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

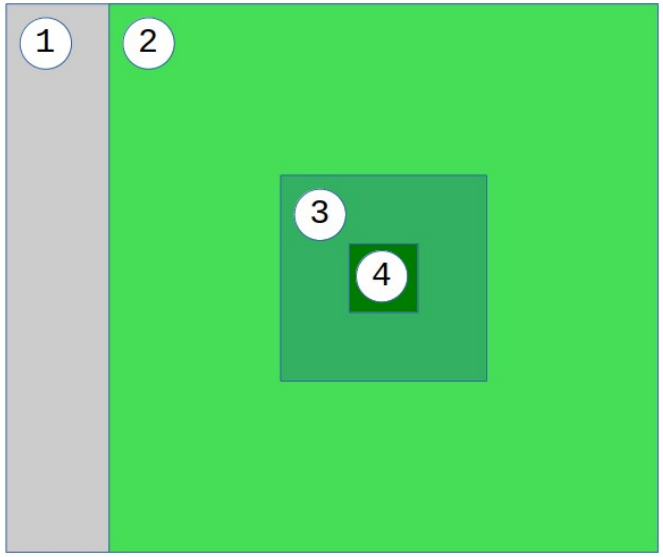
Feedback welcome!

Vorbemerkung:

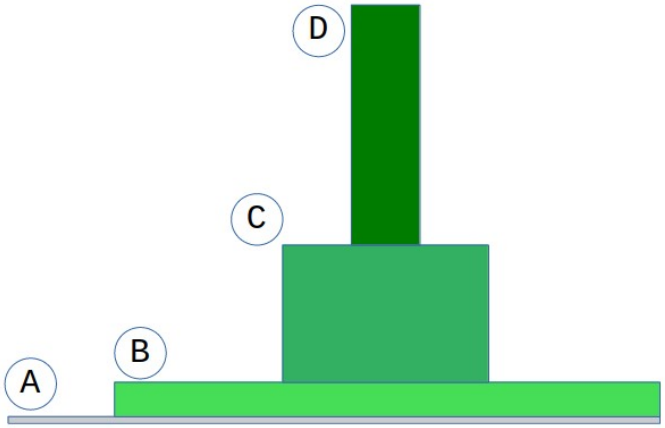
Die Anforderungen von NIS2 sind umfangreich und z. T. aktuell noch widersprüchlich (deshalb sind konkret geforderte Maßnahmen gem § 30 (2) im aktuellen Entwurf noch nicht aufgenommen.
Die betroffenen Organisationen sind verpflichtet, ihre „informationstechnischen Systeme, Komponenten und Prozesse, die 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 Gesetzesentwurf 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.“ Deshalb wird in Abschnitt 1.2 der VdS 10100 (Anwendungs- und Geltungsbereich) festgelegt, dass die Richtlinien in der gesamten Organisation umzusetzen sind.

Gleichzeitig wird im Gesetzestext 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).
Der Aufwand für die Umsetzung gängiger Regelwerke wird z. B. dadurch beschränkt, dass ein Geltungsbereich definiert werden kann. Dies scheint hier nicht möglich zu sein.
Um den Implementationsaufwand zu reduzieren und die zur Verfügung stehenden Ressourcen möglichst effektiv und effizient für die Informationssicherheit einzusetzen, werden wir folgende Vorgehensweise umsetzen:

1. Kriterien für Risikoakzeptanz festlegen (Anhang A.2)
2. Analyse: Welche Teile der IT-Infrastruktur liegen unterhalb der Risikoakzeptanz-Grenze (die Schadenshöhe im Eintrittsfall ist zu gering). Diese Teile werden nicht abgesichert!
3. Der verbleibende Teil wird gem. VdS 10000 behandelt, ggf. mit einer weiteren Klasse („wichtige Teile der IT-Infrastruktur“).



1: IT-Infrastruktur, bei der eine Verletzung ihrer Vertraulichkeit, Verfügbarkeit und Authentizität nur zu einem vernachlässigbaren Schaden führen kann (Risikoakzeptanzgrenze, siehe Anhang A 2) und die von der restlichen IT-Infrastruktur abgeschottet ist
2: die gesamte IT-Infrastruktur mit Ausnahme von (1)
3: IT-Infrastruktur, die für den Betrieb der zentralen Prozesse und der Prozesse mit hohem Schadenspotential unverzichtbar ist
4: besonders sensible IT-Infrastruktur



A: keine Schutzmaßnahmen
B: Basisschiutz der VdS 10000
C: Basisschutz plus individuelle Risikoanalyse
D: Basisschutz plus individuelle Risikoanalyse plus konkrete Maßnahmen

VdS 10100, Version 0.1.0 vom 24.06.2024

0 VdS-Richtlinien für die Informationsverarbeitung

VdS-Richtlinie zur Umsetzung von NIS2

Inhaltsverzeichnis

Vorbemerkung: 1
VdS 10100, Version 0.1.0 vom 24.06.2024 3
0 VdS-Richtlinien für die Informationsverarbeitung 3
VdS-Richtlinie zur Umsetzung von NIS2 3
Anforderungen 7
1 Allgemeines 7
1.1 Anwendungshinweise 7
1.2 Anwendungs- und Geltungsbereich 9
1.2.1 Analyse und Registrierung 9
1.3 Gültigkeit 10
2 Normative Verweise 10
Begriffe 12
4 Organisation der Informationssicherheit 21
4.1 Verantwortlichkeiten 21
4.1.1 Zuweisung und Dokumentation 21
4.1.2 Funktionstrennungen 22
4.1.3 Zeitliche Ressourcen 22
4.1.4 Delegieren von Aufgaben 23
4.2 Topmanagement 23
4.3 Informationssicherheitsbeauftragter (ISB) 24
4.4 Informationssicherheitsteam (IST) 24
4.5 IT-Verantwortliche 25
4.6 Administratoren 26
4.7 Vorgesetzte 26
4.8 Mitarbeiter 26
4.9 Projektverantwortliche 26
4.10 Externe 27
5 Leitlinie zur Informationssicherheit (IS-Leitlinie) 27
5.1 Allgemeine Anforderungen 27

5.2 Inhalte ... 28
6 Richtlinien zur Informationssicherheit (IS-Richtlinien) ... 28
6.1 Allgemeine Anforderungen ... 28
6.2 Inhalte ... 29
6.3 Regelungen für Nutzer ... 29
6.4 Weitere Regelungen ... 31
7 Mitarbeiter ... 32
7.1 Vor Aufnahme der Tätigkeit ... 32
7.2 Aufnahme der Tätigkeit ... 32
7.3 Beendigung oder Wechsel der Tätigkeit ... 33
8 Wissen ... 33
8.1 Aktualität des Wissens ... 33
8.2 Schulung und Sensibilisierung ... 34
9 Identifizieren wichtiger und besonders schützenswerter IT-Ressourcen ... 36
9.1 Prozesse ... 37
9.1 Wichtige IT-Ressourcen ... 37
9.2 Besonders sensible Informationen ... 38
9.3 IT-Ressourcen ... 40
10 IT-Systeme ... 41
10.1 Inventarisierung ... 41
10.2 Lebenszyklus ... 42
10.2.1 Inbetriebnahme und Änderung ... 42
10.2.2 Ausmusterung und Wiederverwendung ... 43
10.3 Basisschutz ... 44
10.3.1 Software ... 45
10.3.2 Beschränkung des Netzwerkverkehrs ... 45
10.3.3 Protokollierung ... 46
10.3.4 Externe Schnittstellen und Laufwerke ... 46
10.3.5 Schadsoftware ... 47
10.3.6 Starten von fremden Medien ... 47
10.3.7 Authentifizierung ... 47
10.3.8 Zugänge und Zugriffe ... 49
10.4 Zusätzliche Maßnahmen für mobile IT-Systeme ... 49
10.4.1 IS-Richtlinie ... 50
10.4.2 Schutz der Informationen ... 50
10.4.3 Verlust ... 51
10.5 Zusätzliche Maßnahmen für wichtige IT-Systeme ... 51
10.5 Zusätzliche Maßnahmen für besonders sensible IT-Systeme ... 52
10.5.1 Risikoanalyse und -behandlung ... 52

