationsverarbeitung der Organisation angewendet werden.

1.2.1 Analyse und Registrierung

In diesem neuen Abschnitt werden folgende Vorgaben des BSIG umgesetzt:
- § 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen
- § 33 Registrierungspflicht
- § 34 Besondere Registrierungspflicht für bestimmte Einrichtungsarten

Kommentar / ToDo	VdS 10100
§ 28 ist komplex und sehr detailliert. Deshalb sind die Vorgaben nicht einfach in eine Richtlinie zu übersetzen: - Wenn sie abgebildet werden müssen sie vollständig und korrekt wiedergegeben werden. Eine genaue Abbildung wäre eine 1:1 Wiederholung des Gesetzestextes und deshalb nicht sinnvoll. Das BSI wird eine entsprechende Prüfung online zur Verfügung stellen. Wir verweisen auf diese.	Die Organisation MUSS prüfen, ob sie als „wichtige“ oder „sehr wichtige“ Einrichtung im Sinne von § 28 BSIG gilt. Dazu SOLLTE die entsprechende vom BSI zur Verfügung gestellte Vorgehensweise genutzt werden.
	Das Ergebnis der Prüfung MUSS zusammen mit seiner Begründung dokumentiert werden.
§ 33 Abs. 1	Es MUSS ein Verfahren etabliert werden, das sicherstellt, dass das entsprechende Registrierungsverfahren gem. BSIG § 33 innerhalb von drei Monaten durchlaufen wird.

- Verbessern: „innerhalb von drei Monaten“ → nach welchem Zeitpunkt?!	
§ 33 Abs. 5	Das Verfahren MUSS sicherstellen, dass geänderte Angaben spätestens zwei Wochen ab ihrer Kenntnis an das BSI übermittelt werden.
§ 34	Das Verfahren MUSS prüfen, ob die Organisation eine Einrichtung im Sinne von § 64 Absatz 1 Satz 1 ist. Wenn die Organisation eine Einrichtung im Sinne von § 64 Absatz 1 Satz 1 ist, MUSS das Verfahren sicherstellen, dass die besondere Registrierungspflicht erfüllt und die in § 34 geforderten Informationen an das BSI übermittelt werden. Hierzu MUSS der entsprechende Meldeweg des BSI genutzt werden.

1.3 Gültigkeit

Kommentar / ToDo	VdS 10100
0.5.7-ToDo für Version 0.9.99–: anpassen	Diese Richtlinien gelten ab dem 01.11.2024

2 Normative Verweise

Kommentar / ToDo	VdS 10100
übernehmen	Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils zuletzt veröffentlichte Fassung.
übernehmen	BSI-Standard 200-4 Notfallmanagement
Wir verweisen auf dieses Regelwerk in Abschnitt A 2.2 Risikoanalyse.	ISO 31000 Risk Management – Principles and guidelines
Wir verweisen auf dieses Regelwerk in Abschnitt A 2.2 Risikoanalyse.	ISO/IEC 27005 Information technology — Security techniques — Information security risk management
Wir verweisen auf dieses Regelwerk in Anhang A 2.1 Methodik.	IEC 31010:2019 - Risk assessment techniques
Wir verweisen auf dieses Regelwerk in Abschnitt 1.1 (Anwendungshinweise).	VdS 10000 - Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU)
Wir verweisen auf dieses Regelwerk in Anhang A 2.2 Risikoanalyse.	ENISA Thread Taxonomy

Wir verweisen auf dieses Regelwerk in Anhang A 2.2 Risikoanalyse.	„Elementare Gefährdungen“, BSI
Wir verweisen auf diese Aufstellung an verschiedenen Stellen in Kapitel 10 und 11 (Kryptografie).	BSI TR-02102-1 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf)

3 Begriffe

ToDo für Version 0.8: Begriffe aus NIS-2 im Laufe der Entwicklung in dieses Kapitel aufnehmen und jene Begriffe entfernen, die in der VdS 10100 nicht neu definiert werden müssen. Low Prio.

Sofern hier nicht anders definiert MÜSSEN die Begriffe gemäß Kapitel 3 der VdS 10000 verwendet werden.

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
1	**Administrativer Zugang:** Zugang, der einen Nutzer dazu befähigt, ein IT-System zu verwalten, d. h. der einem Nutzer umfangreiche Rechte in einem IT-System einräumt.		
D2	**Administrator:** Person, die für Einrichtung, Betrieb, Überwachung und/oder Wartung eines IT-Systems oder Netzwerks zuständig ist.		
D3	**Aktive Netzwerkkomponente:** Netzwerkkomponente, die über eine eigene Logik verfügt, wie z. B. Hub, Switch, Repeater, Bridge, Medienkonverter, Gateway, Firewall usw. Eine aktive Netzwerkkomponente benötigt in aller Regel eine Stromversorgung. Eine aktive Netzwerkkomponente ist ein IT-System.		
4	**Archivierung:** Entfernen aus der operativen Umgebung und Langzeitspeicherung bis zum Erreichen der Aufbewahrungsfrist.		
D5	**Aufgabe:** Dauerhaft wirksame Aufforderung an Handlungsträger, festgelegte Handlungen wahrzunehmen.		
D6	**Ausfall:** Erliegen eines Prozesses, weil notwendige Ressourcen nicht in ausreichender Menge und/oder		

	in ausreichender Qualität zur Verfügung stehen.		
7	**Authentizität:** Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit.		
D8	**Authentifizierungsmerkmal:** Merkmal, mit dessen Hilfe eine anfragende Instanz ihre Identität nachweisen kann. Authentifizierungsmerkmale können Wissen (z. B. Passwort oder PIN), Besitz (z. B. Chipkarte oder Token) oder biometrische Merkmale (z. B. Fingerabdruck oder Iris) sein.		
D9	**Bedrohung:** Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.		
D10	**Business Continuity Management (BCM):** Ganzheitlicher Managementprozess für die systematische Vorbereitung auf das Bewältigen von Schadenereignissen mit dem Ziel, zentrale Geschäftsprozesse auch beim Eintreten von Notfällen, Krisen oder Katastrophen weiter zu betreiben, bzw. schnellstmöglich wieder in Gang zu setzen.		
11	**Cloud Computing:** Technologie, die es erlaubt über ein Netz auf einen geteilten Pool von konfigurierbaren IT-Ressourcen zuzugreifen.		
D12	**Daten:** Gebilde aus Zeichen, die aufgrund bekannter Abmachungen Informationen darstellen.		
D13	**Datenleitung:** Physisches Medium, über das Daten ausgetauscht werden können.		
		0.2.1: Begriff neu aufgenommen. Wenn in VdS 10k verwendet, Definition auch in die VdS 10k aufnehmen	**Dienst:** Eine von IT-Systemen bereitgestellte Funktionalität oder Leistung, die Nutzern zur Verfügung steht und bestimmte Aufgaben oder Funktionen erfüllt.
14	**Echtzeitbetrieb:** Elektronische Datenverarbeitung, die (nahezu) simultan mit den entsprechenden Prozessen in der Realität abläuft.		

D14.1	**Eigenmächtigkeit:** Handeln ohne Auftrag, Erlaubnis oder Befugnis. Diese Formulierung wird wahrscheinlich in zukünftige Versionen der VdS 10000 aufgenommen werden.		
D15	**Externer:** Natürliche Person, die kein Mitarbeiter ist. Externe sind z. B. Geschäftspartner oder Gäste.	I	
16	**Funktion:** Bündel von Aufgaben, durch die ein Teil der Ziele der Organisation erreicht werden soll.		
D17	**Gefahr:** Möglichkeit einer Schadwirkung auf ein zu schützendes Objekt.		
D18	**Gefährdung:** Bedrohung, die konkret über eine Schwachstelle auf ein zu schützendes Objekt einwirkt (Bedrohung plus Schwachstelle).		
19	**Information:** Sinn und Bedeutung, die der Empfänger aus erhaltenen Daten interpretiert.		
D20	**Informationssicherheit:** Schutz von Informationen hinsichtlich gegebener Sicherheitsanforderungen (bspw. Vertraulichkeit, Verfügbarkeit oder Integrität).		
D21	**Informationssicherheitsbeauftragter (ISB):** Person, die die Aufgaben gem. Abschnitt 4.3 wahrnimmt.		
22	**Informationssicherheitsteam (IST):** Gremium, das die Aufgaben gem. Abschnitt 4.4 wahrnimmt.		
D23	**Informationstechnik (IT):** Oberbegriff für die Informations- und Datenverarbeitung sowie –übertragung inklusive der dafür benötigten Hard- und Software.		
D24	**Integrität:** Korrektheit und Unversehrtheit von Informationen bzw. die korrekte Funktionsweise der Datenverarbeitung.		
25	**Inventarisierung:** Bestandsaufnahme zu einem definierten Zeitpunkt.		
D26	**IS-Leitlinie:** Leitlinie zur Informationssicherheit, die die Anforderungen gem. Kapitel 5 erfüllt.		
D27	**IS-Richtlinie:** Sammlung von Regelungen zur Informationssicherheit, die die Anforderungen gem. Kapitel 6 erfüllt.		

28	**IT-Infrastruktur:** Alle langlebigen Einrichtungen materieller und institutioneller Art für den Betrieb von Anwendungssoftware.		
D29	**IT-Ressource:** Betriebsmittel für die elektronische Informationsverarbeitung. Hierzu zählen u. a. IT-Systeme, Datenträger, Verbindungen, Daten, Informationen sowie Mitarbeiter.		
D30	**IT-Verantwortlicher:** Leiter der IT-Abteilung, bzw. das für die Informationstechnik zuständige Management.		
31	**IT-Outsourcing:** Auslagerung von IT-Aufgaben an einen von der Organisation rechtlich unabhängigen Anbieter.		
D32	**IT-System:** Technische Anlage, die der Informationsverarbeitung dient und eine abgeschlossene Funktionseinheit aus Hard- und Software bildet. Typische IT-Systeme sind z. B. Server (physisch und virtuell), Clients, Drucker, Mobiltelefone, Smartphones, Telefonanlagen, Laptops, Tablets und aktive Netzwerkkomponenten.		
D33	**Katastrophaler Schaden:** Schaden, auf den eines der folgenden Kriterien zutrifft:		
33.1	1. Auswirkungen auf Leib und Leben von Personen: Es werden Menschen schwer verletzt oder kommen ums Leben.		
D33.2	2. Auswirkung auf zentrale Prozesse: Zentrale Prozesse der Organisation werden zum Erliegen gebracht und die Rückkehr zum Regelbetrieb ist (innerhalb eines akzeptablen Zeitraums) nicht möglich.		
D33.3	3. Auswirkung auf zentrale Werte: Zentrale Werte der Organisation gehen verloren oder werden zerstört und ihre Wiederherstellung ist (mit den Ressourcen der Organisation) nicht mehr möglich.		
33.4	4. Auswirkungen auf die Rechtskonformität: Gesetze, Verträge oder Normen werden gebrochen und die daraus resultierende Haftung ist für die Organisation		

	oder für die Verantwortlichen ruinös.		
D34	**Kritische Individualsoftware:** Software, die für den Betrieb von kritischen IT-Systemen zwingend benötigt wird und individuell für die Organisation erstellt oder angepasst wurde.		
D35	**Kritische Informationen:** Informationen, die die Bedingungen gem. Abschnitt 9.2 erfüllen.		
D36	**Kritisches IT-System:** IT-System, das die Bedingungen gem. Abschnitt 9.3 erfüllt.		
37	**Kritischer mobiler Datenträger:** Mobiler Datenträger, der die Bedingungen gem. Abschnitt 9.3 erfüllt.		
D38	**Kritische Verbindung:** Verbindung, die die Bedingungen gem. Abschnitt 9.3 erfüllt.		
D39	**Leitlinie:** Dokument des Topmanagements, das ein Ziel der Organisation und seine Priorität definiert sowie Verantwortlichkeiten zu seiner Erreichung festlegt.		
D40	**Maximal tolerierbare Ausfallzeit (MTA):** Zeit, bis zu der eine definierte Leistung (z. B. ein Notbetriebsniveau) wieder verfügbar sein muss.		**Maximal tolerierbare Ausfallzeit (MTA):** Zeit, bis zu der eine definierte Leistung (z. B. ein Notbetriebsniveau) wieder verfügbar sein muss, weil ansonsten ein katastrophaler oder nicht zu tolerierender Schaden entstehen kann.
D41	**Maximal tolerierbarer Datenverlust (MTD):** Zeitspanne, die als noch akzeptierbar für einen Datenverlust erachtet wird.		
D41.1	**Mehr-Faktor-Authentifizierung:** Nachweis der Identität mit Hilfe von mehreren unabhängigen Merkmalen.		
42	**Mitarbeiter:** Natürliche Person, die in einem Vertragsverhältnis oder in einem öffentlich-rechtlichen Dienst- und Treueverhältnis mit der Organisation steht und eine oder mehrere Positionen in der Organisation einnimmt. Mitarbeiter sind z. B. Angestellte, Arbeiter, Beamte, freier Mitarbeiter, Dienstleister oder deren Mitarbeiter bzw.		

	Erfüllungsgehilfen.		
D43	**Mobiler Datenträger:** Datenträger, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile Datenträger sind z. B. Speichersticks und –karten sowie externe Festplatten, aber auch Speichermedien wie CD-ROMs, DVDs und Disketten.		
D44	**Mobiles IT-System:** IT-System, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile IT-Systeme sind z. B. Notebooks, Smartphones, Tablets oder Digitalkameras.		
45	**Netzwerkkomponente:** Technische Anlage, die der Weiterleitung von Daten dient. Es werden aktive und passive Netzwerkkomponenten unterschieden.		
D46	**Netzübergang:** Schnittstelle zwischen zwei unterschiedlichen Netzwerken. Dabei können sich die Netzwerke durch die physikalischen Übertragungsmedien, durch die verwendeten Protokolle oder durch eine unterschiedliche administrative Hoheit voneinander unterscheiden.		
D47	**Notbetrieb:** Auf ein Minimum reduzierte Funktionstüchtigkeit, mit der ein Prozess aufrechterhalten werden kann.		
48	**Notbetriebsniveau:** Definition, welche Funktionen von einer IT-Ressource erbracht werden müssen, damit ein Notbetrieb aufrechterhalten werden kann.		
D49	**Organisationseinheit:** Einheit, in der artverwandte (Teil-)Aufgaben oder Tätigkeiten zusammengefasst sind.		
50	**Passive Netzwerkkomponente:** Netzwerkkomponente ohne eigene Logik, z. B. Kabel, Patchfeld, Dose, Stecker usw. Eine passive Netzwerkkomponente benötigt in aller Regel keine Stromversorgung.		
D51	**Position:** Platz, den ein Mitarbeiter in der Hierarchie einer Organisation einnimmt.		