10.5.2 Notbetriebsniveau ... 52
10.5.3 Robustheit ... 52
10.5.4 Externe Schnittstellen und Laufwerke ... 53
10.5.5 Änderungsmanagement ... 53
10.5.6 Dokumentation ... 53
10.5.7 Datensicherung ... 54
10.5.8 Überwachung ... 54
10.5.9 Ersatzsysteme und -verfahren ... 54
10.5.10 Kritische Individualsoftware ... 55
11 Netzwerke und Verbindungen ... 55
11.1 Netzwerkplan ... 55
11.2 Aktive Netzwerkkomponenten ... 56
11.3 Netzübergänge ... 56
11.4 Basisschutz ... 57
11.4.1 Netzwerkanschlüsse ... 58
11.4.2 Segmentierung ... 58
11.4.3 Fernzugang ... 58
11.4.4 Netzwerkkopplung ... 59
11.5 Zusätzliche Maßnahmen für kritische Verbindungen ... 59
12 Mobile Datenträger ... 60
12.1 IS-Richtlinie ... 60
12.2 Schutz der Informationen ... 60
12.3 Zusätzliche Maßnahmen für kritische mobile Datenträger ... 61
13 Umgebung ... 61
13.1 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen ... 61
13.2 Datenleitungen ... 62
13.3 Zusätzliche Maßnahmen für kritische IT-Systeme ... 62
14 IT-Outsourcing und Cloud Computing ... 63
14.1 IS-Richtlinie ... 63
14.2 Vorbereitung ... 63
14.3 Vertragsgestaltung ... 64
14.4 Zusätzliche Maßnahmen für kritische IT-Ressourcen ... 65
15 Zugänge und Zugriffsrechte ... 66
15.1 Verwaltung ... 66
15.2 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen ... 67
16 Datensicherung und Archivierung ... 67
16.1 IS-Richtlinie ... 68
16.2 Archivierung ... 68
16.3 Verfahren ... 68

16.4 Weiterentwicklung ... 69
16.5 Basisschutz ... 70
16.5.1 Speicherorte ... 71
16.5.2 Server ... 71
16.5.3 Aktive Netzwerkkomponenten ... 71
16.5.4 Mobile IT-Systeme ... 71
16.6 Zusätzliche Maßnahmen für kritische IT-Systeme ... 71
16.6.1 Risikoanalyse ... 72
16.6.2 Verfahren ... 72
17 Sicherheitsvorfälle ... 72
17.1 IS-Richtlinie ... 73
17.2 Erkennen ... 74
17.3 Reaktion ... 74
17.4 Zusätzliche Maßnahmen für kritische IT-Systeme ... 76
17.4.1 Wiederanlaufpläne ... 76
17.4.2 Abhängigkeiten ... 77
Anhang A ... 78
A 1 Verfahren ... 78
A 2 Risikomanagement ... 78
A 2.1 Methodik ... 79
A 2.2 Risikoanalyse ... 80
A 2.3 Risikobehandlung ... 81
A 2.4 Wiederholung und Anpassung ... 81
A 2.5 Überwachung ... 82

Anforderungen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	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.	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Für die Abwehr „klassischer“ Gefahren stehen etablierte Schutz-Standards, insbesondere die Richtlinien der VdS Schadenverhütung GmbH, zur Verfügung. Digitalisierung und Vernetzung bergen jedoch auch neue Gefahren, die Unternehmen in ihrem Risikomanagement berücksichtigen müssen. Eine gut organisierte Informationssicherheit vermindert die Anzahl der Schwachstellen, verringert die verbleibenden Risiken und begrenzt dadurch potentielle Schäden für das Unternehmen.	Muss neu verfasst werden. Low Prio.	
T2	Die vorliegenden Richtlinien legen Mindestanforderungen an die Informationssicherheit fest und beschreiben ein auf kleine und mittlere Unternehmen (KMU) zugeschnittenes Informationssicherheitsmanagementsystem (ISMS).	Streichen.	

1.1 Anwendungshinweise

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Die vorliegenden Richtlinien sind Grundlage für eine Zertifizierung durch VdS Schadenverhütung.	übernehmen	Die vorliegenden Richtlinien sind Grundlage für eine Zertifizierung durch VdS Schadenverhütung.
T2	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	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.
T3	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	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.
E1	*Diese Richtlinien SOLLTEN in bestehende Managementsysteme integriert werden, um potentielle Synergieeffekte zu nutzen.*	übernehmen	*Diese Richtlinien SOLLTEN in bestehende Managementsysteme, insbesondere in das Qualitätsmanagement und in das Risikomanagement integriert werden, um potentielle Synergieeffekte zu nutzen.*
E2	*Insbesondere SOLLTEN sie zusammen mit den Richtlinien VdS 10010 „VdS-Richtlinien zur Umsetzung der DSGVO“ und/oder den Richtlinien VdS 10020 „Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme“ implementiert werden.*	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.
		Referenzierung auf die VdS 10000 aufnehmen: VdS 10100 baut auf der VdS 10000 auf, jedoch ist die vollständige Umsetzung der VdS 10000 nicht zwingend notwendig.	*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.
T4	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.	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Diese Richtlinien sind für KMU, den gehobenen Mittelstand, Verwaltungen, Verbände und sonstige Organisationen anwendbar.	anpassen	Diese Richtlinie ist für Organisationen anwendbar, die als „wichtige“ oder „besonders wichtige“ Einrichtungen im Sinne des BSIG gelten oder gelten könnten. Sie ist nicht für Betreiber kritischer Anlagen im Sinne des BSIG geeignet.
E1	*Die Richtlinien SOLLTEN auf die gesamte Organisation angewendet werden, ihr Geltungsbereich KANN jedoch technisch, geographisch und/oder organisatorisch eingegrenzt werden.*	Gem. NIS2 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

Ref	VdS 10000	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	Die Organisation MUSS prüfen, ob sie als „wichtige“ oder „sehr wichtige“ Einrichtung im Sinne von § 28 BSIG gilt.

		eine 1:1 Wiederholung des Gesetzestextes und deshalb nicht sinnvoll. Idee: In die VdS 10100 wird eine sehr einfache Maßnahme aufgenommen und ansonsten auf den Gesetzestext oder eine Checkliste verwiesen. Letztere stellt die VdS Schadenverhütung online oder als PDF zur Verfügung.	Dazu SOLLTE die entsprechende Vorgehensweise genutzt werden, die von der VdS Schadenverhütung zur Verfügung gestellt wird. Das Ergebnis der Prüfung MUSS zusammen mit seiner Begründung dokumentiert werden.
-	-	§ 33 Abs. 1 - Verbessern: „innerhalb von drei Monaten“ → nach welchem Zeitpunkt?!	Es MUSS ein Verfahren etabliert werden, das sicherstellt, dass das entsprechende Registrierungsverfahren gem. BSIG § 33 innerhalb von drei Monaten durchlaufen wird.
-	-	§ 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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Diese Richtlinien gelten ab dem 9.10.2018 und ersetzen die VdS-Richtlinien 3473 vom 01.07.2015.	anpassen	Diese Richtlinien gelten ab dem 01.11.2024

2 Normative Verweise

Ref	VdS 10000	Kommentar / ToDo	VdS 10100

T1	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	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.
V1	BSI-Standard 100-4 Notfallmanagement	Unklar, ob in der VdS 101000 auf dieses Regelwerk verwiesen werden wird.	
V2	BSI-Standard 200-2 IT-Grundschutz-Vorgehensweise	Unklar, ob in der VdS 101000 auf dieses Regelwerk verwiesen werden wird.	
V3	BSI-Standard 200-3 Risikomanagement	Unklar, ob in der VdS 101000 auf dieses Regelwerk verwiesen werden wird.	
V4	DIN EN 1047-1 Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Teil 1: Datensicherungsschränke und Disketteneinsätze	Die VdS 10100 wird voraussichtlich nicht auf dieses Regelwerk verweisen.	
V5	DIN EN 50173-Reihe Informationstechnik – Anwendungsneutrale Kommunikationskabelanlagen	Die VdS 10100 wird voraussichtlich nicht auf dieses Regelwerk verweisen.	
V6	DIN EN 50174-Reihe Informationstechnik – Installation von Kommunikationsverkabelung	Die VdS 10100 wird voraussichtlich nicht auf dieses Regelwerk verweisen.	
V7	DIN EN ISO 9001 Qualitätsmanagementsysteme – Anforderungen	Unklar, ob in der VdS 101000 auf dieses Regelwerk verwiesen werden wird.	
V8	DIN EN ISO 22301 Sicherheit und Schutz des Gemeinwesens - Business Continuity Management System - Anforderungen	Unklar, ob in der VdS 101000 auf dieses Regelwerk verwiesen werden wird.	
V9	DIN VDE 0100 Normenreihe zum Errichten von Niederspannungsanlagen	Die VdS 10100 wird voraussichtlich nicht auf dieses Regelwerk verweisen.	
V10	ISO 31000 Risk Management – Principles and guidelines	Wir verweisen auf dieses Regelwerk in Abschnitt A 2.2 Risikoanalyse.	ISO 31000 Risk Management – Principles and guidelines
V11	ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements	Unklar, ob in der VdS 101000 auf dieses Regelwerk verwiesen werden wird.	

V12	ISO/IEC 27005 Information technology — Security techniques — Information security risk management	Wir verweisen auf dieses Regelwerk in Abschnitt A 2.2 Risikoanalyse.	ISO/IEC 27005 Information technology — Security techniques — Information security risk management
V13	VdS 2007 Anlagen der Informationstechnologie (IT-Anlagen) - Merkblatt zur Schadenverhütung	Die VdS 10100 wird voraussichtlich nicht auf dieses Regelwerk verweisen.	
			IEC 31010:2019 - Risk assessment techniques
			VdS 10000 - Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU)
		Wir verweisen auf dieses Regelwerk in Abschnitt A 2.2 Risikoanalyse.	ENISA Thread Taxonomy
		Wir verweisen auf dieses Regelwerk in Abschnitt A 2.2 Risikoanalyse.	„Elementare Gefährdungen“, BSI

Begriffe

ToDo: Begriffe aus NIS2 im Laufe der Entwicklung in dieses Kapitel aufnehmen und jene Begriffe entfernen, die in der VdS 10100 nicht neu definiert werden müssen.

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

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.		
40	**Maximal tolerierbare Ausfallzeit (MTA):** Zeit, bis zu der eine definierte Leistung (z. B. ein Notbetriebsniveau) wieder verfügbar sein muss.		
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.		
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.	Neu definieren gem. NIS2-Richtlinie (siehe unten).	
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.		
		ToDo	erheblicher Sicherheitsvorfall: Sicherheitsvorfall, der (...)
		ToDo: Wir verwenden in der VdS 10100 den Begriff „Organisation (gem. VdS 10000 / ISO 27001), NIS2 spricht von „Einrichtungen“. Ausgleich über eine entsprechende Definition finden.	Organisation: … Im Sinne von NIS-2 eine Einrichtung
		Entsprechende Definition In der VdS 10k anpassen.	Sicherheitsvorfall: Ungewöhnliches Ereignis, dass die Verfügbarkeit , Integrität und/oder Vertraulichkeit von Informationen oder der Informationsverarbeitung beeinträchtigt.
			Stand der Technik: Fortschrittliches, bereits praxiserprobtes Verfahren, das von Experten und Fachkreisen allgemein unterstützt und in

			professionellen Umgebungen eingesetzt wird.

4 Organisation der Informationssicherheit

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Um mit möglichst geringem Aufwand das notwendige Sicherheitsniveau zu definieren, umzusetzen und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage anzupassen, ist es notwendig, eine entsprechende Organisation zu etablieren.	ToDo: Text entwerfen, der auf NIS2 abgestimmt ist.	

4.1 Verantwortlichkeiten

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Verantwortlichkeiten (siehe Abschnitte 4.2 bis 4.10) MÜSSEN eindeutig und widerspruchsfrei zugewiesen werden.	NIS2 enthält zu diesem Gebiet keine Vorgaben.	Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.

4.1.1 Zuweisung und Dokumentation

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MUSS für jede Verantwortlichkeit dokumentiert werden:	NIS2 enthält zu diesem Gebiet keine Vorgaben.	Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.
G1.1	1. welche Ziele erreicht werden sollen		
G1.2	2. für welche Ressourcen die Verantwortlichkeit besteht		
G1.3	3. welche Aufgaben erfüllt werden müssen, damit die Ziele erreicht werden		
G1.4	4. welche Berechtigungen an die Verantwortlichkeit gebunden sind, um diese wahrnehmen zu können		
G1.5	5. welche Ressourcen für die Wahrnehmung der Verantwortlichkeit zur Verfügung stehen		
G1.6	6. wie und durch welche Position(en) die Erfüllung der Verantwortlichkeit überprüft wird		

G1.7	7. welche Positionen die Verantwortlichkeit wahrnehmen		

4.1.2 Funktionstrennungen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Bei der Verteilung der Verantwortlichkeiten MUSS das Prinzip der Funktionstrennung umgesetzt werden. Widersprüchliche Verantwortlichkeiten DÜRFEN NICHT von ein und derselben Person oder Organisationseinheit wahrgenommen werden.	NIS2 enthält zu diesem Gebiet keine Vorgaben.	Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.
E1	*Wenn eine Funktionstrennung nicht oder nur mit einem unverhältnismäßig hohen Aufwand durchführbar ist, KÖNNEN widersprüchliche Verantwortlichkeiten von ein und derselben Person oder Organisationseinheit wahrgenommen werden.*		
G2	In diesem Fall MÜSSEN folgende Anforderungen erfüllt werden:		
G2.1	1. Die rechtliche Zulässigkeit wurde geprüft.		
G2.2	2. Es werden andere Maßnahmen wie Überwachung von Tätigkeiten, Kontrollen oder Leitungsaufsicht umgesetzt.		
G2.3	3. Die nicht durchgeführte Funktionstrennung wird in der Dokumentation der Funktionsverteilung (siehe Abschnitt 4.1.1) besonders hervorgehoben und begründet.		
G3	Um Zuständigkeitslücken oder Überschneidungen von Verantwortlichkeiten zu vermeiden, MÜSSEN die entsprechenden Regelungen jährlich vom Informationssicherheitsbeauftragten (ISB) überprüft werden.		

4.1.3 Zeitliche Ressourcen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Um zugewiesene Verantwortlichkeiten	NIS2 enthält zu diesem Gebiet keine Vorgaben.	Dieser Abschnitt SOLLTE gemäß der VdS 10000

	wahrzunehmen, MÜSSEN die entsprechenden Mitarbeiter im erforderlichen Umfang (siehe Abschnitt 4.1.1) von anderen Tätigkeiten freigestellt werden.		umgesetzt werden.

4.1.4 Delegieren von Aufgaben

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
E1	*Verantwortliche für Informationssicherheit KÖNNEN Aufgaben an andere Personen delegieren.*	NIS2 enthält zu diesem Gebiet keine Vorgaben.	*Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.*
G1	Die Verantwortung für delegierte Aufgaben verbleibt jedoch bei ihnen, sodass sie die Erfüllung und das Ergebnis der delegierten Aufgaben überprüfen MÜSSEN.		

4.2 Topmanagement

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Das Topmanagement MUSS sich zur Wahrnehmung folgender Verantwortlichkeiten verpflichten:	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.
G1.1	1. Übernehmen der Gesamtverantwortung für die Informationssicherheit		
G1.2	2. In Kraft setzen von Richtlinien für die Informationssicherheit (IS-Richtlinien)		
G1.3	3. Bereitstellen der notwendigen technischen, finanziellen und personellen Ressourcen für die Informationssicherheit		
G1.4	4. Einbetten der Informationssicherheit in die Strukturen, Hierarchien und Arbeitsabläufe der Organisation		
		§ 38 Abschnitt 1	Zusätzlich MUSS sich das Topmanagement dazu verpflichten, die Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.

4.3 Informationssicherheitsbeauftragter (ISB)

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Das Topmanagement MUSS die Verantwortlichkeiten eines Informationssicherheitsbeauftragten (ISB) einem Mitarbeiter zuweisen.	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.
G2	Dieser MUSS darauf hinwirken, dass die in der Leitlinie zur Informationssicherheit (IS-Leitlinie) definierten Ziele der Informationssicherheit erreicht werden.		
G3	Hierfür MUSS er insbesondere die folgenden Verantwortlichkeiten wahrnehmen:		
G3.1	1. Steuern, Koordinieren und Prüfen der technischen und organisatorischen Maßnahmen, kontinuierliches Verbessern der Informationssicherheit, insbesondere Anpassen der Informationssicherheit an neue Bedrohungen, Änderungen im technischen und organisatorischen Umfeld und an neue gesetzliche, betriebliche und vertragliche Anforderungen	Änderung in der VdS 10000: Risikomanagement erwähnen bzw. stärken! Aufbau verbessern.	
G3.2	2. jährliches Berichten an das Informationssicherheitsteam (IST) über den aktuellen Stand der Informationssicherheit, insbesondere über Mängel, Risiken und Sicherheitsvorfälle	Änderung in der VdS 10000: Risikomanagement erwähnen bzw. stärken!	
E1.1	*Es SOLLTE sichergestellt werden, dass die Verantwortlichkeiten des ISB auch in seiner Abwesenheit wahrgenommen werden.*	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	
E1.2	*Dies KANN z. B. durch eine Stellvertreterregelung umgesetzt werden.*		