D52	**Projektverantwortlicher:** Person, die für die ordnungsgemäße Durchführung eines Projekts verantwortlich ist.		
53	**Prozess:** System von Tätigkeiten, das Eingaben mit Hilfe von Ressourcen in Ergebnisse umwandelt.		
D54	**Prozess mit hohem Schadenspotential:** Prozess, bei dessen Fehlfunktion oder kurzzeitigem Ausfall ein katastrophaler Schaden entstehen kann. Typische Prozesse mit hohem Schadenspotential sind z. B. die Datensicherung und -wiederherstellung.	Satz „Typische Prozesse mit hohem Schadenspotential sind z. B. die Datensicherung und -wiederherstellung.“ hinzugefügt. In VdS 10k aufnehmen.	
D55	**Prozessverantwortlicher:** Person, die inhaltlich für einen oder mehrere Prozesse verantwortlich ist. Sie besitzt den Überblick über die für diese Prozesse benötigten Ressourcen und über die an sie gestellten Anforderungen.		
D56	**Regelung:** Verbindliche Vorgabe.		
D57	**Ressource:** Betriebsmittel, das der Organisation gehört oder ihr zur Verfügung steht.		
D58	**Risiko:** Eine nach Eintrittswahrscheinlichkeit und Schadenshöhe bewertete Gefährdung.		
D59	**Schnittstelle:** Teil eines IT-Systems, das der Kommunikation dient, wie z. B. Ethernet- und Wireless-LAN-Adapter, ISDN-Karten, Modems, USB-Ports, NFC- und Infrarot-Schnittstellen, SD-Slots oder Tastaturen.		
D60	**Schwachstelle:** Umstand, der es ermöglicht, dass eine Bedrohung mit einem zu schützenden Objekt räumlich und/oder zeitlich zusammentreffen kann.		
D61	**Server:** Zentrales IT-System, über das funktionale und/oder infrastrukturelle Netzdienste realisiert werden.		
D61.1	**Sicherheit:** Die Abwesenheit nicht beherrschbarer Gefahren. Eine vollständige Sicherheit kann in der Praxis nicht erreicht werden. Das angemessene Maß an Sicherheit muss deshalb von den beteiligten Parteien definiert und fortlaufend an die Erfordernisse		

	und die Umgebungsbedingungen angepasst werden. (Diese Formulierung wird wahrscheinlich in einer zukünftigen Version der VdS 10000 aufgenommen werden.)		
D62	**Sicherheitsvorfall:** Unerwünschtes Ereignis, das Auswirkungen auf die Informationssicherheit hat und große Schäden nach sich ziehen kann. Was genau als Sicherheitsvorfall eingestuft wird, wird von der Organisation selbst definiert.	Version 0.8: prüfen, ob NIS-2-konform	Sicherheitsvorfall: Unerwünschtes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von IT-Systemen, Informationen, Ressourcen oder Diensten beeinträchtigt.
D63	**Speicherort:** Ort, an dem Nutzer bzw. Applikationen ihre Daten dauerhaft speichern. Bei einem Speicherort kann es sich um einen lokalen Speicherort (wie z. B. Verzeichnisse auf Servern oder Workstations), einen mobilen Speicherort (wie z. B. Smartphones oder Digitalkameras) oder um einen entfernt gelegenen Speicherort (wie z. B. ausgelagerte Server oder Cloud-Dienste) handeln.		
D64	**Störung:** Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als gering einzustufen. Die Beseitigung einer Störung kann im allgemeinen Tagesgeschäft vorgenommen werden.		
D65	**Systemsoftware:** Firmware, Betriebssystem und systemnahe Software. Systemsoftware verwaltet die internen und externen Hardwarekomponenten eines IT-Systems.		
D66	**Topmanagement:** Oberste Führungsebene, wie z. B. Vorstände, Geschäftsführer oder Behördenleiter.		
D67	**Verbindung:** Kanal, über den Daten ausgetauscht werden können.		
D68	**Verfahren:** Festgelegte Art und Weise, wie ein Prozess (oder auch eine einzelne Tätigkeit innerhalb eines Prozesses) auszuführen ist.		
D69	**Verfügbarkeit:** Eine Ressource kann wie vorgesehen genutzt werden.		
D70	**Vertraulichkeit:** Eigenschaft einer Information, nur für einen beschränkten Empfängerkreis vorgesehen		

	zu sein.		
D71	**Zentraler Prozess:** Prozess, der mitentscheidend für die Aufgabenerfüllung der Organisation ist. Dies kann z. B. ein Prozess für die Wertschöpfung oder für den Erhalt bzw. die Verbesserung der Wettbewerbsfähigkeit sein.		
D71.1	**Zentraler Wert:** Materieller oder immaterieller Wert, der für die Aufgabenerfüllung der Organisation (insbesondere für die Durchführung der zentralen Prozesse und für die Prozesse mit hohem Schadenspotential) unverzichtbar ist, wie z. B. Produktionsanlagen, Wissen, Mitarbeiter oder das Vertrauen von Kunden, Partnern oder Geldgebern in die Organisation.		
D72	**Zugang:** Einrichtung, die es erlaubt, die nichtöffentliche IT der Organisation zu nutzen.		
D73	**Zugriff:** Datenaustausch zwischen einer zugreifenden Instanz und einer IT-Ressource.		
D74	**Zutritt:** Umstand, der es ermöglicht, physisch mit einer IT-Ressource zu interagieren.		
		0.2.1: Begriff gem. NIS-2 definiert Alternative: Ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, teilweise oder vollständig zum Erliegen bringt.	**Erheblicher Sicherheitsvorfall:**Ein Sicherheitsvorfall, der schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursachen kann oder Dritte durch erhebliche materielle oder immaterielle Schäden beeinträchtigt oder beeinträchtigen kann.
		0.2.1: Wir verwenden in der VdS 10100 den Begriff „Organisation (gem. VdS 10000 / ISO 27001), NIS-2 spricht von „Einrichtungen“. Entsprechende Definitionen eingeführt	**Organisation:**Eine rechtlich verfasste Einheit wie ein Unternehmen, eine Behörde oder eine Institution, die strukturiert ist, um bestimmte Ziele zu verfolgen.
		0.2.1: Wir verwenden in der VdS 10100 den Begriff „Organisation (gem. VdS 10000 / ISO 27001), NIS-2 spricht von	**Einrichtung:** Organisation im Sinne von NIS-2, siehe Organisation

		„Einrichtungen“. Entsprechende Definitionen eingeführt	
		Entsprechende Definition In der VdS 10k anpassen.	**Sicherheitsvorfall:** Ungewöhnliches Ereignis, dass die Verfügbarkeit, Integrität und/oder Vertraulichkeit von Informationen oder der Informationsverarbeitung beeinträchtigt.
		0.5.7-DISKUSSION: Wird bisher nicht in der VdS 10100 verwendet.	**Stand der Technik:** Fortschrittliches, bereits praxiserprobtes Verfahren, das von Experten und Fachkreisen allgemein unterstützt und in professionellen Umgebungen eingesetzt wird.
		ToDo: Ergänzung zu „IT-Systemen“ – Anlagen sind IT-Systeme. 0.5.7-DISKUSSION: Wahrscheinlich stimmt dies nicht. Es ist nicht klar, was der Gesetzgeber konkret mit diesem Begriff meint. Allerdings scheint er nur im Zusammenhang mit der physischen Sicherheit verwendet zu werden (§ 30 Abs. 2 Punkt 8)	
		ToDo: Begriff „Lieferkette“ und/oder „Lieferanten“ aufnehmen.	

4 Organisation der Informationssicherheit

Kommentar / ToDo	VdS 10100
ToDo für 0.8: Text entwerfen, der auf NIS-2 abgestimmt ist. Low Prio.	

4.1 Verantwortlichkeiten

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

4.1.1 Zuweisung und Dokumentation

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

4.1.2 Funktionstrennungen

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

4.1.3 Zeitliche Ressourcen

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

4.1.4 Delegieren von Aufgaben

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

4.2 Topmanagement

Kommentar / ToDo	VdS 10100
NIS-2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS-2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.
§ 38 (1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.	Zusätzlich MUSS sich das Topmanagement dazu verpflichten, die in diesen Richtlinien geforderten Maßnahmen des Risikomanagements (siehe Anhang A2) umzusetzen und ihre Umsetzung zu überwachen.

4.3 Informationssicherheitsbeauftragter (ISB)

Kommentar / ToDo	VdS 10100
NIS-2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS-2 unerlässlich.	Das Topmanagement MUSS einen Informationssicherheitsbeauftragten (ISB) bestellen.#
	Dieser MUSS darauf hinwirken, dass die in der Leitlinie zur Informationssicherheit (IS-Leitlinie) definierten Ziele der Informationssicherheit erreicht werden.
	Hierfür MUSS er insbesondere die folgenden Verantwortlichkeiten wahrnehmen:
0.4.2: Risikomanagement erwähnt und gestärkt 0.4.2: Aufbau verbessert, Verständlichkeit erhöht. 0.4.4: Formulierung verbessert.	1. Steuern, Koordinieren und Prüfen der technischen und organisatorischen Maßnahmen und des Risikomanagements im Bereich der Informationssicherheit
	2. kontinuierliches Verbessern der Informationssicherheit, insbesondere des entsprechenden Risikomanagements
	3. Anpassen der Informationssicherheit an neue Bedrohungen, neue Schwachstellen und an neue gesetzliche, betriebliche und vertragliche Anforderungen
0.4.2: Risikomanagement erwähnt bzw. gestärkt	4. jährliches Berichten an das Informationssicherheitsteam (IST) über den aktuellen Stand der Informationssicherheit, insbesondere über Mängel, Risiken und Sicherheitsvorfälle sowie über den Stand des entsprechenden Risikomanagements

NIS-2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS-2 unerlässlich.	*Es SOLLTE sichergestellt werden, dass die Verantwortlichkeiten des ISB auch in seiner Abwesenheit wahrgenommen werden.*
	Dies KANN z. B. durch eine Stellvertreterregelung umgesetzt werden.

4.4 Informationssicherheitsteam (IST)

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

4.5 IT-Verantwortliche

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

4.6 Administratoren

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

4.7 Vorgesetzte

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

4.8 Mitarbeiter

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

4.9 Projektverantwortliche

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

4.10 Externe

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

5 Leitlinie zur Informationssicherheit (IS-Leitlinie)

Kommentar / ToDo	VdS 10100
NIS-2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS-2 unerlässlich.	Die Leitlinie zur Informationssicherheit (IS-Leitlinie) ist das zentrale Dokument für die gesamte Informationssicherheit. In ihr werden die zu erreichenden Ziele durch das Topmanagement vorgegeben und Verantwortlichkeiten definiert.

5.1 Allgemeine Anforderungen

Kommentar / ToDo	VdS 10100
MUSS, da Konzepte in Bezug auf die Informationssicherheit gefordert werden (§ 30 (2) Punkt 1).	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

5.2 Inhalte

Wenn Abschnitte 4.2 bis 4.10 verpflichtend werden, kann dieser Abschnitt auf eine Formulierung („Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.“) reduziert werden.

Kommentar / ToDo	VdS 10100
übernehmen	Die Leitlinie MUSS folgende Anforderungen erfüllen:
Anforderungen der VdS 10k plus Umsetzung von NIS-2 als Ziel.	1. Sie definiert die Ziele und den Stellenwert der Informationssicherheit in der Organisation, insbesondere die Umsetzung der EU-Richtlinie NIS-2.
Angepasst, da nicht alle Verantwortlichkeiten von VdS 10000 in der VdS 10100 benötigt werden	2. Sie definiert sämtliche erforderlichen Positionen für die Umsetzung dieser Ziele und weist auf deren Aufgaben hin.
übernehmen	*Die Leitlinie SOLLTE auf die Konsequenzen ihrer Nichtbeachtung hinweisen.*

6 Richtlinien zur Informationssicherheit (IS-Richtlinien)

Kommentar / ToDo	VdS 10100
übernehmen	Zur Unterstützung und Konkretisierung der IS-Leitlinie ist es notwendig, weitere Regelungen für die Informationssicherheit zu verabschieden und in einzelnen Dokumenten, den IS-Richtlinien, zu sammeln.

6.1 Allgemeine Anforderungen

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

6.2 Inhalte

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

6.3 Regelungen für Nutzer

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

6.4 Weitere Regelungen

Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

7 Mitarbeiter

Dieses Kapitel setzt § 30 (2) Punkt 9 um:

§ 30 (2) (…) Die Maßnahmen müssen zumindest Folgendes umfassen: (...)
9. Sicherheit des Personals (...)

Kommentar / ToDo	VdS 10100
übernehmen	Die Mitarbeiter sind ein zentraler Faktor für die Implementierung und Aufrechterhaltung der Informationssicherheit. Es ist deshalb notwendig, folgende Anforderungen der Informationssicherheit zu berücksichtigen.

7.1 Vor Aufnahme der Tätigkeit

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

7.2 Aufnahme der Tätigkeit

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

7.3 Beendigung oder Wechsel der Tätigkeit

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

8 Wissen

Kommentar / ToDo	VdS 10100
ToDo für Version 0.8: Text anpassen an NIS-2. Low Prio.	Viele Gefährdungen entstehen aus Unkenntnis oder mangelndem Problembewusstsein oder werden zumindest durch diese Faktoren verstärkt. Deshalb ist es notwendig, dass die Organisation über aktuelles Wissen in Bezug

	auf Informationssicherheit verfügt, die Mitarbeiter ihre Verantwortlichkeiten verstehen und für ihre Aufgaben geeignet und qualifiziert sind.

8.1 Aktualität des Wissens

Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

8.2 Schulung und Sensibilisierung

Kommentar / ToDo	VdS 10100
übernehmen	Es MUSS ein Verfahren (siehe Anhang A 1) für Schulungs- und Sensibilisierungsmaßnahmen implementiert werden, das folgende Punkte sicherstellt:
übernehmen	1. Sie werden regelmäßig sowie bei Bedarf durchgeführt.
übernehmen	2. Ihre Art und ihr Intervall werden zielgruppenorientiert festgelegt.
übernehmen	3. Sie vermitteln in ihrer Gesamtheit die Inhalte der IS-Leitlinie und sämtlicher für die Zielgruppe relevanter Regelungen zur Informationssicherheit (wie z. B. die Inhalte entsprechender IS-Richtlinien und Verfahren).
VdS 10000: „Störungen, Ausfällen und“ streichen, da wir die entsprechenden Kapitel zusammengelegt haben.	4. Sie klären über Gefährdungen auf und schulen den Umgang mit den vorhandenen Sicherheitsmaßnahmen sowie das Verhalten bei ~~Störungen, Ausfällen und~~ Sicherheitsvorfällen.
Änderung in der VdS 10000: „... technischen und organisatorischen Sicherheitsmaßnahmen...“ um zu verdeutlichen, dass die im RM identifizierten Maßnahmen gemeint sind	5. Sie vermitteln den Teilnehmern ihre Verantwortung für die Informationssicherheit und fördern bei ihnen die Akzeptanz der Sicherheitsmaßnahmen.
übernehmen	6. Ihre Inhalte und die Teilnahme an ihnen werden dokumentiert.
übernehmen	*Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN mit einer Lernerfolgskontrolle abschließen, um das Verständnis der Teilnehmer und den Bedarf weiterer Schulungs- oder Sensibilisierungsmaßnahmen zu ermitteln.*
übernehmen	*Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN von den Teilnehmern bewertet werden, um ihren Inhalt, ihre Form und ihren Ablauf zu verbessern.*
ToDo für 0.4: Gesetzestext ergänzen (Doku) § 38	Das Verfahren für Schulungs- und Sensibilisierungsmaßnahmen MUSS sicherstellen, dass das Topmanagement regelmäßig an Schulungen teilnimmt.
	Die Schulungen für das Topmanagement MÜSSEN Wissen und Fähigkeiten vermitteln, das Risikomanagement zu verstehen und bewerten zu können, insbesondere: - der Aufbau des Risikomanagements - die Vorgehensweise für das Erkennen, Bewerten und Behandeln von Risiken - die Abhängigkeit der erbrachten Dienste von der Informationsverarbeitung und - die Auswirkung von Risiken auf die erbrachten Dienste

	Die Schulungen SOLLTEN weiteren Zielgruppen angeboten werden, insbesondere dem ISB, Mitgliedern des IST, den IT-Verantwortlichen und den Administratoren.