4.4 Informationssicherheitsteam (IST)

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Das Topmanagement MUSS ein Informationssicherheitsteam (IST) bestellen.	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

G2	In diesem MÜSSEN folgende Organisationseinheiten bzw. Positionen persönlich oder durch einen Repräsentanten vertreten sein:	Umsetzung von NIS2 unerlässlich.	
G2.1	1. Topmanagement		
G2.2	2. ISB		
G2.3	3. IT-Verantwortliche		
G2.4	4. Mitarbeiter (z. B. über Betriebsrat)		
G2.5	5. Verantwortliche für den Datenschutz (z. B. Datenschutzmanager und/oder Datenschutzbeauftragter)		
G3	Das Team MUSS den ISB unterstützen, insbesondere bei den folgenden Tätigkeiten:		
G3.1	1. Erkennen und Bewerten neuer Bedrohungen und Schwachstellen		
G3.2	2. Entwickeln und Bewerten von Maßnahmen zur Informationssicherheit		
G3.3	3. organisationsweites Steuern und Koordinieren der Maßnahmen zur Informationssicherheit		

4.5 IT-Verantwortliche

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Aufgaben eines IT-Verantwortlichen MÜSSEN vom Topmanagement mindestens einem Mitarbeiter zugewiesen werden.	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.
G2	IT-Verantwortliche MÜSSEN folgende Aufgaben wahrnehmen:		
G2.1	1. Umsetzen der IS-Richtlinien in ihrem Verantwortungsbereich durch entsprechende technische und organisatorische Maßnahmen		
G2.2	2. Abstimmen aller Maßnahmen mit dem ISB, die aus ihrer Sicht zur Verbesserung und Erhaltung der Informationssicherheit in ihrem Verantwortungsbereich ergriffen werden müssen sowie deren Planung, Koordination und Umsetzung		

4.6 Administratoren

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Verantwortlichkeiten eines Administrators MÜSSEN mindestens einem Mitarbeiter zugewiesen werden.	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.
G2	Administratoren MÜSSEN in Abstimmung mit dem IT-Verantwortlichen die technischen Maßnahmen für die Informationssicherheit implementieren.		

4.7 Vorgesetzte

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Vorgesetzte, die Verantwortung für Mitarbeiter tragen, MÜSSEN sicherstellen, dass die getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeiter umgesetzt werden.	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

4.8 Mitarbeiter

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Mitarbeiter MÜSSEN folgende Aufgaben wahrnehmen:	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.
G1.1	1. Einhalten und Umsetzen aller sie oder ihre Tätigkeit betreffenden Maßnahmen zur Informationssicherheit		
G1.2	2. Melden von Störungen, Ausfällen und Sicherheitsvorfällen		

4.9 Projektverantwortliche

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Projektverantwortliche MÜSSEN den ISB bei allen Projekten mit Auswirkung auf die Informationsverarbeitung konsultieren, um	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

	sicherzustellen, dass sicherheitsrelevante Aspekte ausreichend beachtet werden.		

4.10 Externe

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Externe MÜSSEN verpflichtet werden, die sie betreffenden Maßnahmen und Regelungen zur Informationssicherheit einzuhalten bzw. umzusetzen, sofern sie Zugriff auf kritische Informationen besitzen oder sie nichtöffentliche Bereiche der Informationstechnologie (IT) der Organisation nutzen.	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 unerlässlich.	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.

5 Leitlinie zur Informationssicherheit (IS-Leitlinie)

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	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.	NIS2 enthält zu diesem Gebiet keine Vorgaben. Diese Vorgaben sind jedoch für die effektive und effiziente Umsetzung von NIS2 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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Leitlinie MUSS vom Topmanagement erstellt und in Kraft gesetzt werden.		Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.
G2	Das Topmanagement MUSS die Leitlinie jährlich auf Aktualität prüfen und bei Bedarf aktualisieren.		
G3	Die Leitlinie MUSS nach jeder Aktualisierung zeitnah bekannt gegeben werden und in der jeweils aktuellen Form allen Betroffenen zur Verfügung stehen.		

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.

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Leitlinie MUSS folgende Anforderungen erfüllen:	1:1 VdS 10k	Die Leitlinie MUSS folgende Anforderungen erfüllen:
G1.1	1. Sie definiert die Ziele und den Stellenwert der Informationssicherheit in der Organisation.	Anforderungen der VdS 10k plus Umsetzung von NIS2 als Ziel.	1. Sie definiert die Ziele und den Stellenwert der Informationssicherheit in der Organisation, insbesondere die Umsetzung der EU-Richtlinie NIS2.
G1.2	2. Sie definiert sämtliche erforderlichen Positionen (siehe Abschnitte 4.2 bis 4.10) und weist auf deren Aufgaben hin.	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.
E1	*Die Leitlinie SOLLTE auf die Konsequenzen ihrer Nichtbeachtung hinweisen.*	übernehmen	*Die Leitlinie SOLLTE auf die Konsequenzen ihrer Nichtbeachtung hinweisen.*

6 Richtlinien zur Informationssicherheit (IS-Richtlinien)

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	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.	NIS2 basiert auf Risikomanagement (RM). Die im Zuge des RM erkannten organisatorischen Maßnahmen können/sollten/müssen in Richtlinien oder Verfahren verankert werden. Dies sollte bei der Formulierung dieser Anforderung berücksichtigt werden.	

6.1 Allgemeine Anforderungen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Jede IS-Richtlinie MUSS vom ISB unter Mitarbeit des IST erstellt und vom Topmanagement in Kraft gesetzt werden.		Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.
G2	Der ISB MUSS jede IS-Richtlinie jährlich auf Aktualität prüfen und ggf. aktualisieren.		

E1	*Bei der Erstellung und Anpassung von IS-Richtlinien SOLLTEN alle gesetzlichen, behördlichen und vertraglichen Anforderungen ermittelt und entsprechend umgesetzt werden.*		
G3	Die IS-Richtlinien MÜSSEN nach jeder Aktualisierung den Zielgruppen zeitnah bekannt gegeben werden.		
G4	Dies MUSS in einer für die Zielgruppe zugänglichen und verständlichen Form geschehen, bspw. im Zuge einer Schulung.		
G5	IS-Richtlinien MÜSSEN umgesetzt oder vom Topmanagement aufgehoben werden.		

6.2 Inhalte

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Jede IS-Richtlinie MUSS folgende Anforderungen erfüllen:		Dieser Abschnitt SOLLTE gemäß der VdS 10000 umgesetzt werden.
G1.1	1. Sie enthält, für wen sie verbindlich ist (Zielgruppe).		
G1.2	2. Sie begründet, warum sie erstellt wurde und legt fest, was mit ihr erreicht werden soll.		
G1.3	3. Sie verstößt nicht gegen Leitlinien oder andere Richtlinien.		
G1.4	4. Sie weist auf die Konsequenzen ihrer Nichtbeachtung hin.		
E1	*IS-Richtlinien KÖNNEN begründete Ausnahmen ermöglichen, sofern diese im Vorfeld genehmigt und dokumentiert werden.*		
E2	*IS-Richtlinien KÖNNEN auf weitere mitgeltende Unterlagen verweisen.*		

6.3 Regelungen für Nutzer

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MÜSSEN Regelungen für den Umgang mit der		

	IT getroffen werden, die in ihrer Gesamtheit für alle Nutzer (inkl. aller Führungsebenen) sowie für die gesamte IT verbindlich sind:		
G1.1	1. Generelle Nutzungsbedingungen		
G1.1.a	a. Das unrechtmäßige Abrufen oder Verbreiten von urheberrechtlich geschützten Inhalten wird untersagt.		
G1.1.b	b. Das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten wird untersagt.		
G1.2	2. Privatnutzung		
G1.2.a	a. Es wird definiert, ob die private Nutzung der IT erlaubt ist.		
G1.2.b	b. Wenn die private Nutzung der IT erlaubt ist, so wird sie im Sinne der Organisation ausgestaltet.		
G1.3	3. Grundlegende Verhaltensregeln		
G1.3.a	a. Es wird nur freigegebene Hard- und Software in der IT-Infrastruktur installiert, genutzt oder betrieben.		
G1.3.b	b. Es wird untersagt, eigenmächtig Netzübergänge (wie z. B. Zugänge zum Internet, Fernwartungszugänge oder VPN-Verbindungen) zu installieren; es werden ausschließlich die von der Organisation bereitgestellten Netzübergänge genutzt.		
G1.3.c	c. Die in der IT-Infrastruktur installierten Sicherheitseinrichtungen werden nicht eigenmächtig deinstalliert, deaktiviert oder in ihrer Konfiguration verändert bzw. mutwillig umgangen.		
G1.3.d	d. Authentifizierungsmerkmale werden nicht weitergegeben.		
G1.4	4. Umgang mit den Informationen der Organisation		
G1.4.a	a. Informationen der Organisation werden nicht eigenmächtig verschlüsselt oder vor lesendem Zugriff geschützt; hierfür werden die von der Organisation explizit freigegebenen technischen		

	Verfahren genutzt.		
G1.5	5. Informationsfluss bei Abwesenheit		
G1.5.a	a. Es wird geregelt, ob neu eintreffende Nachrichten für einen abwesenden Nutzer weitergeleitet werden.		
G1.5.b	b. Es wird geregelt, ob und wann auf den Datenbestand eines Abwesenden zugegriffen werden darf.		
G1.6	6. Missbrauchskontrolle		
G1.6.a	a. Es werden Mechanismen zur Missbrauchskontrolle definiert und den Betroffenen mitgeteilt.		
E1	*Bei der Umsetzung von Überwachungs- und Protokollierungsmaßnahmen SOLLTEN die gesetzlichen Vorgaben, insbesondere die des Datenschutzes, beachtet werden.*		
G2	Ausnahmen MÜSSEN vom ISB genehmigt werden.		

6.4 Weitere Regelungen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Im Rahmen dieser VdS-Richtlinien MÜSSEN ggf. weitere themenspezifische IS-Richtlinien erarbeitet werden:		
G1.1	1. Mobile IT-Systeme (siehe Abschnitt 10.4)		
G1.2	2. Mobile Datenträger (siehe Abschnitt 12.1)		
G1.3	3. IT-Outsourcing und Cloud Computing (siehe Abschnitt 14.1)		
G1.4	4. Datensicherung (siehe Abschnitt 16.1)		
G1.5	5. Störungen und Ausfälle (siehe Abschnitt 17.1)		
G1.6	6. Sicherheitsvorfälle (siehe Abschnitt 18.1)		
G2	Der Bedarf für weitere IS-Richtlinien MUSS jährlich vom ISB ermittelt werden.		

7 Mitarbeiter

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Wenn eine für die Informationssicherheit relevante Position besetzt wird, MUSS die Organisation sicherstellen, dass der Bewerber über die notwendige Eignung und die erforderliche Vertrauenswürdigkeit verfügt.		

7.2 Aufnahme der Tätigkeit

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das im Zuge der Aufnahme der Tätigkeit eines Mitarbeiters folgende Punkte sicherstellt:		
G1.1	1. Mitarbeiter verpflichten sich mittels einer schriftlichen Erklärung zur Vertraulichkeit; die Erklärung definiert auch die Pflichten in Bezug auf Informationssicherheit, die nach Beendigung oder Veränderung des Arbeitsverhältnisses fortbestehen.		
G1.2	2. Mitarbeiter werden in die IS-Leitlinie und in sämtliche für sie relevante Regelungen zur Informationssicherheit (wie z. B. in die Inhalte entsprechender Richtlinien und Verfahren) eingewiesen.		
G1.3	3. Mitarbeiter werden im Umgang mit den für sie		

	relevanten Sicherheitsmaßnahmen geschult (siehe Abschnitt 8.2).		
G1.4	4. Mitarbeiter erhalten die benötigten IT-Ressourcen, Zugänge und Zugriffsrechte und werden in deren Nutzung geschult.		

7.3 Beendigung oder Wechsel der Tätigkeit

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das bei Beendigung oder Wechsel der Tätigkeit eines Mitarbeiters folgende Punkte sicherstellt:		
G1.1	1. Soweit erforderlich, werden Mitarbeiter, Kunden sowie relevante externe Stellen über die Änderungen informiert.		
G1.2	2. Die zur Verfügung gestellten IT-Ressourcen, Zugänge und Zugriffsrechte des Mitarbeiters werden umgehend überprüft und bei Bedarf angepasst.		

8 Wissen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	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.	Anpassen an NIS2. Low Prio.	

8.1 Aktualität des Wissens

Ref	VdS 10000	Kommentar / ToDo	VdS 10100

G1	Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, mit dem alle relevanten Stellen der Organisation sowie ggf. relevante externe Stellen in geeigneter Weise über geänderte rechtliche und technische Bedingungen im Bereich der Informationssicherheit informiert werden.	1:1 übernehmen	Dieser Abschnitt MUSS gemäß der VdS 10000 umgesetzt werden.
G2	Das Verfahren MUSS folgende Punkte sicherstellen:		
G2.1	1. Es werden regelmäßig aus verlässlichen Quellen Informationen über die aktuellen technischen und rechtlichen Entwicklungen im Bereich der Informationssicherheit, insbesondere über neue Gefährdungen und mögliche Gegenmaßnahmen, bezogen.		
G2.2	2. Die Informationen werden im Hinblick auf die Bedeutung für die Informationssicherheit zeitnah ausgewertet, um geänderte Gefahrenlagen zu erkennen.		
G2.3	3. Die jeweils Verantwortlichen werden über relevante Entwicklungen zeitnah informiert.		
E1	*Es SOLLTEN Kontakte und Verbindungen zu Interessengruppen und Sicherheitsforen gepflegt werden, damit die Verantwortlichen auf dem aktuellen Wissensstand sind und auf Fachinformationen und -beratung zugreifen können.*		
		§5 BSIG § 5 (Allgemeine Meldestelle für die Sicherheit in der Informationstechnik), Abs. 3	*Zusätzlich SOLLTE das entsprechende Verfahren sicherstellen, dass die Organisation Warnungen, Empfehlungen und Hinweise des BSI erhält und auswertet.*

8.2 Schulung und Sensibilisierung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MUSS ein Verfahren (siehe Anhang A 1) für Schulungs- und Sensibilisierungsmaßnahmen implementiert werden, das folgende Punkte		

	sicherstellt:		
G1.1	1. Sie werden regelmäßig sowie bei Bedarf durchgeführt.		
G1.2	2. Ihre Art und ihr Intervall werden zielgruppenorientiert festgelegt.		
G1.3	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).		
G1.4	4. Sie klären über Gefährdungen auf und schulen den Umgang mit den vorhandenen Sicherheitsmaßnahmen sowie das Verhalten bei ~~Störungen, Ausfällen und~~ Sicherheitsvorfällen.	VdS 10000: „Störungen, Ausfällen und“ streichen, da wir die entsprechenden Kapitel zusammengelegt haben.	
G1.5	5. Sie vermitteln den Teilnehmern ihre Verantwortung für die Informationssicherheit und fördern bei ihnen die Akzeptanz der Sicherheitsmaßnahmen.	Änderung in der VdS 10000: „... technischen und organisatorischen Sicherheitsmaßnahmen...“ um zu verdeutlichen, dass die im RM identifizierten Maßnahmen gemeint sind	
G1.6	6. Ihre Inhalte und die Teilnahme an ihnen werden dokumentiert.		
E1	*Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN mit einer Lernerfolgskontrolle abschließen, um das Verständnis der Teilnehmer und den Bedarf weiterer Schulungs- oder Sensibilisierungsmaßnahmen zu ermitteln.*		
E2	*Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN von den Teilnehmern bewertet werden, um ihren Inhalt, ihre Form und ihren Ablauf zu verbessern.*		
		§ 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.

Kapitel 9 muss überarbeitet und ggf. erweitert werden.
- Ermitteln von informationstechnischen Systeme, Komponenten und Prozesse (haben wir bereits)
- Informationen mit besonderen Anforderungen an die Vertraulichkeit (→ Kryptografie)
- Informationen mit besonderen Anforderungen an die Integrität (→ Kryptografie)
- Ggf. Überschrift ändern in „Kategorisieren der IT-Ressourcen“ o. ä.
- IT-Ressourcen mit geringem Risiko identifizieren → Nein.
- Begriff „kritisch“ ersetzen, sonst kollidieren wir mit KRITIS und den Begrifflichkeiten des BSI (kritisch → sensibel). Das sollten wir ggf. auch in der VdS 10000 machen...?!

9 Identifizieren wichtiger und besonders schützenswerter IT-Ressourcen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Der ISB MUSS die kritischen IT-Ressourcen der Organisation ermitteln, jährlich prüfen, ob die Aufstellung der kritischen IT-Ressourcen aktuell ist und sie bei Bedarf anpassen.	kritisch → wichtige und besonders schützenswerte	Der ISB MUSS die wichtigen und die besonders schützenswerten IT-Ressourcen der Organisation ermitteln, jährlich prüfen, ob die Aufstellung der kritischen IT-Ressourcen aktuell ist und sie bei Bedarf anpassen.
E1	*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	*Die Organisation SOLLTE deshalb eine Informationsklassifizierung auf Basis eines anerkannten Standards wie ISO/IEC 27001 oder eine Schutzbedarfsanalyse gemäß BSI-Standard 200-2 durchführen.*
G2	Wenn eine andere Vorgehensweise gewählt wird,	übernehmen	Wenn eine andere Vorgehensweise gewählt wird,

	so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.		so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.