9 Analyse

Kommentar / ToDo	VdS 10100
kritisch → wichtige und besonders sensible ACHTUNG! Der jährliche Rhythmus wird mittlerweile nicht mehr als ausreichend angesehen. Die Prüfung SOLLTE quartalsweise erfolgen. (Hinweis aufnehmen?!)	Der ISB MUSS die wichtigen und die kritischen IT-Ressourcen der Organisation ermitteln, jährlich prüfen, ob die Aufstellung der entsprechenden IT-Ressourcen aktuell ist und sie bei Bedarf anpassen.
übernehmen	*Die Organisation SOLLTE deshalb eine Informationsklassifizierung auf Basis eines anerkannten Standards wie ISO/IEC 27001 oder eine Schutzbedarfsanalyse gemäß BSI-Standard 200-2 durchführen.*
übernehmen	Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.

9.1 Prozesse

Kommentar / ToDo	VdS 10100
übernehmen	Die Organisation MUSS ihre zentralen Prozesse und ihre Prozesse mit hohem Schadenspotential identifizieren und dokumentieren.
übernehmen	Die Dokumentation MUSS folgende Anforderungen erfüllen:
übernehmen	1. Sie enthält eine kurze Beschreibung des Prozesses.
übernehmen	2. Sie begründet, warum der Prozess ein zentraler Prozess bzw. ein Prozess mit hohem Schadenspotential ist.
übernehmen	3. Sie enthält, wer für den Prozess verantwortlich ist (Prozessverantwortlicher).
übernehmen	4. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) des Prozesses.
übernehmen	Die Aufstellung der Prozesse und deren Dokumentation MUSS vom Topmanagement freigegeben werden.

9.2 IT-Ressourcen

Kommentar / ToDo	VdS 10100
0.4.6-ToDo: Einführungstext schreiben.	Der ISB MUSS die wichtigen und die kritischen IT-Ressourcen der Organisation ermitteln, jährlich prüfen, ob die Aufstellung der entsprechenden IT-Ressourcen aktuell ist und sie bei Bedarf anpassen.
	Um wichtige oder kritische IT-Ressourcen zu ermitteln KANN ein Top-Down-Ansatz (prozessorientierte Sicht),

	ein Bottom-Up-Ansatz (systemorientierte Sicht) oder eine Mischung aus beiden verwendet werden. Eine Mischung aus beiden Ansätzen bietet die Möglichkeit, die entsprechenden IT-Ressourcen zuverlässig zu identifizieren.

9.2.1 Wichtige IT-Ressourcen

Kommentar / ToDo	VdS 10100
neu	Die Organisation MUSS ihre wichtigen IT-Ressourcen (insbesondere die wichtigen IT-Systeme, mobilen Datenträger, Verbindungen sowie die wichtige Individualsoftware) bestimmen und diese dokumentieren.
neu	Wichtige IT-Ressourcen sind IT-Ressourcen, die für den Betrieb eines zentralen Prozesses oder eines Prozesses mit hohem Schadenspotential (siehe Abschnitt 9.1) zwingend benötigt werden.
neu	Die Dokumentation MUSS folgende Anforderungen erfüllen:
neu	1. Sie enthält eine kurze Beschreibung der IT-Ressource.
neu	2. Sie begründet, warum sie wichtig ist.
neu	3. Sie enthält ihre maximal tolerierbare Ausfallzeit (MTA).
neu	Die MTA MUSS ebenso kurz oder kürzer sein, als die kürzeste MTA aller zentralen Prozesse und Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1), die von der wichtigen IT-Ressource direkt oder indirekt abhängig sind.
neu	*Bei der Bestimmung der MTA SOLLTEN Abhängigkeiten zwischen wichtigen IT-Ressourcen berücksichtigt werden.*
neu	Die Aufstellung der wichtigen IT-Ressourcen und deren Dokumentation MUSS vom IT-Verantwortlichen freigegeben werden.

9.2.2 Kritische Informationen

Kommentar / ToDo	VdS 10100
übernehmen	Die Organisation MUSS ermitteln, ob sie kritische Informationen verarbeitet, überträgt und/oder speichert und diese dokumentieren.
übernehmen	Kritische Informationen sind Informationen, bei denen folgende Faktoren zu katastrophalen Schäden führen können:
übernehmen	1. unberechtigte Einsicht, Kenntnisnahme oder Weitergabe (Kriterium „Vertraulichkeit“)
übernehmen	2. Verfälschung (Kriterium „Integrität“)
übernehmen	3. Datenverlust von weniger als 24 Stunden (Kriterium „Maximal tolerierbarer Datenverlust – MTD“)
übernehmen	4. Nichtverfügbarkeit im Echtzeitbetrieb (Kriterium „Zugesicherte Verfügbarkeit“)
übernehmen	Hierfür MÜSSEN die zentralen Prozesse und die Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1)

	untersucht werden.
übernehmen	Die Dokumentation MUSS folgende Anforderungen erfüllen:
übernehmen	1. Sie enthält die Kriterien, anhand derer die Informationen als kritisch eingestuft wurden.
übernehmen	*Kritische Informationen SOLLTEN anhand ihrer qualitativen und quantitativen Merkmale beschrieben werden. Qualitative Merkmale definieren die Eigenschaften der kritischen Informationen. Quantitative Merkmale definieren, ab welcher Menge Informationen mit den genannten Eigenschaften kritisch sind. Die Erfassung quantitativer und qualitativer Merkmale bietet die Möglichkeit, die entsprechenden Informationen zuverlässiger zu erfassen.*
übernehmen	2. Sie begründet, warum die Informationen kritisch sind.
übernehmen	Die Aufstellung der kritischen Informationen und deren Dokumentation MUSS vom Topmanagement freigegeben werden.

9.2.3 Kritische IT-Ressourcen

Kommentar / ToDo	VdS 10100
	Die Organisation MUSS die kritischen IT-Ressourcen (insbesondere die kritischen IT-Systeme, mobilen Datenträger, Verbindungen sowie die kritische Individualsoftware) bestimmen und diese dokumentieren.
	Kritische IT-Ressourcen sind IT-Ressourcen, die kritische Informationen (siehe Abschnitt 9.2) verarbeiten, speichern oder übertragen oder die für den Betrieb von kritischen IT-Ressourcen zwingend benötigt werden. Sie sind eine Untermenge der wichtigen IT-Ressourcen.
	Hierfür MÜSSEN die kritischen Informationen (siehe Abschnitt 9.2) untersucht werden.
	Dabei SOLLTE der gesamte Lebensweg der kritischen Informationen berücksichtigt werden.
	Um IT-Ressourcen zu ermitteln, die für den Betrieb von kritischen IT-Ressourcen zwingend benötigt werden, KANN ebenfalls ein Top-Down-Ansatz, ein Bottom-Up-Ansatz oder eine Mischung aus beiden Ansätzen verwendet werden (siehe Abschnitt 9.2).
	Die Dokumentation MUSS folgende Anforderungen erfüllen:
	1. Sie enthält eine kurze Beschreibung der kritischen IT-Ressource.
	2. Sie begründet, warum sie kritisch ist.
	3. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) der kritischen IT-Ressource.
	Die MTA MUSS ebenso kurz oder kürzer sein, als die kürzeste MTA aller zentralen Prozesse und Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1), die von der kritischen IT-Ressource direkt oder indirekt abhängig sind.
	Bei der Bestimmung der MTA SOLLTEN Abhängigkeiten zwischen kritischen IT-Ressourcen berücksichtigt werden.
	Die Aufstellung der kritischen IT-Ressourcen und deren Dokumentation MUSS vom IT-Verantwortlichen

	freigegeben werden.

9.2.4 Weitere Kategorien von IT-Ressourcen

Kommentar / ToDo	VdS 10100
	Die Organisation SOLLTE prüfen, ob es notwendig oder sinnvoll ist, im Zuge des Risikomanagements weitere Kategorien von IT-Ressourcen zu definieren, diese zyklisch oder fortlaufend zu erfassen und sie mit individuell zusammengestellten technischen und organisatorischen Maßnahmen abzusichern.

9.3 Lieferanten

Kommentar / ToDo	VdS 10100
	Die Organisation MUSS die wichtigen und die kritischen Lieferanten der Organisation ermitteln, jährlich prüfen, ob die entsprechende Aufstellung aktuell ist und sie bei Bedarf anpassen.
	Um wichtige oder kritische Lieferanten zu ermitteln KANN ein Top-Down-Ansatz (prozessorientierte Sicht), ein Bottom-Up-Ansatz (systemorientierte Sicht) oder eine Mischung aus beiden verwendet werden. Eine Mischung aus beiden Ansätzen bietet die Möglichkeit, die entsprechenden Lieferanten zuverlässig zu identifizieren.

9.3.1 Wichtige Lieferanten

Kommentar / ToDo	VdS 10100
0.5.6-ToDo: Redundant. Kürzen.	Die Organisation MUSS ihre wichtigen Lieferanten bestimmen und dokumentieren.
0.5.6-ToDo: Verschieben in Kap. 3	Wichtige Lieferanten sind Lieferanten, die IT-Produkte oder IT-Dienstleistungen die für den Betrieb eines zentralen Prozesses oder eines Prozesses mit hohem Schadenspotential (siehe Abschnitt 9.1) zwingend benötigt werden liefern oder die Zugriff auf wichtige IT-Ressourcen besitzen.
	Die Dokumentation MUSS folgende Anforderungen erfüllen:
	1. Sie enthält eine kurze Beschreibung des Lieferanten und eine Aufstellung der wichtigen Waren und Dienstleistungen.
	3. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) der gelieferten Waren und Dienstleistungen.
	Die MTA MUSS ebenso kurz oder kürzer sein, als die kürzeste MTA aller zentralen Prozesse und Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1), die von den gelieferten Waren oder Dienstleistungen direkt oder indirekt abhängig sind.
	Bei der Bestimmung der MTA SOLLTEN Abhängigkeiten zwischen wichtigen Lieferanten berücksichtigt werden.
	Die Aufstellung der wichtigen Lieferanten und deren Dokumentation MUSS von den jeweiligen Prozessverantwortlichen freigegeben werden.

9.3.2 Kritische Lieferanten

Kommentar / ToDo	VdS 10100
	Die Organisation MUSS ihre kritischen Lieferanten bestimmen und dokumentieren.
	Kritische Lieferanten sind Lieferanten, bei denen ein Sicherheitsvorfall zu einem katastrophalen Schaden für die Organisation führen kann.
	Hierfür MÜSSEN die kritischen Informationen (siehe Abschnitt 9.2.2) und die kritischen IT-Ressourcen (siehe Abschnitt 9.2.3) untersucht werden.
	Die Dokumentation MUSS folgende Anforderungen erfüllen:
	1. Sie enthält eine kurze Beschreibung des Lieferanten und eine Aufstellung der gelieferten Waren und Dienstleistungen.
	2. Sie begründet, warum er kritisch ist.
	3. Sie enthält ihre maximal tolerierbare Ausfallzeit (MTA) der gelieferten Waren und Dienstleistungen.
	Die MTA MUSS ebenso kurz oder kürzer sein, als die kürzeste MTA aller zentralen Prozesse und Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1), die von den gelieferten Waren oder Dienstleistungen direkt oder indirekt abhängig sind.
	Bei der Bestimmung der MTA SOLLTEN Abhängigkeiten zwischen kritischen Lieferanten berücksichtigt werden.
	Die Aufstellung der kritischen Lieferanten und deren Dokumentation MUSS vom IT-Verantwortlichen freigegeben werden.

9.3.4 Weitere Kategorien von Lieferanten

Kommentar / ToDo	VdS 10100
0.4.6: neu	Die Organisation SOLLTE prüfen, ob es notwendig oder sinnvoll ist, im Zuge des Risikomanagements weitere Kategorien von Lieferanten zu definieren, diese zyklisch oder fortlaufend zu erfassen und mit ihnen individuelle technische und organisatorische Maßnahmen für die Absicherung ihrer Informationsverarbeitung zu vereinbaren.

10 IT-Systeme

Kommentar / ToDo	VdS 10100
übernehmen	Die Informationsverarbeitung einer Organisation geschieht zum größten Teil elektronisch. Es ist deshalb notwendig, IT-Systeme strukturiert zu verwalten und abzusichern.

10.1 Inventarisierung

Kommentar / ToDo	VdS 10100
übernehmen	Es MUSS eine Inventarisierung vorhanden sein, in der alle IT-Systeme der Organisation verzeichnet sind.
übernehmen	Die Inventarisierung MUSS durch entsprechende Verfahren (siehe Abschnitte 10.2.1 und 10.2.2) vollständig und aktuell gehalten werden.
übernehmen	In ihr MÜSSEN folgende Informationen für jedes IT-System verzeichnet sein:
übernehmen	1. eindeutiges Identifizierungsmerkmal
übernehmen	2. Informationen, die eine schnelle Lokalisierung erlauben
übernehmen	3. Einsatzzweck
neu	4. seine Schutzkategorie (siehe Kapitel 9)
übernehmen	*Darüber hinaus SOLLTEN für jedes IT-System weitere Informationen erhoben und aktuell gehalten werden, wie z. B. Namen, Versionen und Lizenzinformationen der installierten System- und Anwendungssoftware, Seriennummern von Hardwarekomponenten sowie Informationen über Garantien und Serviceverträge.*
übernehmen	*Besonderheiten der Installation und Konfiguration SOLLTEN in einer Dokumentation verzeichnet sein.*

10.2 Lebenszyklus

Kommentar / ToDo	VdS 10100
angepasst („Inbetriebnahme“ → „Auswahl“) Änderung in der VdS 10000: „zu deren“ → „zur“	IT-Systeme bilden eine abgeschlossene Funktionseinheit aus Hard- und Software (siehe Abschnitt 10.3). Sie unterliegen einem Lebenszyklus, der sich üblicherweise von der Beschaffung bis zur Ausmusterung erstreckt.

10.2.1 Beschaffung

0.5.1:
Hier wird eine IS-Richtlinie für die Beschaffung von IT-Systemen gefordert.
Die konkreten Anforderungen werden in den einzelnen Abschnitten spezifiziert.

Kommentar / ToDo	VdS 10100
	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für die Beschaffung von IT-Systemen getroffen werden:
0.4.4-ToDo/Diskussion: Anforderungen gem. NIS-2 aufnehmen:	1. Der ISB definiert in Zusammenarbeit mit den Projektverantwortlichen, den betreffenden Prozesseigentümern und den betreffenden IT-Verantwortlichen die notwendigen Sicherheitseigenschaften der IT-Systeme.

§30 (2) (…) Die Maßnahmen müssen zumindest Folgendes umfassen: (...) 5. Sicherheitsmaßnahmen bei Erwerb (...) von informationstechnischen Systemen (...), einschließlich Management und Offenlegung von Schwachstellen,	
	2. Dabei werden die Anforderungen an das Management von Schwachstellen durch den Anbieter festgelegt und definiert, wie die Organisation über bestehende Schwachstellen und notwendige Gegenmaßnahmen informiert wird.
	3. Es wird festgelegt, für welchen Zeitraum der Anbieter Sicherheitsupdates zur Verfügung stellt.

10.2.2 Inbetriebnahme und Änderung

Kommentar / ToDo	VdS 10100
übernehmen	Es MUSS ein Verfahren (siehe Anhang A 1) für die Inbetriebnahme und Änderung der IT-Systeme implementiert werden, das folgende Punkte sicherstellt:
angepasst	1. Die Schutzkategorie des IT-Systems wird ermittelt bzw. seine Einstufung überprüft (siehe Kapitel 9).
angepasst	2. Die Maßnahmen der entsprechenden Schutzkategorie werden umgesetzt.
übernehmen	3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und der Netzwerkplan (siehe Abschnitt 11.1) werden aktualisiert.
übernehmen	4. Bei Inbetriebnahme werden die Arbeitsschritte dokumentiert.