9.1 Prozesse

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Organisation MUSS ihre zentralen Prozesse und ihre Prozesse mit hohem Schadenspotential identifizieren und dokumentieren.	übernehmen	
G2	Die Dokumentation MUSS folgende Anforderungen erfüllen:	übernehmen	
G2.1	1. Sie enthält eine kurze Beschreibung des Prozesses.	übernehmen	
G2.2	2. Sie begründet, warum der Prozess ein zentraler Prozess bzw. ein Prozess mit hohem Schadenspotential ist.	übernehmen	
G2.3	3. Sie enthält, wer für den Prozess verantwortlich ist (Prozessverantwortlicher).	übernehmen	
G2.4	4. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) des Prozesses.	übernehmen	
G3	Die Aufstellung der Prozesse und deren Dokumentation MUSS vom Topmanagement freigegeben werden.	übernehmen	

9.1 Wichtige IT-Ressourcen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	-	neu	Die Organisation MUSS ihre wichtigen IT-Ressourcen (insbesondere die wichtigen IT-Systeme, mobilen Datenträger, Verbindungen sowie die wichtige Individualsoftware) bestimmen und diese dokumentieren.
D1	-	neu	Wichtige IT-Ressourcen sind IT-Ressourcen, die für den Betrieb von zentralen Prozessen oder für den Betrieb von Prozessen mit hohem

			Schadenspotential (siehe Abschnitt 9.2) unbedingt benötigt werden.
E1	-	neu	*Um wichtige 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.*
G3	-	neu	Die Dokumentation MUSS folgende Anforderungen erfüllen:
G3.1	-	neu	1. Sie enthält eine kurze Beschreibung der wichtigen IT-Ressource.
G3.2	-	neu	2. Sie begründet, warum die IT-Ressource wichtig ist.
G3.3	-	neu	3. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) der IT-Ressource.
G4	-	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.
E3	-	neu	*Bei der Bestimmung der MTA SOLLTEN Abhängigkeiten zwischen wichtigen IT-Ressourcen berücksichtigt werden.*
G5	-	neu	Die Aufstellung der wichtigen IT-Ressourcen und deren Dokumentation MUSS vom IT-Verantwortlichen freigegeben werden.

9.2 Besonders sensible Informationen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Organisation MUSS ermitteln, ob sie kritische Informationen verarbeitet, überträgt und/oder speichert und diese dokumentieren.	kritisch → besonders sensibel	Die Organisation MUSS ermitteln, ob sie besonders sensible Informationen verarbeitet, überträgt und/oder speichert und diese dokumentieren.
D1	Kritische Informationen sind Informationen, bei	kritisch → besonders sensibel	Besonders sensible Informationen sind

	denen folgende Faktoren zu katastrophalen Schäden führen können:		Informationen, bei denen folgende Faktoren zu katastrophalen Schäden führen können:
D1.1	1. unberechtigte Einsicht, Kenntnisnahme oder Weitergabe (Kriterium „Vertraulichkeit“)	übernehmen	1. unberechtigte Einsicht, Kenntnisnahme oder Weitergabe (Kriterium „Vertraulichkeit“)
D1.2	2. Verfälschung (Kriterium „Integrität“)	übernehmen	2. Verfälschung (Kriterium „Integrität“)
D1.3	3. Datenverlust von weniger als 24 Stunden (Kriterium „Maximal tolerierbarer Datenverlust – MTD“)	übernehmen	3. Datenverlust von weniger als 24 Stunden (Kriterium „Maximal tolerierbarer Datenverlust – MTD“)
D1.4	4. Nichtverfügbarkeit im Echtzeitbetrieb (Kriterium „Unmittelbare Verfügbarkeit“)	übernehmen	4. Nichtverfügbarkeit im Echtzeitbetrieb (Kriterium „Unmittelbare Verfügbarkeit“)
G2	Hierfür MÜSSEN die zentralen Prozesse und die Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1) untersucht werden.	übernehmen	Hierfür MÜSSEN die zentralen Prozesse und die Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1) untersucht werden.
G3	Die Dokumentation MUSS folgende Anforderungen erfüllen:	übernehmen	Die Dokumentation MUSS folgende Anforderungen erfüllen:
G3.1	1. Sie enthält die Kriterien, anhand derer die Informationen als kritisch eingestuft wurden.	kritisch → besonders sensibel	1. Sie enthält die Kriterien, anhand derer die Informationen als besonders sensibel eingestuft wurden.
E1	*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 die Informationen mit den genannten Eigenschaften kritisch sind. Die Erfassung quantitativer und qualitativer Merkmale bietet die Möglichkeit, kritische Informationen zuverlässiger zu erfassen.*	kritisch → besonders sensibel	*Besonders sensible Informationen SOLLTEN anhand ihrer qualitativen und quantitativen Merkmale beschrieben werden. Qualitative Merkmale definieren die Eigenschaften der besonders sensible Informationen. Quantitative Merkmale definieren, ab welcher Menge die Informationen mit den genannten Eigenschaften besonders sensibel sind. Die Erfassung quantitativer und qualitativer Merkmale bietet die Möglichkeit, die entsprechenden Informationen zuverlässiger zu erfassen.*
G3.2	2. Sie begründet, warum die Informationen kritisch sind.	kritisch → besonders sensibel	2. Sie begründet, warum die Informationen besonders sensibel sind.
G4	Die Aufstellung der kritischen Informationen und deren Dokumentation MUSS vom Topmanagement freigegeben werden.	kritisch → besonders sensibel	Die Aufstellung der besonders sensiblen Informationen und deren Dokumentation MUSS vom Topmanagement freigegeben werden.

9.3 IT-Ressourcen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Organisation MUSS ihre kritischen IT-Ressourcen (insbesondere die kritischen IT-Systeme, mobilen Datenträger, Verbindungen sowie die kritische Individualsoftware) bestimmen und diese dokumentieren.	kritisch → besonders sensibel	Die Organisation MUSS ihre besonders sensiblen IT-Ressourcen (insbesondere die besonders sensiblen IT-Systeme, mobilen Datenträger, Verbindungen sowie die besonders sensible Individualsoftware) bestimmen und diese dokumentieren.
D1	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.	kritisch → besonders sensibel	Besonders sensible IT-Ressourcen sind IT-Ressourcen, die besonders sensible Informationen (siehe Abschnitt 9.2) verarbeiten, speichern oder übertragen oder die für den Betrieb von besonders sensiblen IT-Ressourcen zwingend benötigt werden.
G2	Hierfür MÜSSEN die kritischen Informationen (siehe Abschnitt 9.2) untersucht werden.	kritisch → besonders sensibel	Hierfür MÜSSEN die besonders sensiblen Informationen (siehe Abschnitt 9.2) untersucht werden.
E1	*Um IT-Ressourcen zu ermitteln, die kritische Informationen verarbeiten, speichern oder übertragen KANN ein Top-Down-Ansatz (prozessorientierte Sicht), ein Bottom-Up-Ansatz (systemorientierte Sicht) oder eine Mischung aus beiden verwendet werden. Bei Top-Down wird ermittelt, wo die kritischen Informationen verarbeitet, gespeichert und übertragen werden. Bei Bottom-Up hingegen werden die einzelnen Elemente der IT-Infrastruktur (insbesondere IT-Systeme, mobile Datenträger und Verbindungen) untersucht, ob sie kritische Informationen verarbeiten, speichern oder übertragen. Eine Mischung aus beiden Ansätzen bietet die Möglichkeit, die entsprechenden IT-Ressourcen zuverlässig zu identifizieren.*	kritisch → besonders sensibel, leicht gekürzt	*Um besonders sensible IT-Ressourcen zu ermitteln KANN ein Top-Down-Ansatz (prozessorientierte Sicht), ein Bottom-Up-Ansatz (systemorientierte Sicht) oder eine Mischung aus beiden verwendet werden. Bei Top-Down wird ermittelt, wo die besonders sensiblen Informationen verarbeitet, gespeichert und übertragen werden. Bei Bottom-Up hingegen werden die einzelnen Elemente der IT-Infrastruktur untersucht, ob sie besonders sensible Informationen verarbeiten, speichern oder übertragen. Eine Mischung aus beiden Ansätzen bietet die Möglichkeit, die entsprechenden IT-Ressourcen zuverlässig zu identifizieren.*
E2	*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.*	kritisch → besonders sensibel	*Um IT-Ressourcen zu ermitteln, die für den Betrieb von besonders sensiblen IT-Ressourcen zwingend benötigt werden, KANN ebenfalls ein Top-Down-Ansatz, ein Bottom-Up-Ansatz oder eine Mischung aus beiden Ansätzen verwendet werden.*