10.2.3 Ausmusterung und Wiederverwendung

Kommentar / ToDo	VdS 10100
übernehmen	Es MUSS ein Verfahren (siehe Anhang A 1) für das Ausmustern und Wiederverwenden der IT-Systeme implementiert werden, das folgende Punkte sicherstellt:
übernehmen	1. Die auf dem IT-System gespeicherten Informationen werden bei Bedarf gesichert bzw. archiviert.
übernehmen	2. Alle Informationen werden vor unrechtmäßigem Zugriff geschützt, indem sie z. B. zuverlässig gelöscht, überschrieben, aus dem IT-System entfernt werden oder indem das IT-System insgesamt zerstört wird.
übernehmen	3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und der Netzwerkplan (siehe Abschnitt 11.1) werden aktualisiert.
übernehmen	4. Bei Ausmusterung werden die Arbeitsschritte dokumentiert.

10.3 Basisschutz

Kommentar / ToDo	VdS 10100

„ sofern eine entsprechende Funktionalität gegeben ist“ gestrichen. NIS-2 passt sich nicht der vorhandenen IT-Infrastruktur an.	Die Maßnahmen der folgenden Abschnitte MÜSSEN für alle IT-Systeme implementiert werden.
neu - Wir können hier nur die Schadenshöhe im Eintrittsfall als Kriterium heranziehen. - vernachlässigbarer Schaden in Kapitel 3 aufnehmen vernachlässigbarer Schaden: Schaden, der weder unmittelbar noch mittelbar zu einer Beeinträchtigung der zentralen Prozesse oder der Prozesse mit hohem Schadenspotential führen kann und dessen Auswirkungen (…) - DISKUSSION: Auch in die VdS 10k aufnehmen? :-)	*IT-Systeme KÖNNEN von der Umsetzung der Maßnahmen des Basisschutzes generell ausgenommen werden, wenn die Verletzung ihrer Vertraulichkeit, Verfügbarkeit und Authentizität nur zu einem vernachlässigbaren Schaden führen kann (Risikoakzeptanzgrenze, siehe Anhang A 2) und der Netzwerkverkehr von und zu ihnen auf das für ihre Funktionsfähigkeit notwendige Minimum beschränkt ist, z. B. durch eine geeignete Segmentierung des Netzwerks (siehe Abschnitt 11.4.2), lokale Filtermechanismen oder durch das Deaktivieren nicht benötigter Dienste.*
übernehmen	Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

10.3.1 Software

Kommentar / ToDo	VdS 10100
übernehmen	System- und Anwendungssoftware MUSS aus vertrauenswürdigen Quellen bezogen werden.
übernehmen	*Es SOLLTE ausschließlich System- und Anwendungssoftware eingesetzt werden, die Sicherheitsupdates des Herstellers erhält.*
übernehmen	*Es SOLLTE nur Software auf IT-Systemen installiert werden, die zur Aufgabenerfüllung benötigt wird; nicht benötigte Software SOLLTE deinstalliert werden.*
übernehmen	*Sämtliche Zugriffsrechte und Privilegien der Anwendungssoftware SOLLTEN auf ein Mindestmaß reduziert werden.*
übernehmen	Vom Hersteller zur Verfügung gestellte Sicherheitsupdates für die System- und Anwendungssoftware MÜSSEN nach einem implementierten Verfahren (siehe Anhang A 1) getestet, bei Eignung freigegeben und nach ihrer Freigabe umgehend installiert werden.

10.3.2 Beschränkung des Netzwerkverkehrs

Kommentar / ToDo	VdS 10100
übernehmen	Der Netzwerkverkehr von und zu IT-Systemen MUSS auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden, wenn eines der folgenden Kriterien zutrifft:

übernehmen	1. Es existieren über das Netzwerk ausnutzbare Schwachstellen, die nicht behoben werden (z. B. wenn keine Sicherheitsupdates installiert werden können, Passwörter nicht geändert werden können oder unsichere technische Verfahren eingesetzt werden).
übernehmen	2. Es handelt sich um besonders exponierte IT-Systeme (z. B. um IT-Systeme, die aus dem Internet erreichbar, oder die in öffentlich zugänglichen Räumen platziert sind oder die in weniger vertrauenswürdigen Umgebungen eingesetzt werden).
übernehmen	*Zusätzlich SOLLTE der Netzwerkverkehr von und zu IT-Systemen, für die die Organisation keinen administrativen Zugang besitzt, auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden.*
übernehmen	*Die Beschränkung des Netzwerkverkehrs KANN bspw. durch eine geeignete Segmentierung des Netzwerks (siehe Abschnitt 11.4.2), lokale Filtermechanismen oder durch das Deaktivieren nicht benötigter Dienste erfolgen.*

10.3.3 Protokollierung

Kommentar / ToDo	VdS 10100
übernehmen	Jedes IT-System MUSS erfolgreiche und erfolglose Anmeldeversuche, Fehler und Informationssicherheitsereignisse protokollieren.
übernehmen	*Protokolldaten SOLLTEN zentral gespeichert werden.*
übernehmen	Protokolldaten MÜSSEN 6 Monate lang aufbewahrt werden, sofern keine gesetzlichen Lösch- oder Aufbewahrungspflichten entgegenstehen.
übernehmen	Die Uhren aller IT-Systeme MÜSSEN auf eine gemeinsame Zeit synchronisiert sein, um Auswertungen von Logeinträgen zu ermöglichen.

10.3.4 Externe Schnittstellen und Laufwerke

Kommentar / ToDo	VdS 10100
übernehmen	*Externe Schnittstellen und Laufwerke, die nicht für die Aufgabenerfüllung benötigt werden, SOLLTEN ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht werden.*

10.3.5 Schadsoftware

Kommentar / ToDo	VdS 10100
übernehmen	Alle IT-Systeme MÜSSEN über einen Schutz vor Schadsoftware verfügen.
übernehmen	Jedes IT-System MUSS mit Hilfe geeigneter Software täglich vollständig auf Anwesenheit von Schadsoftware untersucht werden.
übernehmen	*Darüber hinaus SOLLTEN alle IT-Systeme über einen Echtzeitschutz verfügen, der alle Dateien bei Zugriff auf*

	Schadsoftware prüft.
übernehmen	*Bei IT-Systemen mit einem Echtzeitschutz KANN die vollständige Untersuchung auf Schadsoftware auf einen wöchentlichen Rhythmus reduziert werden.*
übernehmen	Das Ausführen erkannter Schadsoftware MUSS verhindert werden.
übernehmen	Die Software zum Schutz gegen Schadsoftware MUSS automatisch in kurzen zeitlichen Abständen (z. B. stündlich oder täglich) nach den neuesten Suchmustern der Hersteller suchen und diese verwenden.

10.3.6 Starten von fremden Medien

Kommentar / ToDo	VdS 10100
übernehmen	Es MUSS sichergestellt werden, dass IT-Systeme nur von autorisierten Medien gestartet werden können.
übernehmen	*Dies KANN z. B. über BIOS-Passwörter oder über einen Zutrittsschutz umgesetzt werden.*

10.3.7 Authentifizierung

Kommentar / ToDo	VdS 10100
übernehmen	Der Zugang zu allen nichtöffentlichen Bereichen der IT-Systeme MUSS durch geeignete Anmeldeverfahren abgesichert werden, die eine Authentifizierung verlangen.
übernehmen	Die Anmeldeverfahren MÜSSEN folgende Punkte sicherstellen:
übernehmen	1. Das systematische Ausprobieren von Anmeldeinformationen wird erschwert.
übernehmen	2. Interaktive Sitzungen werden beendet oder gesperrt, wenn der Nutzer innerhalb einer vorgegebenen Zeitspanne keine Eingaben tätigt.
übernehmen	3. Erfolgt die Anmeldung über ein Netzwerk, so wird die Vertraulichkeit und Integrität der Anmeldeinformationen (z. B. mit Hilfe entsprechender Authentifizierungsprotokolle) sichergestellt.
übernehmen	Damit die Anmeldeverfahren zuverlässig arbeiten können, MÜSSEN folgende Punkte sichergestellt werden:
übernehmen	1. Zugänge werden strukturiert verwaltet (siehe Kapitel 15).
§ 30 (2) (...) Die Maßnahmen müssen zumindest Folgendes umfassen: (...) „10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, (...).“	2. Es werden ausschließlich zuverlässige Authentifizierungsmechanismen wie z. B. Mehr-Faktor-Authentifizierungen oder kontinuierliche Authentifizierungen verwendet.
übernehmen (auch wenn MFA eingesetzt wird, sollten die eingesetzten Passwörter nicht trivial sein)	3. Es werden keine trivialen Authentifizierungsmerkmale (z. B. Standard-Passwörter oder einfach zu erratende Passwörter) verwendet.

10.3.8 Zugänge und Zugriffe

Kommentar / ToDo	VdS 10100
Verbessert. Wird in die VdS 10k aufgenommen.	Administrative Tätigkeiten MÜSSEN über die speziell dafür vorgesehenen Zugänge erfolgen.
Verbessert. Wird in die VdS 10k aufgenommen.	Diese DÜRFEN NICHT für die alltägliche Nutzung der IT-Systeme verwendet werden.
übernehmen	*Darüber hinaus SOLLTEN folgende Anforderungen erfüllt werden:*
übernehmen	*1. Nutzer können nur auf Informationen lesend zugreifen, wenn dies für die Erfüllung ihrer Aufgaben notwendig ist („Need-to-Know“).*
übernehmen	*2. Nutzer können nur auf Informationen schreibend zugreifen, wenn dies für die Erfüllung ihrer Aufgaben notwendig ist („Least-Privileges“).*

10.4 Zusätzliche Maßnahmen für mobile IT-Systeme

Kommentar / ToDo	VdS 10100
übernehmen	Mobile IT-Systeme sind in besonderer Weise Gefährdungen durch Diebstahl, unautorisierten Zutritt oder unsichere Netze ausgesetzt, die zusätzliche Maßnahmen erforderlich machen.
übernehmen	Folgende Maßnahmen MÜSSEN für alle mobilen IT-Systeme umgesetzt werden.

10.4.1 IS-Richtlinie

Kommentar / ToDo	VdS 10100
übernehmen	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit mobilen IT-Systemen getroffen werden:
übernehmen, Kürzung möglich: „ erhoben, verarbeitet, gespeichert und übertragen“ → „verarbeitet“	1. Es wird festgelegt, welche Informationen auf den mobilen IT-Systemen erhoben, verarbeitet, gespeichert und übertragen werden dürfen.
übernehmen	2. Die Verantwortung für die Datensicherung wird definiert.
übernehmen	3. Die Nutzer werden über die spezifischen Risiken mobiler IT-Systeme (z. B. Gefahren durch Ausspähung bei der Nutzung in der Öffentlichkeit, Verlust oder Diebstahl) informiert und zur Ergreifung entsprechender Gegenmaßnahmen verpflichtet.
übernehmen	4. Es wird untersagt, mobile IT-Systeme an unberechtigte Dritte weiterzugeben.
übernehmen	5. Es wird definiert, ob und welche Software auf den mobilen IT-Systemen von den Nutzern installiert werden darf.
übernehmen	6. Es wird definiert, ob und unter welchen Bedingungen ein Administrator das mobile IT-System orten darf.
übernehmen	7. Es wird definiert, ob und unter welchen Bedingungen ein Administrator die auf einem mobilen IT-System gespeicherten Informationen aus der Ferne löschen darf.

10.4.2 Schutz der Informationen

Kommentar / ToDo	VdS 10100
übernehmen – die Informationen können auch durch nicht-kryptografische Maßnahmen geschützt werden	Die auf dem mobilen IT-System gespeicherten Informationen der Organisation MÜSSEN vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.
Verschärfung gegenüber der VdS 10k: „Du MUSST eine Risikoanalyse in Sachen Kryptografie machen“. 0.5.6-ToDo: redundant. verbessern	Es MUSS mit Hilfe einer Risikoanalyse und -behandlung (siehe Anhang A 2) festgelegt werden, welche Informationen durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.
nicht übernehmen, wird ersetzt durch Zeile weiter oben	

10.4.3 Verlust

Kommentar / ToDo	VdS 10100
übernehmen	Es MÜSSEN Verfahren (siehe Anhang A 1) implementiert werden, die festlegen, wie Nutzer und Administratoren bei Verlust eines mobilen IT-Systems vorzugehen haben.
übernehmen	Die Verfahren MÜSSEN insbesondere festlegen, wie und an wen der Verlust zu melden ist und welche Sofortreaktion erfolgt.
übernehmen	Die Verfahren MÜSSEN sicherstellen, dass die auf dem Gerät hinterlegten Zugänge der Organisation nach der Verlustmeldung nicht unberechtigt genutzt werden können (z. B. indem die entsprechenden Authentifizierungsmerkmale umgehend zurückgesetzt oder indem Anrufweiterleitungen modifiziert sowie Sprachnachrichten gelöscht werden).
übernehmen	Der Verlust eines mobilen IT-Systems MUSS als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.

10.5 Zusätzliche Maßnahmen für wichtige IT-Systeme

Kommentar / ToDo	VdS 10100
neu	Für wichtige IT-Systeme MUSS eine Risikoanalyse und –behandlung etabliert werden (siehe Anhang A 2).
neu	Zusätzlich zur Risikoanalyse und –behandlung MÜSSEN für alle wichtigen IT-Systeme die Maßnahmen der folgenden Abschnitte umgesetzt werden.
neu	Wenn Maßnahmen der folgenden Abschnitte nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko in der Risikoanalyse und -behandlung der entsprechenden IT-Systeme begegnet werden.

10.5.1 Dokumentation

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Für jedes wichtige IT-System MUSS eine Dokumentation vorhanden sein.

übernehmen	Anhand der Dokumentation MUSS es fachlich versierten Personen möglich sein, folgende Punkte nachzuvollziehen:
übernehmen	1. wer für das IT-System verantwortlich ist
übernehmen	2. wie und mit welchen Zugängen und Authentifizierungsmerkmalen der administrative Zugang zum IT-System möglich ist
übernehmen	3. welche grundlegenden Designentscheidungen bei der Installation getroffen wurden
übernehmen	4. welche Änderungen vorgenommen wurden
übernehmen	5. wann sie vorgenommen wurden
übernehmen	6. wer sie vorgenommen hat
übernehmen	7. warum sie vorgenommen wurden

10.5.2 Datensicherung

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Alle wichtigen IT-Systeme MÜSSEN über eine Datensicherung (siehe Abschnitt 16.6) verfügen.

10.5.3 Überwachung

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Es MUSS überwacht werden, ob sich die wichtigen IT-Systeme im Regelbetrieb befinden.
kritisch → wichtig	Dabei MUSS sichergestellt werden, dass der Ausfall eines wichtigen IT-Systems erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.
kritisch → wichtig	*Darüber hinaus SOLLTEN die Ressourcen der wichtigen IT-Systeme überwacht werden, um Engpässe zu erkennen, bevor sie akut werden.*

10.5.4 Wichtige Individualsoftware

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Die Organisation MUSS durch vertragliche und/oder organisatorische Regelungen sicherstellen, dass sie wichtige Individualsoftware auch in Zukunft verwenden und ihren Bedürfnissen anpassen kann.

10.5.5 Entwicklung, Beschaffung und Wartung wichtiger IT-Systeme, IT-Komponenten und Individualsoftware

§ 30 (2) (…) Die Maßnahmen müssen zumindest Folgendes umfassen:
(...)
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von (...) informationstechnischen Systemen (und) Komponenten,

einschließlich Management und Offenlegung von Schwachstellen,

Kommentar / ToDo	VdS 10100
	Bei Entwicklung, Beschaffung und Wartung von wichtiger Software, wichtigen IT-Systemen und wichtigen IT-Komponenten MÜSSEN die folgenden Anforderungen erfüllt werden:
	1. Die Sicherheitsanforderungen an das Produkt werden durch eine Risikoanalyse und -behandlung definiert.
	2. Es ist durch vertragliche und/oder organisatorische Regelungen sichergestellt, dass sie wichtige IT-Systeme, IT-Komponenten und Individualsoftware auch in Zukunft verwenden und ihren Bedürfnissen anpassen kann.
	Bei umfangreicheren Projekten SOLLTE ein Lasten- und Pflichtenheft erstellt und gepflegt werden.

10.6 Zusätzliche Maßnahmen für kritische IT-Systeme

Kommentar / ToDo	VdS 10100
übernehmen	Folgende Maßnahmen MÜSSEN zusätzlich für alle kritischen IT-Systeme umgesetzt werden.
übernehmen	Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko in der Risikoanalyse und -behandlung der entsprechenden IT-Systeme begegnet werden.

10.6.1 Notbetriebsniveau

Kommentar / ToDo	VdS 10100
übernehmen	*Für jedes kritische IT-System SOLLTE ein Notbetriebsniveau definiert werden.*

10.6.2 Robustheit

Kommentar / ToDo	VdS 10100
übernehmen	Auf kritischen IT-Systemen DÜRFEN KEINE Entwicklungen oder Tests durchgeführt werden.
übernehmen	Auf kritischen IT-Systemen MÜSSEN alle Netzwerkdienste, die nicht zur Aufgabenerfüllung benötigt werden, deinstalliert, abgeschaltet oder durch geeignete Filtermechanismen unzugänglich gemacht werden.

10.6.3 Kryptografie

Kommentar / ToDo	VdS 10100
	Im Zuge der Risikoanalyse und -behandlung (siehe Abschnitt 10.n1) MUSS festgelegt werden, welche Informationen auf den kritischen IT-Systemen durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.

	Die dabei eingesetzten kryptografischen Maßnahmen MÜSSEN auf anerkannt sicheren technischen Verfahren basieren, wie sie z. B. in BSI TR-02102-1 aufgeführt sind.

10.6.4 Externe Schnittstellen und Laufwerke

Kommentar / ToDo	VdS 10100
übernehmen	Externe Schnittstellen und Laufwerke, die nicht für die Aufgabenerfüllung benötigt werden, MÜSSEN ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht werden.

10.6.5 Änderungsmanagement

Kommentar / ToDo	VdS 10100
übernehmen	Änderungen, die auf kritischen IT-Systemen umgesetzt werden sollen, MÜSSEN zuvor in einer Testumgebung getestet und freigegeben worden sein.
übernehmen	Für kritische IT-Systeme MUSS ein Mechanismus vorhanden sein, der sicherstellt, dass bei einer Fehlfunktion oder einem Ausfall des IT-Systems aufgrund einer Änderung sein ursprünglicher Zustand innerhalb seiner MTA wiederhergestellt werden kann, sofern keine Ersatzsysteme oder –verfahren verfügbar sind (siehe Abschnitt 10.5.5).

10.6.6 Ersatzsysteme und -verfahren

Kommentar / ToDo	VdS 10100
übernehmen	Wenn ein kritisches IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, MUSS die Organisation über ein Ersatzsystem oder –verfahren verfügen, das es ermöglicht, die vom kritischen IT-System abhängigen zentralen Prozesse und Prozesse mit hohem Schadenspotential weiter zu betreiben.
übernehmen	*Das Ersatzsystem oder –verfahren SOLLTE das Notbetriebsniveau (siehe Abschnitt 10.5.2) des kritischen IT-Systems sicherstellen.*

10.6.7 Entwicklung, Beschaffung und Wartung besonders sensibler IT-Systeme, IT-Komponenten und Individualsoftware

§ 30 (2) (…) Die Maßnahmen müssen zumindest Folgendes umfassen:
(...)
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,

Kommentar / ToDo	VdS 10100
0.5.6-ToDo: Geeignete Sicherheitsmaßnahmen. Diese können	Bei Entwicklung und Beschaffung von kritischen IT-Systemen, kritischen IT-Komponenten und besonders

sein:	sensibler Individualsoftware MÜSSEN die folgenden Anforderungen erfüllt werden:
	1. Es wird eine Sicherheitsarchitektur definiert, die die ermittelten Sicherheitsanforderungen (siehe Abschnitt X.Y) erfüllt.
	2. Der Produkt- und Entwicklungslebenszyklus ist so gestaltet, dass die Sicherheitsanforderungen im gesamten Lebenszyklus (Planung, Implementierung, Test, Betrieb, Anpassung und Ausmusterung) berücksichtigt werden.
	3. Es ist über ihren gesamten Lebenszyklus sichergestellt, dass Sicherheitsrisiken dokumentiert sowie ausgenutzte Schwachstellen und Sicherheitsvorfälle aktiv gemeldet werden.
	4. Für die Dauer des Support-Zeitraums ist sichergestellt, dass Schwachstellen wirksam behandelt werden (z. B. durch Updates oder Hinweise zur sicheren Konfiguration).
	5. Es wird eine Anleitung für die sichere Inbetriebnahme, den sicheren Betrieb und die sichere Ausmusterung der Produkte erstellt und bei Bedarf (z. B. nach Sicherheitsvorfällen oder bekannt gewordenen Schwachstellen) angepasst.

11 Netzwerke und Verbindungen

Kommentar / ToDo	VdS 10100
übernehmen	Netzwerke und Verbindungen übertragen Informationen und vernetzen IT-Systeme miteinander. Deshalb ist es notwendig, sie angemessen abzusichern.

11.1 Netzwerkplan

Kommentar / ToDo	VdS 10100
übernehmen	Die Netzwerke der Organisation MÜSSEN so erfasst sein, dass fachlich versierte Personen folgende Punkte nachvollziehen können:
übernehmen	1. physikalische Netzwerkstruktur
übernehmen	a. aktive Netzwerkkomponenten und deren Verbindungen untereinander
übernehmen	b. physikalisches Medium der Verbindungen
übernehmen	2. logische Netzwerkstruktur
übernehmen	a. Netzwerksegmente (siehe Abschnitt 11.4.2), deren Einsatzzweck und deren Verbindungen untereinander
übernehmen	b. Fernzugänge (siehe Abschnitt 11.4.3)
übernehmen	c. Netzwerkkopplungen (siehe Abschnitt 11.4.4)
übernehmen	d. Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken (siehe Abschnitt 11.3)

11.2 Aktive Netzwerkkomponenten

Kommentar / ToDo	VdS 10100
übernehmen	Aktive Netzwerkkomponenten sind IT-Systeme und MÜSSEN gemäß Kapitel 10 behandelt werden.

11.3 Netzübergänge

Kommentar / ToDo	VdS 10100
übernehmen	Folgende Maßnahmen MÜSSEN für alle Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken umgesetzt werden:
übernehmen	1. Der Netzwerkverkehr wird auf das für die Funktionsfähigkeit notwendige Minimum beschränkt.
übernehmen	2. Der Inhalt erlaubter Verbindungen wird auf Schadsoftware und Angriffe untersucht; erkannte Schadsoftware und Angriffe werden blockiert.
übernehmen	3. Hinweise auf Schadsoftware in der IT-Infrastruktur der Organisation und Angriffe aus der IT-Infrastruktur der Organisation heraus werden als Sicherheitsvorfall behandelt.
übernehmen	Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.
übernehmen	*Weitere Sicherheitsmaßnahmen SOLLTEN im Zuge einer Risikoanalyse und -behandlung (siehe Anhang A 2) ermittelt und umgesetzt werden.*
übernehmen	Die Konfiguration der Netzwerkkomponenten, die einen Netzwerkübergang zu weniger oder nicht vertrauenswürdigen Netzwerken implementieren, MUSS jährlich überprüft werden und folgende Anforderungen erfüllen:
übernehmen	1. Für die sicherheitsrelevanten Einstellungen sind folgende Punkte dokumentiert:
übernehmen	a. wer sie implementiert hat
übernehmen	b. wann sie implementiert wurden
übernehmen	c. was sie bewirken
übernehmen	d. warum sie benötigt werden
übernehmen	2. Die angestrebten Verkehrsbeschränkungen werden wirksam umgesetzt.

11.4 Basisschutz

Kommentar / ToDo	VdS 10100
„sofern eine entsprechende Funktionalität gegeben ist“ gestrichen. NIS-2 passt sich nicht der vorhandenen IT-Infrastruktur an.	Die Maßnahmen der folgenden Abschnitte MÜSSEN für alle Netzwerke implementiert werden.

neu	*Netzwerke KÖNNEN von der Umsetzung der Maßnahmen des Basisschutzes generell ausgenommen werden, wenn die Verletzung ihrer Vertraulichkeit, Verfügbarkeit und Authentizität nur zu einem vernachlässigbaren Schaden führen kann (Risikoakzeptanzgrenze, siehe Anhang A 2) und der Netzwerkverkehr von und zu ihnen auf das für ihre Funktionsfähigkeit notwendige Minimum beschränkt ist, z. B. durch eine geeignete Segmentierung.*
übernehmen	Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

11.4.1 Netzwerkanschlüsse

Kommentar / ToDo	VdS 10100
übernehmen	Dauerhaft nicht genutzte Netzwerkanschlüsse MÜSSEN vor unberechtigter Nutzung gesichert werden.
übernehmen	*Dies KANN bspw. durch eine Zutrittsbeschränkung, eine Deaktivierung der Netzwerkanschlüsse oder durch eine Netzwerkzugangskontrolle geschehen.*

11.4.2 Segmentierung

Kommentar / ToDo	VdS 10100
Regelung der VdS 10100 wurde in die VdS 10k übernommen.	Es MÜSSEN Kriterien definiert werden, anhand derer die Netzwerke der Organisation in einzelne Sicherheitszonen unterteilt werden (Segmentierung).
übernehmen	Die Umsetzung der Segmentierung MUSS eine möglichst umfassende Beschränkung der Verbindungen sowie die Möglichkeit der Protokollierung von blockierten Verbindungen beinhalten.
neu	Die Segmentierung MUSS gewährleisten, dass der Netzwerkverkehr zwischen IT-Systemen mit unterschiedlichen Schutzkategorien (siehe Kapitel 9) auf das für die Funktionsfähigkeit notwendige Minimum beschränkt ist.

11.4.3 Fernzugang

Kommentar / ToDo	VdS 10100
übernehmen	Der Zugang zu nichtöffentlichen Bereichen von IT-Systemen der Organisation über weniger oder nicht vertrauenswürdige Netzwerke MUSS abgesichert werden.
übernehmen	Dabei MÜSSEN folgende Anforderungen erfüllt werden:
übernehmen	1. Die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen wird geschützt.
Empfehlung für den Einsatz von Kryptografie aufgenommen.	*Dies KANN durch den Einsatz von anerkannt sicheren kryptografischen Maßnahmen sichergestellt werden, wie sie z. B. in BSI TR-02102-1 verzeichnet sind.*
übernehmen	2. Der Zugang wird so gestaltet, dass über ihn nur IT-Systeme erreichbar sind, die der jeweilige Nutzer für seine

	Aufgabenerfüllung benötigt.
	3. Der Zugang wird so gestaltet, dass der Nutzer und das zugreifende IT-System authentifiziert werden und sichergestellt ist, dass das IT-System grundlegende Sicherheitsanforderungen erfüllt oder der Zugang erfolgt über eine Remote-Desktop-Verbindung, die sicherstellt, dass Informationen nicht auf die zugreifenden IT-Systeme kopiert werden können.
MFA wird von NIS-2 umfassend gefordert. Hier sollten wir eher ein MUSS gestalten und die Maßnahmen durch eine RA abschwächen lassen (Basisschutz). 0.5.7-NEU: gleiche Formulierung wie in 10.3.7 (Authentifizierung) gewählt.	4. Der Nutzer wird, vor allem wenn er umfangreiche Zugriffsrechte besitzt, mit Hilfe zuverlässiger Authentifizierungsmechanismen wie z. B. Mehr-Faktor-Authentifizierungen oder kontinuierliche Authentifizierungen authentifiziert, um die Gefahr eines unberechtigten Zugangs zu verringern.

11.4.4 Netzwerkkopplung

Kommentar / ToDo	VdS 10100
übernehmen	Die Kopplung von Netzwerken der Organisation über weniger oder nicht vertrauenswürdige Netzwerke hinweg MUSS abgesichert werden.
übernehmen	Dabei MÜSSEN die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen gewährleistet werden.

11.5 Zusätzliche Maßnahmen für wichtige Verbindungen

Kommentar / ToDo	VdS 10100
kritisch → wichtig 0.4.1 Diskussion/ToDO: nur für kritische Verbindungen oder Basisschutz für wichtige,MUSS für kritische Verbindungen?	Für alle wichtigen Verbindungen, MUSS eine Risikoanalyse und –behandlung (siehe Anhang A 2) etabliert werden.
§ 30 (2) (…) Die Maßnahmen müssen zumindest Folgendes umfassen: 10. (...) gesicherte Sprach-, Video- und Textkommunikation	Dabei MUSS festgelegt werden, welche Verbindungen, insbesondere welche wichtige Sprach-, Video- und Textkommunikation, durch kryptografische Maßnahmen geschützt werden.
0.5.7-DISKUSSION: Beispiele geben? * Prüfen Sie, welche Mail-Accounts mit einer Ende-zu-Ende-Verschlüsselung und/oder durch digitale Signaturen abgesichert werden sollten (S/MIME). * Prüfen Sie, ob VoIP-Verbindungen innerhalb der Organisation verschlüsselt sind. * Prüfen Sie, ob die in der Organisation eingesetzten Instant Messenger über eine verlässliche Ende-zu-Ende-	

Verschlüsselung verfügen. * Prüfen Sie, ob die in der Organisation eingesetzten Videokonferenzsysteme über schlüssige Sicherheitskonzepte verfügen.	
	Die dabei eingesetzten kryptografischen Maßnahmen MÜSSEN auf anerkannt sicheren technischen Verfahren basieren, wie sie z. B. in BSI TR-02102-1 aufgeführt sind.

12 Mobile Datenträger

Kommentar / ToDo	VdS 10100
übernehmen	Mobile Datenträger sind aufgrund ihrer exponierten Nutzungsart besonders gefährdet. Deshalb ist es notwendig, die damit verbundenen Risiken angemessen zu behandeln.

12.1 IS-Richtlinie

Kommentar / ToDo	VdS 10100
übernehmen	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit mobilen Datenträgern getroffen werden:
übernehmen	1. Es wird festgelegt, welche Informationen der Organisation auf mobilen Datenträgern gespeichert werden dürfen.
übernehmen	2. Die Nutzer werden über die spezifischen Risiken mobiler Datenträger (z. B. Gefahren durch Verlust oder Diebstahl oder durch das Einschleppen von Schadsoftware) informiert und zur Ergreifung entsprechender Gegenmaßnahmen verpflichtet.
übernehmen	3. Mobile Datenträger auf denen Daten der Organisation gespeichert sind, werden grundsätzlich vertraulich behandelt; sie werden nicht an unberechtigte Dritte weitergegeben oder verliehen und nicht für andere Personen zugänglich aufbewahrt.

12.2 Schutz der Informationen

Kommentar / ToDo	VdS 10100
übernehmen	*Die auf den mobilen Datenträgern gespeicherten Informationen der Organisation SOLLTEN vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.*
Verschärfung gegenüber der VdS 10k: die Empfehlung wurde zu einem „Du MUSST eine Risikoanalyse machen“.	Es MUSS mit Hilfe einer Risikoanalyse und -behandlung (siehe Anhang A 2) festgelegt werden, welche Informationen auf mobilen Datenträgern durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.
neu	Die dabei eingesetzten kryptografischen Maßnahmen MÜSSEN auf anerkannt sicheren technischen Verfahren

	basieren, wie sie z. B. in BSI TR-02102-1 aufgeführt sind.

12.3 Zusätzliche Maßnahmen für wichtige mobile Datenträger

0.3.5 - DISKUSSION:
Wenn in einer Organisation wichtige mobile Datenträger vorhanden sind, sollten wir sicherstellen, dass bei einem Ausfall/Verlust eines solchen Datenträgers die Prozesse wieder ans Laufen kommen – „Wiederanlaufpläne“ für wichtige mobile Datenträger?!