G3	Die Dokumentation MUSS folgende Anforderungen erfüllen:	übernehmen	Die Dokumentation MUSS folgende Anforderungen erfüllen:
G3.1	1. Sie enthält eine kurze Beschreibung der kritischen IT-Ressource.	kritisch → besonders sensibel	1. Sie enthält eine kurze Beschreibung der besonders sensiblen IT-Ressource.
G3.2	2. Sie begründet, warum die IT-Ressource kritisch ist.	kritisch → besonders sensibel	2. Sie begründet, warum die IT-Ressource besonders sensible ist.
G3.3	3. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) der IT-Ressource.	übernehmen	3. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) der IT-Ressource.
G4	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.	übernehmen	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.
E3	*Bei der Bestimmung der MTA SOLLTEN Abhängigkeiten zwischen kritischen IT-Ressourcen berücksichtigt werden.*	kritisch → besonders sensibel	*Bei der Bestimmung der MTA SOLLTEN Abhängigkeiten zwischen besonders sensiblen IT-Ressourcen berücksichtigt werden.*
G5	Die Aufstellung der kritischen IT-Ressourcen und deren Dokumentation MUSS vom IT-Verantwortlichen freigegeben werden.	kritisch → besonders sensibel	Die Aufstellung der besonders sensiblen IT-Ressourcen und deren Dokumentation MUSS vom IT-Verantwortlichen freigegeben werden.

10 IT-Systeme

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Die Informationsverarbeitung einer Organisation geschieht zum größten Teil elektronisch. Es ist deshalb notwendig, IT-Systeme strukturiert zu verwalten und abzusichern.	übernehmen	Die Informationsverarbeitung einer Organisation geschieht zum größten Teil elektronisch. Es ist deshalb notwendig, IT-Systeme strukturiert zu verwalten und abzusichern.

10.1 Inventarisierung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MUSS eine Inventarisierung vorhanden sein, in der alle IT-Systeme der Organisation verzeichnet sind.		
G2	Die Inventarisierung MUSS durch entsprechende		

	Verfahren (siehe Abschnitte 10.2.1 und 10.2.2) vollständig und aktuell gehalten werden.		
G3	In ihr MÜSSEN folgende Informationen für jedes IT-System verzeichnet sein:		
G3.1	1. eindeutiges Identifizierungsmerkmal		
G3.2	2. Informationen, die eine schnelle Lokalisierung erlauben		
G3.3	3. Einsatzzweck		
E1	*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.*		
E2	*Besonderheiten der Installation und Konfiguration SOLLTEN in einer Dokumentation verzeichnet sein.*		

10.2 Lebenszyklus

ToDo:
Muss angepasst werden. NIS2 fordert z. B. bereits Maßnahmen bei der Auswahl von IT-Systemen.

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	IT-Systeme bilden eine abgeschlossene Funktionseinheit aus Hard- und Software (siehe Abschnitt 10.3). Sie unterliegen einem Lebenszyklus, der sich üblicherweise von der Inbetriebnahme bis zu deren Ausmusterung erstreckt.		

10.2.1 Inbetriebnahme und Änderung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100

G1	Es MUSS ein Verfahren (siehe Anhang A 1) für die Inbetriebnahme und Änderung der IT-Systeme implementiert werden, das folgende Punkte sicherstellt:		
G1.1	1. Es wird ermittelt, ob das IT-System kritisch ist (siehe Abschnitt 9.3).		
G1.2	2. Der Basisschutz (siehe Abschnitt 10.3) wird umgesetzt.		
G1.3	3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und der Netzwerkplan (siehe Abschnitt 11.1) werden aktualisiert.		
G1.4	4. Bei Inbetriebnahme werden die Arbeitsschritte dokumentiert.		

10.2.2 Ausmusterung und Wiederverwendung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MUSS ein Verfahren (siehe Anhang A 1) für das Ausmustern und Wiederverwenden der IT-Systeme implementiert werden, das folgende Punkte sicherstellt:		
G1.1	1. Die auf dem IT-System gespeicherten Informationen werden bei Bedarf gesichert bzw. archiviert.		
G1.2	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.		
G1.3	3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und der Netzwerkplan (siehe Abschnitt 11.1) werden aktualisiert.		
G1.4	4. Bei Ausmusterung werden die Arbeitsschritte dokumentiert.		

10.3 Basisschutz

Verpflichtende Maßnahmen gem. BSIG können nicht mit dem Konzept des Basisschutzes umgesetzt werden, da es immer den Vorbehalt der entsprechenden Funktionalität und der eigenverantwortlichen Auslegung des Umsetzungsgrades gibt. Das passt PERFEKT, weil NIS2 den gleichen risikobasierten Ansatz wie die VdS 10k hat. :-)

→ § 30 ist aktuell noch ein ziemlich verbesserungswürdiges Gebilde. Hier müssen wir auf deng nächsten Referentenentwurf warten.
→ Wir können IT-Systeme von den Maßnahmen ausschließen, wenn sie die Kriterien der Risikoakzeptanz (siehe Abschnitt A 2.1) erfüllen.

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für alle IT-Systeme implementiert werden.	„ sofern eine entsprechende Funktionalität gegeben ist“ gestrichen. NIS2 passt sich nicht der vorhandenen IT-Infrastruktur an.	Die Maßnahmen der folgenden Abschnitte MÜSSEN für alle IT-Systeme implementiert werden.
		- 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 (…) - Auch in die VdS 10k aufnehmen? :-)	*IT-Systeme KÖNNEN von der Umsetzung der Maßnahmen des Basisschutzes generell ausgenommen werden, ~~wenn sie die Kriterien der Risikoakzeptanz (siehe Abschnitt A 2.1) erfüllen.~~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.*
E1	*Wenn eine entsprechende Funktionalität nicht gegeben ist, SOLLTE dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.*	Können wir so in NIS2 nicht übernehmen. Streichen.	
B2	Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.	übernehmen	Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

10.3.1 Software

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	System- und Anwendungssoftware MUSS aus vertrauenswürdigen Quellen bezogen werden.		
E1	*Es SOLLTE ausschließlich System- und Anwendungssoftware eingesetzt werden, die Sicherheitsupdates des Herstellers erhält.*		
E2	*Es SOLLTE nur Software auf IT-Systemen installiert werden, die zur Aufgabenerfüllung benötigt wird; nicht benötigte Software SOLLTE deinstalliert werden.*		
E3	*Sämtliche Zugriffsrechte und Privilegien der Anwendungssoftware SOLLTEN auf ein Mindestmaß reduziert werden.*		
B2	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Der Netzwerkverkehr von und zu IT-Systemen MUSS auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden, wenn eines der folgenden Kriterien zutrifft:		
B1.1	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).		
B1.2	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).		
E1	*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.*		
E2	*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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Jedes IT-System MUSS erfolgreiche und erfolglose Anmeldeversuche, Fehler und Informationssicherheitsereignisse protokollieren.		
E1	*Protokolldaten SOLLTEN zentral gespeichert werden.*		
B2	Protokolldaten MÜSSEN 6 Monate lang aufbewahrt werden, sofern keine gesetzlichen Lösch- oder Aufbewahrungspflichten entgegenstehen.		
B3	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
E1	*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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Alle IT-Systeme MÜSSEN über einen Schutz vor Schadsoftware verfügen.		
B2	Jedes IT-System MUSS mit Hilfe geeigneter Software täglich vollständig auf Anwesenheit von Schadsoftware untersucht werden.		
E1	*Darüber hinaus SOLLTEN alle IT-Systeme über einen Echtzeitschutz verfügen, der alle Dateien bei Zugriff auf Schadsoftware prüft.*		
E2	*Bei IT-Systemen mit einem Echtzeitschutz KANN die vollständige Untersuchung auf Schadsoftware auf einen wöchentlichen Rhythmus reduziert werden.*		
B3	Das Ausführen erkannter Schadsoftware MUSS verhindert werden.		
B4	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Es MUSS sichergestellt werden, dass IT-Systeme nur von autorisierten Medien gestartet werden können.		
E1	*Dies KANN z. B. über BIOS-Passwörter oder über einen Zutrittsschutz umgesetzt werden.*		

10.3.7 Authentifizierung

Frage: Sollten wir die Formulierung der VdS 10100 vielleicht in die VdS 10k übernehmen?
Folge wäre für die Organisationen, die die VdS 10k umsetzen: Kein MFA? → Risikoanalyse durchführen!