0.4.1 – Entscheidung:
- Wenn hier kein konkreter Anwendungsfall bekannt wird bitte streichen bzw. keine Maßnahmen für einen Wiederanlauf fordern.
- Bitte den Schwarm fragen.

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Für alle wichtigen mobilen Datenträger MUSS eine Risikoanalyse und –behandlung (siehe Anhang A 2) etabliert werden.

13 Umgebung

Kommentar / ToDo	VdS 10100
übernehmen	Die Organisation MUSS ihre IT-Systeme und Datenleitungen gegen negative Umwelteinflüsse absichern.
übernehmen	*Dies SOLLTE auf Basis eines anerkannten Standards wie z. B. VdS 2007 erfolgen.*
übernehmen	Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.

13.1 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen

Kommentar / ToDo	VdS 10100
übernehmen	Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen (z. B. Patchfelder) MÜSSEN vor Beschädigung und unberechtigtem Zutritt geschützt werden.
übernehmen	*Dies KANN z. B. durch bauliche Maßnahmen (Serverraum) oder durch abschließbare Schränke (Server- oder Netzwerkschränke) umgesetzt werden.*
übernehmen	*Insbesondere SOLLTEN folgende Bedrohungen bewertet und behandelt werden:*
übernehmen	*1. ungeeignete Umgebungsbedingungen (wie z. B. ungeeignete Temperatur oder Luftfeuchtigkeit, Staub oder Rauch)*
übernehmen	*2. negative Umwelteinflüsse (wie z. B. Feuer, Wasser, Blitzschlag)*

übernehmen	*3. unzuverlässige Stromversorgung (wie z. B. Unter- oder Überspannung, Spannungsspitzen, Unterbrechung)*
übernehmen	*Fest installierte Niederspannungsanlagen SOLLTEN gemäß gängiger Normen und Standards wie z. B. der DIN VDE 0100-Reihe errichtet sein.*
übernehmen	*4. Beschädigung und Verlust (wie z. B. Löschmittel, Vandalismus, Diebstahl)*

13.2 Datenleitungen

Kommentar / ToDo	VdS 10100
übernehmen	*Sämtliche Datenleitungen SOLLTEN gemäß gängiger Normen und Standards wie z. B. DIN EN 50173/4-Reihe installiert werden.*
übernehmen	Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN fest installierte Datenleitungen durch entsprechende bauliche Maßnahmen vor Beschädigung geschützt werden.
übernehmen	*Dies KANN z. B. durch das Verlegen der Datenleitungen in Kabelkanälen umgesetzt werden.*

13.3 Zusätzliche Maßnahmen für wichtigen IT-Systeme

Kommentar / ToDo	VdS 10100
kritisch → wichtig (ToDo: Prüfen, ob das passt)	Im Zuge der Risikoanalyse und -behandlung (siehe Abschnitt 10.5.1) MÜSSEN für alle wichtigen IT-Systeme folgende Bedrohungen behandelt werden:
übernehmen	1. ungeeignete Umgebungsbedingungen (wie z. B. ungeeignete Temperatur oder Luftfeuchtigkeit, Staub oder Rauch)
übernehmen	2. negative Umwelteinflüsse (wie z. B. Feuer, Wasser, Blitzschlag)
übernehmen	3. unzuverlässige Stromversorgung (wie z. B. Unter- oder Überspannung, Spannungsspitzen, Unterbrechung)
übernehmen	4. Beschädigung und Verlust (wie z. B. Löschmittel, Vandalismus, Diebstahl)
übernehmen	5. unautorisierter Zutritt
übernehmen	6. Ausspähen vertraulicher Informationen
übernehmen	*Insbesondere SOLLTE geprüft werden, kritische IT-Systeme in zusätzlich abgesicherten Gebäuden oder Gebäudeteilen unterzubringen (Sicherheitszonen).*

14 IT-Outsourcing und Cloud Computing

Kommentar / ToDo	VdS 10100
übernehmen	Wenn IT-Ressourcen ausgelagert werden, ist es notwendig, dass die Sicherheitsinteressen der Organisation berücksichtigt werden.

14.1 IS-Richtlinie

Kommentar / ToDo	VdS 10100
übernehmen	In Ergänzung zu Abschnitt 6.2 MÜSSEN in einer IS-Richtlinie die Bedingungen, unter welchen IT-Ressourcen ausgelagert werden dürfen, festgelegt werden.

14.2 Vorbereitung

Kommentar / ToDo	VdS 10100
übernehmen	Für Jedes Vorhaben, das zur Auslagerung von IT-Ressourcen führt, MÜSSEN folgende Punkte dokumentiert werden:
übernehmen	1. welche IT-Ressourcen ausgelagert werden sollen
übernehmen	2. welche betrieblichen, gesetzlichen und vertraglichen Bestimmungen, insbesondere in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität der ausgelagerten IT-Ressourcen, erfüllt werden müssen
kritisch → wichtig oder besonders sensibel	3. ob die auszulagernden IT-Ressourcen wichtig oder kritisch sind
übernehmen	Wenn IT-Ressourcen ausgelagert werden, MUSS die Organisation darauf vorbereitet werden:
übernehmen	1. Kompetenzen für die Steuerung der auszulagernden IT-Ressourcen werden aufgebaut.
übernehmen	2. Die IT-Infrastruktur wird auf das Zusammenspiel mit den auszulagernden IT-Ressourcen vorbereitet.

14.3 Vertragsgestaltung

Kommentar / ToDo	VdS 10100
übernehmen	Wenn IT-Ressourcen ausgelagert werden sollen, so MUSS mit dem Anbieter ein Vertrag geschlossen werden, der die Anforderungen aus Abschnitt 14.2 enthält und den Anbieter zu deren Erfüllung verpflichtet.
übernehmen	*Darüber hinaus SOLLTEN folgende Punkte sichergestellt sein:*
übernehmen	*1. Ansprüche aus Vertragsverletzungen können durchgesetzt werden, auch wenn sich der Anbieter nicht im gleichen Rechtsraum wie die Organisation befindet.*
übernehmen	*2. Die Mitwirkungspflichten des Anbieters im Falle einer Vertragsauflösung oder Insolvenz sind vereinbart, insbesondere die vollständige Herausgabe der IT-Ressourcen der Organisation sowie die aktive Unterstützung des Migrationsprozesses durch den Anbieter.*

14.4 Zusätzliche Maßnahmen für wichtige IT-Ressourcen

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Wenn wichtige IT-Ressourcen ausgelagert werden, MÜSSEN die Anforderungen aus Abschnitt 14.1 an ihre

	Vertraulichkeit, Verfügbarkeit und Integrität im Rahmen einer Risikoanalyse (siehe Anhang A 2.1) ermittelt und folgende Punkte vertraglich geregelt werden:
übernehmen	1. Leistungen
übernehmen	a. Die vom Anbieter zu erbringenden Leistungen werden definiert und deren Messung und Überwachung werden vereinbart.
übernehmen	b. Die Standorte, an denen Leistungen erbracht werden, werden festgelegt.
übernehmen	c. Die Sicherheitsmaßnahmen, die der Anbieter zum Schutz der ausgelagerten IT-Ressourcen treffen muss, werden vereinbart.
0.5.6-NEU	*Diese SOLLTEN angemessene kryptografische Maßnahmen zum Schutz der Vertraulichkeit und Integrität beinhalten.*
übernehmen	d. Eine Beschreibung der Schnittstellen zwischen der IT-Infrastruktur der Organisation und den ausgelagerten IT-Ressourcen wird definiert.
übernehmen	*Es SOLLTEN Konsequenzen bei Nichteinhaltung der vertraglich vereinbarten Leistungen vereinbart werden.*
übernehmen	2. Kommunikation
übernehmen	a. Die Ansprechpartner auf Seiten der Organisation und des Anbieters werden benannt.
übernehmen	b. Eine Vertraulichkeitsvereinbarung wird getroffen.
übernehmen	c. Es wird vereinbart, ob und unter welchen Bedingungen der Anbieter dazu berechtigt ist, Daten an Dritte weiterzugeben.
übernehmen	d. Eine Informationspflicht des Anbieters bei Sicherheitsvorfällen, die die ausgelagerten IT-Ressourcen betreffen, wird vereinbart.
übernehmen	3. Leistungsänderungen und Vertragsauflösung
übernehmen	a. Die Mitwirkungspflichten des Anbieters im Falle einer Vertragsauflösung oder Insolvenz werden vereinbart, insbesondere die vollständige Herausgabe der IT-Ressourcen der Organisation sowie die aktive Unterstützung des Migrationsprozesses durch den Anbieter.
übernehmen	b. Eine schriftliche Dokumentation und Meldung bei Änderungen an einem der oben genannten Punkte wird vereinbart.
übernehmen	Es MUSS sichergestellt sein, dass Ansprüche aus Vertragsverletzungen durchgesetzt werden können, auch wenn sich der Anbieter nicht im gleichen Rechtsraum wie die Organisation befindet.

15 Zugänge und Zugriffsrechte

Kommentar / ToDo	VdS 10100
Übernehmen, auch in die VdS 10k	Digitale und analoge Zugänge und Zugriffsrechte erlauben es, auf die nichtöffentliche IT der Organisation und ihre Daten zuzugreifen. Deshalb ist es notwendig, beide strukturiert zu verwalten.

15.1 Verwaltung

Kommentar / ToDo	VdS 10100
übernehmen	Es MÜSSEN Verfahren (siehe Anhang A 1) für das Anlegen und Ändern von Zugängen und Zugriffsrechten sowie für das Zurücksetzen von Authentifizierungsmerkmalen implementiert werden, die folgende Punkte sicherstellen:
übernehmen	1. Die jeweiligen Vorgänge werden vor ihrer Umsetzung beantragt, geprüft und genehmigt.
übernehmen	2. Zugänge und Zugriffsrechte werden nur genehmigt, wenn sie für die Aufgabenerfüllung des jeweiligen Nutzers oder für die betrieblichen Abläufe der Organisation notwendig sind.
übernehmen	3. Wenn ein Nutzer administrative Zugänge oder Zugriffsrechte erhalten soll, wird dies besonders begründet und vom IT-Verantwortlichen entschieden.
übernehmen	4. Antragssteller und Nutzer werden zeitnah über die erfolgte Durchführung informiert.
übernehmen	*Wenn Zugänge oder Zugriffsrechte entzogen werden, KANN auf das Informieren des Nutzers verzichtet werden.*
übernehmen	5. Vor dem Löschen eines Zugangs werden die Daten, die mit ihm verknüpft sind, weitergegeben, gelöscht oder gesichert bzw. archiviert.
übernehmen	6. Die jeweiligen Vorgänge werden dokumentiert.

15.2 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen

Kommentar / ToDo	VdS 10100
übernehmen	Alle Zugänge zu kritischen IT-Systemen sowie sämtliche Zugriffsrechte auf kritische Informationen MÜSSEN jährlich erfasst und daraufhin überprüft werden, ob sie gemäß der Verfahren aus Abschnitt 15.1 angelegt wurden und benötigt werden.
übernehmen	Nicht ordnungsgemäß angelegte Zugänge und Zugriffsrechte MÜSSEN als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.

16 Datensicherung und Archivierung

Kommentar / ToDo	VdS 10100
übernehmen	Daten können unbrauchbar werden oder verloren gehen. Deshalb ist es notwendig, durch eine Datensicherung die Integrität und Verfügbarkeit der Daten sicherzustellen.
übernehmen	*Die Datensicherung SOLLTE auf Basis eines anerkannten Standards wie z. B. BSI-Standard 200-2 unter Berücksichtigung der IT-Grundschutz-Kataloge des BSI implementiert werden.*
übernehmen	Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN die Anforderungen folgender Abschnitte erfüllt

	werden.

16.1 IS-Richtlinie

Kommentar / ToDo	VdS 10100
übernehmen	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie die Speicherorte für die Daten der Organisation festgelegt werden.
0.5.8-DISKUSSION: Wir haben in Kapitel 9 die Organisation verpflichtet, „wichtige“ IT-Ressourcen zu identifizieren (also IT-Ressourcen die zwingend benötigt werden, um einen zentralen Prozess oder einen Prozess mit hohem Schadenspotential zu betreiben). Hierzu zählen auch die entsprechenden Anwendungen (siehe Definition von „IT-Ressource“). Doch lieber in die Kommentierung?!	*Zur Kontrolle der Vollständigkeit SOLLTEN die Speicherorte der wichtigen Anwendungen untersucht werden.*

16.2 Archivierung

DISKUSSION:
Wäre es nicht sinnvoll, die Archivierung aus der VdS 10k zu streichen?
Archivierung hat mit der Informationssicherheit eigentlich nichts zu tun. Wir könnten uns also diesen Aufwand sparen.

0.2.1:
- Auch wenn Archivierung grundsätzlich nichts mit Informationssicherheit zu tun hat (Archivierung ist kein Backup), bringt der Punkt einen gewissen Mehrwert, da sichergestellt wird, dass Organisationen diese Aspekte berücksichtigen und gesetzliche Vorgaben einhalten können. Genau diese Art von Mehrwert zeichnet die VdS 10000 aus, weil sie über den Tellerrand schaut.
- Archivierung in ein SOLLTE umwandeln?
- Schwierig, aber ich würde es drin lassen, da es wir eine Brücke zur VdS 100010 bauen können und wir könnten mal überlegen als SOLLTE - Anforderung

Kommentar / ToDo	VdS 10100
In VdS 10k als SOLLTE gestalten ToDo für Version 0.4: Übernahme in VdS 10100 vermeiden?! Achtung: § 30 fordert Kryptografie vor , hier wird eine Archivierung von Schlüsselmaterial notwendig sein.	Die Organisation ~~MUSS~~ SOLLTE prüfen, welche Daten archiviert werden müssen, um betrieblichen, gesetzlichen und vertraglichen Anforderungen zu genügen.

16.3 Verfahren

Kommentar / ToDo	VdS 10100
übernehmen	Für die Datensicherung, -wiederherstellung und -archivierung MÜSSEN Verfahren (siehe Anhang A 1) implementiert werden, die die folgenden Punkte sicherstellen:
übernehmen	1. Die gesicherten Daten werden bei Übertragung, Lagerung und Transport vor Änderungen, Beschädigung, Verlust und unberechtigter Einsichtnahme geschützt.
übernehmen	*Der Schutz der Vertraulichkeit KANN z. B. durch eine Verschlüsselung der Daten oder der Sicherungsmedien erreicht werden.*
übernehmen	2. Die gesicherten Daten werden nicht im gleichen Brandabschnitt wie die gesicherten IT-Systeme aufbewahrt.
übernehmen	*Ein eigener Brandabschnitt KANN durch geeignete Datensicherungsschränke umgesetzt werden. In Bereichen mit Brandmeldesystemen SOLLTEN Datensicherungsschränke nach DIN EN 1047-1, Ausführung S 60 DIS, und in Bereichen ohne Brandmeldesysteme nach DIN EN 1047-1, Ausführung S 120 DIS zertifiziert sein.*
- VdS 10k: Mehrgenerationenprinzip aufgenommen - übernehmen	3. Die Sicherung der Daten setzt das Mehr-Generationen-Prinzip um; es gibt z. B. zusätzliche Wochen-, Monats- und Jahressicherungen, damit bei Bedarf mehrere Versionen der gesicherten Daten zur Verfügung stehen.
- VdS 10k: verteile Datensicherungen aufgenommen - übernehmen	4. Datensicherungen werden an mehreren Orten gelagert, damit die gesicherten Daten auch bei größeren Schadensereignissen verfügbar bleiben.
übernehmen	*Dazu KANN eine vollständige Datensicherung in festen zeitlichen Abständen (z. B. wöchentlich) an einen entfernten Standort ausgelagert werden.*
- VdS 10k: redundante Medien/Anbieter aufgenommen - übernehmen	5. Für die Datensicherung werden mehrere Medien eingesetzt und dabei ist sichergestellt, dass der Ausfall eines Mediums nicht zum Verlust von wesentlichen Teilen der gesicherten Daten führt - wenn für die Datensicherung ausschließlich Cloud-Dienste in Anspruch genommen werden, ist sichergestellt, dass die Verfügbarkeit der Datensicherung auch bei Ausfall eines Cloud-Dienstes gewährleistet ist (z. B. durch das Nutzen mehrerer unabhängiger Cloud-Anbieter).
übernehmen	6. Die Datensicherung und -wiederherstellung wird jährlich oder bei einer Änderung des Verfahrens getestet, indem ein betroffenes IT-System nach dem Zufallsprinzip ausgewählt, gesichert und in einer Testumgebung wiederhergestellt wird.
übernehmen	*Die Tests SOLLTEN ohne Unterstützung durch den jeweiligen Verantwortlichen für die Datensicherung erfolgen. Vielmehr SOLLTEN sie von einem anderen Mitarbeiter anhand der vorliegenden Dokumentation bewältigt werden.*
übernehmen	7. Die Durchführung und die Ergebnisse der Tests werden dokumentiert.
Die mögliche Anzahl der Verfahren sollte gering gehalten werden (da 1/3 der Verfahren jährlich geprüft werden müssen), allerdings sollten die Vorgehensweisen für die Datensicherung und -wiederherstellung einem KVP unterliegen.	*Es KÖNNEN mehrere Vorgehensweisen für die Datensicherung, -wiederherstellung oder -archivierung in einem Verfahren zusammengefasst werden, wenn die betroffenen IT-Systeme ähnliche Wiederherstellungsprozesse erfordern oder logisch zusammengefasst werden können.*

16.4 Weiterentwicklung

Kommentar / ToDo	VdS 10100
übernehmen	Der ISB MUSS jährlich prüfen, ob Änderungen an IT-Systemen sowie an betrieblichen, gesetzlichen oder vertraglichen Rahmenbedingungen eine Anpassung der Sicherungs-, Wiederherstellungs- und/oder Archivierungsverfahren erforderlich machen.
übernehmen	Notwendige Anpassungen MÜSSEN zeitnah implementiert werden.

16.5 Basisschutz

Kommentar / ToDo	VdS 10100
„ sofern eine entsprechende Funktionalität gegeben ist“ gestrichen. NIS-2 passt sich nicht der vorhandenen IT-Infrastruktur an.	Die Maßnahmen der folgenden Abschnitte MÜSSEN für alle Speicherorte (siehe Abschnitt 16.1), Server, aktive Netzwerkkomponenten und mobile IT-Systeme implementiert werden.
neu - Auch in die VdS 10k aufnehmen? 0.5.8: Nein. In der VdS 10k frühstücken wir das über den Geltungsbereich ab.	*Speicherorte, Server, aktive Netzwerkkomponenten und mobile IT-Systeme KÖNNEN von der Umsetzung der Maßnahmen des Basisschutzes generell ausgenommen werden, wenn die Verletzung ihrer Vertraulichkeit, Verfügbarkeit und Authentizität nur zu einem vernachlässigbaren Schaden führen kann (Risikoakzeptanzgrenze, siehe Anhang A 2).*
übernehmen	Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

16.5.1 IT-Systeme für die Datensicherung und -wiederherstellung

Kommentar / ToDo	VdS 10100
übernehmen	Die für die Datensicherung und -wiederherstellung eingesetzten IT-Systeme MÜSSEN besonders vor unbefugtem Zugang geschützt werden:
übernehmen	1. Auf den IT-Systemen dürfen ausschließlich Zugänge für administrative Tätigkeiten vorhanden sein.
übernehmen	2. Die Anzahl der administrativen Zugänge ist auf das für den Betrieb absolut notwendige Minimum reduziert
übernehmen	3. Die administrativen Zugänge werden unabhängig von der restlichen IT verwaltet undsie verfügen über eigene, exklusive Authentifizierungsmerkmale oder sie nutzen eine Mehr-Faktor-Authentifizierung, die unabhängig von der restlichen IT arbeitet.
übernehmen	4. Der Netzwerkverkehr von und zu den IT-Systemen ist auf das für die Funktionsfähigkeit notwendige Minimum beschränkt.

16.5.2 Speicherorte

Kommentar / ToDo	VdS 10100
übernehmen	Speicherorte MÜSSEN so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand nicht älter als 24 Stunden ist.

16.5.3 Server

Kommentar / ToDo	VdS 10100
übernehmen	Server MÜSSEN so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand (Systemsoftware, Konfigurationen, Anwendungssoftware, Anwendungs-, Logdaten, usw.) nicht älter als 24 Stunden ist.

16.5.4 Aktive Netzwerkkomponenten

Kommentar / ToDo	VdS 10100
übernehmen	Systemsoftware und Konfiguration der aktiven Netzwerkkomponenten MÜSSEN nach jeder Änderung gesichert werden.

16.5.5 Mobile IT-Systeme

Kommentar / ToDo	VdS 10100
übernehmen	Es MUSS eine Vorgehensweise für die Datensicherung von einem Administrator vorgegeben werden.

16.6 Zusätzliche Maßnahmen für wichtige IT-Systeme

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Jedes wichtige IT-System MUSS über eine Datensicherung verfügen, die in Ergänzung zu Abschnitts 16.5 folgende Anforderungen erfüllt.

16.6.1 Risikoanalyse

Kommentar / ToDo	VdS 10100
übernehmen	Im Zuge der Risikoanalyse und -behandlung (siehe Abschnitt 10.5.1) MÜSSEN die Folgen eines Datenverlusts analysiert und dabei der MTD bestimmt werden.

16.6.2 Verfahren

Kommentar / ToDo	VdS 10100
übernehmen	Die Verfahren zur Datensicherung und -wiederherstellung MÜSSEN in Ergänzung zu Abschnitt 16.3 folgende Punkte sicherstellen:
kritisch → wichtig	1. Wichtige IT-Systeme werden vollständig gesichert (Systemsoftware, Konfigurationen, Anwendungssoftware, Anwendungs-, Logdaten, usw.).
übernehmen	2. Der MTD wird nicht überschritten.
übernehmen	3. Die Wiederherstellung innerhalb der MTA wird gewährleistet, sofern keine Ersatzsysteme oder –verfahren verfügbar sind (siehe Abschnitt 10.5.9).

17 Sicherheitsvorfälle und Krisenmanagement

Kapitel 17 und 18 werden in der VdS 10000 unter der Überschrift „Sicherheitsvorfälle“ zusammengefasst.

Sicherheitsvorfall: Ungewöhnliches Ereignis, dass die Verfügbarkeit , Integrität und/oder Vertraulichkeit von Informationen oder der Informationsverarbeitung beeinträchtigt. (aufgenommen in Kapitel 3)

0.5.6-ToDo: Krise und Krisenmanagement in dieses Kapitel aufnehmen.
0.5.6-ToDO: Krise in Kap. 3 aufnehmen.

Kommentar / ToDo	VdS 10100
übernehmen	Eine angemessene Reaktion auf Sicherheitsvorfälle ermöglicht es, Schäden zu begrenzen und zügig den Regelbetrieb wieder aufzunehmen. Deshalb ist es notwendig, angemessen auf Sicherheitsvorfälle vorbereitet zu sein.
übernehmen	*Zu diesem Zweck SOLLTE die Organisation ein Business Continuity Management (BCM) auf Basis eines anerkannten Standards wie BSI-Standard 200-4 oder DIN EN ISO 22301 implementieren.*
übernehmen	Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN die Anforderungen folgender Abschnitte erfüllt werden.

17.1 IS-Richtlinie

Kommentar / ToDo	VdS 10100
übernehmen	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit Sicherheitsvorfällen getroffen werden:
angepasst	1. Die Begriffe „Sicherheitsvorfall“ und „erheblicher Sicherheitsvorfall“ werden klar definiert.

übernehmen	*Hierbei SOLLTE aufgezählt werden, welche Auffälligkeiten zur Meldung eines möglichen Sicherheitsvorfalls führen müssen.*
übernehmen	2. Jeder Mitarbeiter meldet mögliche Sicherheitsvorfälle über die dafür vorgesehenen Meldewege.
übernehmen	3. Die Verantwortlichen untersuchen, ggf. in Zusammenarbeit mit den jeweiligen Prozessverantwortlichen, den IT-Verantwortlichen und dem ISB, Sicherheitsvorfälle vordringlich.
übernehmen	4. Es wird definiert, in welchen Fällen das Topmanagement über Sicherheitsvorfälle informiert wird.
übernehmen	5. Es wird definiert, wie die Organisation intern und nach außen über akute und bewältigte Sicherheitsvorfälle kommuniziert.

17.2 Erkennen

Kommentar / ToDo	VdS 10100
übernehmen	*Es SOLLTEN Maßnahmen implementiert werden, die es ermöglichen, Sicherheitsvorfälle zu erkennen, wie z. B.:*
aktualisiert	*1. Systeme zum Erkennen und Verhindern von Angriffen (host- oder netzwerkbasierte IDS/IDP-Systeme)*
neu	*2. Systeme zur Isolation und Analyse potenziell schädlicher Software (Sandboxing-Technologien)*
übernehmen	*3. Integritätsprüfungen auf Prüfsummenbasis*
übernehmen	*4. Sensor-Systeme (Honeypots)*
	5. Überwachen der Zugriffe auf kritische Informationen (siehe Kapitel 9)
übernehmen	*6. Erfassen und Auswerten von Logmeldungen*
übernehmen	*Das Melden von Sicherheitsvorfällen SOLLTE durch eine positive Fehlerkultur und/oder anonyme Meldewege gefördert werden.*

17.3 Reaktion

Kommentar / ToDo	VdS 10100
übernehmen	Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das beim Auftreten eines Sicherheitsvorfalls folgende Reaktionen zeitnah sicherstellt:
übernehmen	1. Es wird ein Überblick über die Situation gewonnen.
übernehmen	2. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen.
Hinweis auf Ersatzverfahren?	3. Der Schaden wird durch Sofortmaßnahmen eingedämmt.
übernehmen	4. Der Schaden wird dokumentiert.
übernehmen	5. Beweismittel werden gesichert.
übernehmen	6. Der Schaden wird behoben und der Regelbetrieb wieder aufgenommen.

übernehmen	7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden; insbesondere werden dabei betroffene Verfahren (siehe Anhang A 1) und Risikoanalysen (siehe Anhang A 2) geprüft.
übernehmen	*Bei geringfügigen Störungen oder Ausfällen KÖNNEN einzelne Punkte ausgelassen und/oder das Verfahren vorzeitig beendet werden.*
0.2.1: Entscheidung: In die VdS 10k aufnehmen. Organisationen sind z. B. auch ohne NIS-2 verpflichtet, Informationen an Dritte (z. B. an Versicherungen, Datenschutz-Aufsichtsbehörden usw.) weiterzugeben.	Zusätzlich MUSS das Verfahren bei einem erheblichen Sicherheitsvorfall die folgenden Punkte sicherstellen:
0.4.2: aufgenommen.	1. Es stehen autarke Kommunikationswege für die interne und externe Kommunikation zur Verfügung, die auch bei einer Störung oder einem Ausfall der IT-Infrastruktur genutzt werden können.
Grundlage für die Zusammenarbeit mit dem BSI legen.	2. Der Sicherheitsvorfall wird von Beginn an fortlaufend so dokumentiert, dass die Organisation ihre Informationspflichten erfüllen kann.
	3. Entsprechende interne Stellen (wie Topmanagement, Abteilungsleiter, Prozesseigentümer eines zentralen Prozesses oder eines Prozesses mit hohem Schadenspotential) und externe Stellen (wie Partner, Kunden, Versicherungen und Aufsichtsbehörden) werden zeitnah informiert; entsprechende Adresslisten und Inhalte sind vorbereitet.
Für die Erfüllung von § 32 Abs. 1,2 und 3, insbesondere Anfragen des BSI zu beantworten. Ist das nicht Aufgabe des ISB?! Gesicht nach außen und innen?!	4. Einem Mitarbeiter mit entsprechender Fachkompetenz wird die Verantwortlichkeit zugeordnet, mit dem BSI zu kommunizieren.
neu	*Diese Verantwortlichkeit KANN z. B. der ISB wahrnehmen.*
BSIG § 32 Abs. 1,2 und 3	5. Die Informationspflichten gem. § 32 BSIG (Erstmeldung, Bewertung des Sicherheitsvorfalls, Zwischenmeldungen auf Anfrage des BSI, ggf. Fortschrittsmeldungen und Abschlussmeldung) werden über das entsprechende Meldeverfahren des BSI erfüllt.
BSIG § 35 Abs. 1 – Ggf. müssen wir die Krisenkommunikation näher beschreiben bzw. aus der Aufzählung heraus lösen, da sie umfangreich ist und wir hier „Best Pract“ anbieten/vorschreiben sollten. Ziel muss es sein, die Organisation auf eine Krisenkommunikation vorzubereiten.	6. Auf Anweisung des BSI werden die Empfänger der betroffenen Dienste unverzüglich über den Sicherheitsvorfall unterrichtet; hierzu werden entsprechende Inhalte, Empfängerlisten und Kommunikationswege vorbereitet
BSIG § 35 Abs. 2 – Ggf. müssen wir die Krisenkommunikation näher beschreiben bzw. aus der Aufzählung heraus lösen, da sie umfangreich ist und wir hier „Best Pract“ anbieten/vorschreiben sollten. Zusätzlich sollte die Empfehlung aufgenommen werden, auch für die interne Kommunikation	7. Fällt die Organisation unter § 35 Abs. 2, werden dem BSI und den Empfängern der betroffenen Dienste darüber hinaus Informationen über die Bedrohung selbst und über mögliche Schutzmaßnahmen mitgeteilt, hierzu werden entsprechende Inhalte vorbereitet, die im Bedarfsfall nur noch angepasst werden müssen.

entsprechende Vorkehrungen zu treffen.	
BSIG § 11	*Das BSI SOLLTE in besonderen Fällen hinzugezogen werden, z. B. wenn ein Angriff besonderer technischer Qualität vorliegt oder wenn die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen IT-Systems von besonderem öffentlichem Interesse ist.*

17.4 Zusätzliche Maßnahmen für wichtige IT-Systeme

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Folgende Maßnahmen MÜSSEN zusätzlich für alle wichtigen IT-Systeme umgesetzt werden.

17.4.1 Wiederanlaufpläne

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Für jedes wichtige IT-System MUSS ein Verfahren (siehe Anhang A 1) für den Wiederanlauf implementiert werden (Wiederanlaufplan), das folgende Anforderungen erfüllt:
übernehmen	1. Es enthält alle Informationen, Arbeitsschritte und deren Reihenfolge, die es fachlich versierten Personen ermöglichen, das IT-System innerhalb der MTA soweit wiederherzustellen, dass zumindest das Notbetriebsniveau (siehe Abschnitt 10.5.2) erreicht ist.
übernehmen	2. Wenn das IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, enthält der Wiederanlaufplan alle Informationen, Arbeitsschritte und deren Reihenfolge, die es fachlich versierten Personen ermöglichen, die entsprechenden Ersatzsysteme oder –verfahren (siehe Abschnitt 10.5.9) soweit in Betrieb zu nehmen, dass die vom IT-System abhängigen zentralen Prozesse und Prozesse mit hohem Schadenspotential betrieben werden können.
übernehmen 0.3.2: Hinzugefügt: „und kryptografische Schlüssel“ – auch in die VdS 10k übernehmen.	3. Er enthält eine Aufstellung der für die Wiederherstellung zwingend benötigten Ressourcen, wie z. B. Mitarbeiter und deren Kontaktdaten, Hardware, Software, Netzwerke, Dienste, Authentifizierungsmerkmale, kryptografische Schlüssel und Lizenzinformationen.
übernehmen	4. Er ist verständlich und übersichtlich strukturiert.
übernehmen	5. Er ist im Bedarfsfall schnell verfügbar.
übernehmen	6. Er wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.
	Es *KÖNNEN mehrere Wiederanlaufpläne in einem übergeordneten Verfahren zusammengefasst werden, wenn die betroffenen IT-Systeme ähnliche Wiederherstellungsprozesse erfordern oder logisch zusammengefasst werden können.*

17.4.2 Abhängigkeiten

Kommentar / ToDo	VdS 10100
kritisch → wichtig	Es MÜSSEN die Abhängigkeiten der wichtigen IT-Systeme untereinander dokumentiert werden.
kritisch → wichtig	*Darüber hinaus SOLLTEN die Abhängigkeiten der wichtigen IT-Systeme von sämtlichen wichtigen IT-Ressourcen dokumentiert und dabei die Notwendigkeit weiterer Wiederanlaufpläne geprüft werden.*
übernehmen	Die Dokumentation MUSS folgende Anforderungen erfüllen:
kritisch → wichtig	1. Aus ihr geht eindeutig hervor, in welcher Reihenfolge die wichtigen IT-Systeme wiederhergestellt werden müssen.
übernehmen	2. Sie ist verständlich und übersichtlich strukturiert.
übernehmen	3. Sie ist im Bedarfsfall schnell verfügbar.
übernehmen	4. Sie wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.

17.5 Zentrale Prozesse und Prozesse mit hohem Schadenspotential

Kommentar / ToDo	VdS 10100
0.5.6-ToDo: Hinweis aufnehmen: Prozesse untersuchen, mögliche Schadensereignisse identifizieren, Reaktion darauf planen - BIA	Die Organisation SOLLTE...

18. Lieferkette

Aus der Begründung zu § 30:
„Die hier genannten Vorgaben insbesondere im Bereich der Sicherheit der Lieferkette können auch die Durchführung von External Attack Surface (EAS) Scans beinhalten.“ (Seite 160)

„Unter Maßnahmen zur Sicherheit der Lieferkette sind beispielsweise vertragliche Vereinbarungen mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, Bewältigung von Cybersicherheitsvorfällen, Patchmanagement, sowie der Berücksichtigung von Empfehlungen des Bundesamt in Bezug auf deren Produkten und Dienstleistungen zu nennen.
Ebenfalls kann dies beinhalten, Zulieferer und Dienstleister zur Beachtung von grundsätzlichen Prinzipien wie Security by Design oder Security by Default anzuhalten. Hierbei Bei der Erwägung geeigneter Maßnahmen nach Absatz 4 Nummer 4 sind durch die Einrichtung die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse zu berücksichtigen. Einrichtungen müssen bei der Erwägung geeigneter Maßnahmen nach Satz 1 die

Ergebnisse der gemäß Artikel 22 Absatz 1 der NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen kritischer Lieferketten berücksichtigen.“ (Seite 161)

Kommentar / ToDo	VdS 10100
	Wenn Produkte und Dienstleistungen eingekauft werden ist es notwendig, dass die Sicherheitsinteressen der Organisation berücksichtigt werden.

18.1 Wichtige Lieferanten

Kommentar / ToDo	VdS 10100
0.5.6-ToDo: neu Formulierung Durch geeignete Maßnahmen nachzuweisen. Dies KÖNNEN sein… 1. Basisschutzmaßnahmen gem. VdS 10000 2. Zertifizierungen (…) 3. Sicherheitskonzept 4. Prüfung durch Dritte 5. (...)	
	Sie MÜSSEN vertraglich verpflichtet werden, für diese Teile ihrer IT-Infrastruktur die folgenden Maßnahmen umzusetzen:
	1. Basisschutz für IT-Systeme (siehe Abschnitt X.Y)
	2. Basisschutz für Netzwerke (siehe Abschnitt X.Y)
	3. Basisschutz Datensicherung (siehe Abschnitt 16.5)
	4. Wiederanlaufpläne für wichtige IT-Systeme (siehe Abschnitt 17.4)
	Darüber hinaus SOLLTE der Lieferant weitere notwendige Sicherheitsmaßnahmen im Rahmen einer Risikoanalyse und -behandlung identifizieren.
	Wenn Maßnahmen nicht oder nicht vollständig umgesetzt werden, MUSS die Organisation dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

18.2 Kritische Lieferanten

Kommentar / ToDo	VdS 10100
0.5.6-ToDo: neu Formulierung	Als „besonders sensibel“ eingestufte Lieferanten MÜSSEN vertraglich verpflichtet werden, ein Informationssicherheitsmanagementsystem (ISMS) vorzuweisen, das folgende Anforderungen erfüllt:

Durch geeignete Maßnahmen nachzuweisen. Dies KÖNNEN sein… 1. Basisschutzmaßnahmen gem. VdS 10000 2. Zertifizierungen (…) 3. Sicherheitskonzept 4. Prüfung durch Dritte 5. (...)	
	1. Es genügt einem anerkannten Standard wie z. B. ISO 27001, BSI-Standard 200-1 oder VdS 10000.
	2. Es sichert alle Teile der Informationsverarbeitung des Lieferanten ab, die er benötigt, um die Produkte und Dienstleistungen für die Organisation in der vereinbarten Qualität, Menge und zum vereinbarten Zeitpunkt zu liefern.
	3. Es ist von unabhängiger Stelle zertifiziert.
	Wenn Maßnahmen dieses Abschnitts nicht oder nicht vollständig vollständig umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

Anhang A

A 1 Verfahren

§ 30 (2) (…) Die Maßnahmen müssen zumindest Folgendes umfassen:
(...)
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von (...) Prozessen, einschließlich Management und Offenlegung von Schwachstellen,

Kommentar / ToDo	VdS 10100
übernehmen	Die Organisation MUSS die in diesen Richtlinien geforderten Verfahren planen, steuern und stetig verbessern.
übernehmen	*Dies SOLLTE im Rahmen eines Qualitätsmanagements auf Basis eines anerkannten Standards wie z. B. DIN EN ISO 9001 geschehen.*
übernehmen	Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN folgende Anforderungen erfüllt werden:
0.5.1-DISKUSSION: Sicherheitsmaßnahme für die Entwicklung und Wartung von Verfahren.	1. Es wird definiert, welche Ziele in Bezug auf die Informationssicherheit mit dem Verfahren erreicht werden sollen.
0.5.1-DISKUSSION: KPIs	*Zusätzlich SOLLTE definiert werden, anhand welcher Kennzahlen erkannt werden kann, ob die in Bezug auf die Informationssicherheit gesetzten Ziele erreicht wurden.*
übernehmen	2. Es wird definiert, wer für die Durchführung verantwortlich ist.
neu	*Zusätzlich SOLLTE definiert werden, wer für seine Etablierung verantwortlich ist.*

übernehmen	3. Verfahren werden in einer für die jeweilige Zielgruppe zugänglichen und verständlichen Form dokumentiert und bekannt gegeben.
Wartung der Verfahren, Management von Schwachstellen.	4. Verfahren werden verbessert, wenn Mängel in ihrer Umsetzung, Angemessenheit oder Effektivität erkannt werden.
Wartung der Verfahren, KVP.	5. Umsetzung, Angemessenheit und Effektivität werden jährlich bei einem Drittel der Verfahren überprüft. Die zu überprüfenden Verfahren werden nach dem Zufallsprinzip ausgewählt. Wenn die jährliche Überprüfung ergibt, dass mehr als die Hälfte der überprüften Verfahren mängelbehaftet ist, werden alle Verfahren überprüft.

A 2 Risikomanagement

Kommentar / ToDo	VdS 10100
0.5.6-ToDo: Risikomanagementmaßnahmen implementieren (…) --- in Analogie A1 Verfahren. Vorlage: Die Organisation MUSS die in diesen Richtlinien geforderten Risikomanagementmaßnahmen implementieren und stetig verbessern.	Die Organisation MUSS die in diesen Richtlinien geforderten Risikoanalysen durchführen und erkannte Risiken zeitnah und angemessen behandeln.
übernehmen	*Dies SOLLTE im Rahmen eines Risikomanagements auf Basis eines anerkannten Standards wie BSI-Standard 200-3, ISO/IEC 27005 oder ISO 31000 erfolgen.*
übernehmen - Durch diese Vorgabe wird die Vorgehensweise für die Risikoidentifikation, der Risikoanalyse und der Risikobehandlung definiert und dokumentiert.	Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.

A 2.1 Methodik

Kommentar / ToDo	VdS 10100
neu	Die Vorgehensweisen für die Risikoidentifikation, -analyse und -behandlung MÜSSEN festgelegt sein.
0.5.6-ToDo: Aufspalten in zwei Sätze.	Es MÜSSEN Kriterien für die Bewertung der Schadenshöhe und der Eintrittswahrscheinlichkeit festgelegt werden, anhand derer Risiken bewertet werden.
0.5.7-neu	Es MÜSSEN Kriterien für die Bewertung der Schadenshöhe und der Eintrittswahrscheinlichkeit festgelegt werden, anhand derer zuverlässig festgestellt werden kann, ob ein Risiko generell akzeptiert werden kann (Risikoakzeptanzgrenze).
neu	Die Vorgehensweisen MÜSSEN so gewählt sein, dass sie zu reproduzierbaren und schlüssigen Ergebnissen führen.
- BSIG § 30 Abs.2: „Maßnahmen nach Absatz 1 sollen den	*Die Auswahl der Vorgehensweisen SOLLTE auf Basis eines anerkannten Standards wie z. B. ISO 31010*

Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen.“	*erfolgen.*

A 2.2 Risikoidentifikation

Kommentar / ToDo	VdS 10100
	Jede Risikoidentifikation MUSS folgende Anforderungen erfüllen:
	1. Ihre Durchführung und ihre Ergebnisse werden dokumentiert.
unterscheidet sich von der VdS 10k: Erfüllung von § 30 (1) „um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse (...) zu vermeiden und Auswirkungen (…) möglichst gering zu halten“ und (2) „gefahrenübergreifender Ansatz“	2. Die Vorgehensweise gewährleistet, dass umfassend nach möglichen Bedrohungen und Schwachstellen gesucht wird (gefahrenübergreifender Ansatz), die Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse hervorrufen können.
- Rad nicht neu erfinden.	*Dabei SOLLTEN entsprechende Kataloge wie z. B. ENISA Thread Taxonomy, der Annex der ISO 27005 oder die Aufstellung „Elementare Gefährdungen“ des BSI berücksichtigt werden.*

A 2.3 Risikoanalyse

Kommentar / ToDo	VdS 10100
Explizierter formuliert	Jede Risikoanalyse MUSS die folgenden Anforderungen erfüllen:
	1. Ihre Durchführung und ihre Ergebnisse werden dokumentiert.
übernehmen	2. Die Bewertung von Risiken erfolgt auf Basis der potentiellen Schäden und deren Eintrittswahrscheinlichkeit.
übernehmen	3. Das Ergebnis der Risikoanalyse ermöglicht eine Priorisierung bei der Risikobehandlung.

A 2.3 Risikobehandlung

Kommentar / ToDo	VdS 10100
Text gesplittet, in die VdS 10k übernehmen?	Identifizierte Risiken MÜSSEN angemessen und priorisiert behandelt werden.
§ 30 (1): „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen“ → Text der VdS 10k entsprechend angepasst ToDo 0.4.2: Formulierung zu proaktiven und reaktiven	Dazu MÜSSEN geeignete, verhältnismäßige und wirksame technische und/oder organisatorische Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der Risiken (z. B. durch den Abschluss einer Versicherung) definiert, dokumentiert und umgesetzt werden oder die entsprechenden Risiken MÜSSEN akzeptiert werden.

Maßnahmen aufnehmen. Satz in Unterpunkte aufdröseln.	
Mit dieser Formulierung bereiten wir den Ausschluss von IT-Systemen oder gesamten Netzwerksegmenten usw. von den geforderten Maßnahmen vor. Diese Empfehlung stellt eigentlich eine Selbstverständlichkeit dar und kann ggf. gestrichen werden.	*Risiken KÖNNEN generell akzeptiert werden, wenn sie die Kriterien der Risikoakzeptanz (siehe Abschnitt A 2.1) erfüllen.*
neu § 30 Abs. 1 („Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.“) 0.4.4: Dokumentation der Einschätzung der Wirksamkeit gestrichen. Wirksamkeit wird durch die folgenden Maßnahmen geprüft und dokumentiert. 0.5.6: Wird hier gestrichen. Die Einhaltung wird durch die entsprechende Formulierung im Zuge der Überwachung durch das Topmanagement dokumentiert.	~~Die Dokumentation der Maßnahmen MUSS beinhalten, warum sie als geeignet und verhältnismäßig angesehen werden.~~
übernehmen	Die Umsetzung der Maßnahmen MUSS kontrolliert und auf Wirksamkeit geprüft werden.
neu	*Hierzu SOLLTEN erhebliche Risiken einzelnen Mitarbeitern (Risk Owner) zugeordnet und konkrete zeitliche Vorgaben für deren Behandlung definiert werden.*
0.4.4 DISKUSSION: Wir sollten das Wort „erheblich“ einfügen, damit das Topmanagement nicht bei jeder Kleinigkeit einbezogen wird.	Wenn erhebliche Risiken nicht angemessen behandelt werden können, MÜSSEN sie vom Topmanagement akzeptiert und dies dokumentiert werden.

A 2.4 Wiederholung und Anpassung

Kommentar / ToDo	VdS 10100
übernehmen	Risikoidentifikationen, Risikoanalysen und Risikobehandlungen MÜSSEN jährlich auf ihre Aktualität geprüft und bei Bedarf wiederholt werden.
übernehmen	Sie MÜSSEN darüber hinaus zeitnah überarbeitet werden, wenn eine der folgenden Faktoren auftritt:
übernehmen	1. Der untersuchte Gegenstand hat sich wesentlich verändert (z. B. Hardware, Software oder Konfiguration eines IT-Systems).
übernehmen	2. Der Einsatzzweck des untersuchten Gegenstands hat sich wesentlich geändert.
übernehmen	3. Die Gefährdungslage hat sich erhöht (z. B. wenn eine neue Gefährdung bekannt wurde oder sich eine bestehende Gefährdung wesentlich erhöht hat).

A 2.5 Überwachung

Kommentar / ToDo	VdS 10100
§ 38 (1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen. 0.4.4: In Absatz 4.2 übernimmt das Topmanagement die Gesamtverantwortung für die Informationssicherheit. 4.2 G1 und G1.1 zusammenfassen. In die VdS 10k aufnehmen: Hierbei SOLLTE das Risikomanagement berücksichtigt werden (Anhang A.2)	Das Topmanagement MUSS jährlich prüfen, ob die Maßnahmen des Risikomanagements umgesetzt sind und ob Änderungen an gesetzlichen, betrieblichen oder vertraglichen Rahmenbedingungen eine Anpassung der Maßnahmen erforderlich machen.
	Notwendige Anpassungen MÜSSEN zeitnah implementiert werden.
0.5.6-ToDo: Die Prüfung bzw. Freigabe der Risikomanagementmaßnahmen gem. § 30 (1) MUSS dokumentiert werden (positive Prüfung) 0.5.8-DISKUSSION: Unter dem Begriff „Risikomanagementmaßnahmen“ können zwei unterschiedliche Dinge verstanden werden: - die Maßnahmen, die das Risikomanagement definieren - die Maßnahmen, die durch das Risikomanagement als notwendig definiert wurden	