Würde passen!

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Der Zugang zu allen nichtöffentlichen Bereichen der IT-Systeme MUSS durch geeignete Anmeldeverfahren abgesichert werden, die eine Authentifizierung verlangen.	übernehmen	Der Zugang zu allen nichtöffentlichen Bereichen der IT-Systeme MUSS durch geeignete Anmeldeverfahren abgesichert werden, die eine Authentifizierung verlangen.
B2	Die Anmeldeverfahren MÜSSEN folgende Punkte sicherstellen:	übernehmen	Die Anmeldeverfahren MÜSSEN folgende Punkte sicherstellen:
B2.1	1. Das systematische Ausprobieren von Anmeldeinformationen wird erschwert.	übernehmen	1. Das systematische Ausprobieren von Anmeldeinformationen wird erschwert.
B2.2	2. Interaktive Sitzungen werden beendet oder gesperrt, wenn der Nutzer innerhalb einer vorgegebenen Zeitspanne keine Eingaben tätigt.	übernehmen	2. Interaktive Sitzungen werden beendet oder gesperrt, wenn der Nutzer innerhalb einer vorgegebenen Zeitspanne keine Eingaben tätigt.
B2.3	3. Erfolgt die Anmeldung über ein Netzwerk, so wird die Vertraulichkeit und Integrität der Anmeldeinformationen (z. B. mit Hilfe entsprechender Authentifizierungsprotokolle) sichergestellt.	übernehmen	3. Erfolgt die Anmeldung über ein Netzwerk, so wird die Vertraulichkeit und Integrität der Anmeldeinformationen (z. B. mit Hilfe entsprechender Authentifizierungsprotokolle) sichergestellt.
B3	Damit die Anmeldeverfahren zuverlässig arbeiten können, MÜSSEN folgende Punkte sichergestellt werden:	übernehmen	Damit die Anmeldeverfahren zuverlässig arbeiten können, MÜSSEN folgende Punkte sichergestellt werden:
B3.1	1. Zugänge werden strukturiert verwaltet (siehe Kapitel 15).	übernehmen	1. Zugänge werden strukturiert verwaltet (siehe Kapitel 15).
B3.2	2. Es werden zuverlässige Authentifizierungsmechanismen verwendet.	§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen (2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. 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.

B3.3	3. Es werden keine trivialen Authentifizierungsmerkmale (z. B. Standard-Passwörter oder einfach zu erratende Passwörter) 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.
E1	*Es SOLLTE Mehr-Faktor-Authentifizierung eingesetzt werden, um die Gefahr eines unberechtigten Zugangs zu verringern, insbesondere wenn Nutzer umfangreiche Zugriffsrechte besitzen.*	nicht übernehmen, MFA ist nichjt nur eine Empfehlung.	

10.3.8 Zugänge und Zugriffe

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Es MUSS sichergestellt werden, dass Nutzer keine administrativen Arbeiten durchführen können.		
E1	*Dies KANN mit Hilfe getrennter Zugänge und geeigneter Zugriffsrechte umgesetzt werden.*		
E2	*Darüber hinaus SOLLTEN folgende Anforderungen erfüllt werden:*		
E2.1	*1. Nutzer können nur auf Informationen lesend zugreifen, wenn dies für die Erfüllung ihrer Aufgaben notwendig ist („Need-to-Know“).*		
E2.2	*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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Mobile IT-Systeme sind in besonderer Weise Gefährdungen durch Diebstahl, unautorisierten Zutritt oder unsichere Netze ausgesetzt, die zusätzliche Maßnahmen erforderlich machen.		
G1	Folgende Maßnahmen MÜSSEN für alle mobilen IT-Systeme umgesetzt werden.		

10.4.1 IS-Richtlinie

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit mobilen IT-Systemen getroffen werden:		
G1.1	1. Es wird festgelegt, welche Informationen auf den mobilen IT-Systemen erhoben, verarbeitet, gespeichert und übertragen werden dürfen.		
G1.2	2. Die Verantwortung für die Datensicherung wird definiert.		
G1.3	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.		
G1.4	4. Es wird untersagt, mobile IT-Systeme an unberechtigte Dritte weiterzugeben.		
G1.5	5. Es wird definiert, ob und welche Software auf den mobilen IT-Systemen von den Nutzern installiert werden darf.		
G1.6	6. Es wird definiert, ob und unter welchen Bedingungen ein Administrator das mobile IT-System orten darf.		
G1.7	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die auf dem mobilen IT-System gespeicherten Informationen der Organisation MÜSSEN vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.		

E1	*Der Schutz der Vertraulichkeit KANN z. B. durch eine Verschlüsselung der Datenträger erreicht werden.*		

10.4.3 Verlust

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MÜSSEN Verfahren (siehe Anhang A 1) implementiert werden, die festlegen, wie Nutzer und Administratoren bei Verlust eines mobilen IT-Systems vorzugehen haben.		
G2	Die Verfahren MÜSSEN insbesondere festlegen, wie und an wen der Verlust zu melden ist und welche Sofortreaktion erfolgt.		
G3	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).		
G4	Der Verlust eines mobilen IT-Systems MUSS als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.		

10.x Zusätzliche Maßnahmen für wichtige IT-Systeme

Hier Maßnahmen für wichtige IT-Systeme einfügen:
- Maßnahme: Risikoanalyse durchführen.

10.5 Zusätzliche Maßnahmen für *besonders sensible* IT-Systeme

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Folgende Maßnahmen MÜSSEN zusätzlich für alle kritischen IT-Systeme umgesetzt werden.	kritisch → besonders sensibel	Folgende Maßnahmen MÜSSEN zusätzlich für alle *besonders sensiblen* IT-Systeme umgesetzt

			werden.
Z2	Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.	übernehmen	Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

10.5.1 Risikoanalyse und -behandlung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Für kritische IT-Systeme MUSS eine Risikoanalyse und –behandlung etabliert werden (siehe Anhang A 2).	kritisch → besonders sensibel	Für *besonders sensible* IT-Systeme MUSS eine Risikoanalyse und –behandlung etabliert werden (siehe Anhang A 2).

10.5.2 Notbetriebsniveau

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
E1	*Für jedes kritische IT-System SOLLTE ein Notbetriebsniveau definiert werden.*	kritisch → besonders sensibel	*Für jedes besonders sensible IT-System SOLLTE ein Notbetriebsniveau definiert werden.*

10.5.3 Robustheit

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Auf kritischen IT-Systemen DÜRFEN KEINE Entwicklungen oder Tests durchgeführt werden.	kritisch → besonders sensibel	Auf *besonders sensibl*en IT-Systemen DÜRFEN KEINE Entwicklungen oder Tests durchgeführt werden.
Z2	Auf kritischen IT-Systemen MÜSSEN alle Netzwerkdienste, die nicht zur Aufgabenerfüllung benötigt werden, deinstalliert, abgeschaltet oder durch geeignete Filtermechanismen unzugänglich gemacht werden.	kritisch → besonders sensibel	Auf *besonders sensiblen* IT-Systemen MÜSSEN alle Netzwerkdienste, die nicht zur Aufgabenerfüllung benötigt werden, deinstalliert, abgeschaltet oder durch geeignete Filtermechanismen unzugänglich gemacht werden.

10.5.4 Externe Schnittstellen und Laufwerke

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Externe Schnittstellen und Laufwerke, die nicht für	übernehmen	Externe Schnittstellen und Laufwerke, die nicht für

	die Aufgabenerfüllung benötigt werden, MÜSSEN ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht werden.		die Aufgabenerfüllung benötigt werden, MÜSSEN ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht werden.

10.5.5 Änderungsmanagement

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Änderungen, die auf kritischen IT-Systemen umgesetzt werden sollen, MÜSSEN zuvor in einer Testumgebung getestet und freigegeben worden sein.	kritisch → besonders sensibel	Änderungen, die auf besonders sensiblen IT-Systemen umgesetzt werden sollen, MÜSSEN zuvor in einer Testumgebung getestet und freigegeben worden sein.
Z2	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 10.5.9).	kritisch → besonders sensibel	Für besonders sensiblen 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 10.5.9).

10.5.6 Dokumentation

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Für jedes kritische IT-System MUSS eine Dokumentation vorhanden sein.	kritisch → besonders sensibel	Für jedes besonders sensible IT-System MUSS eine Dokumentation vorhanden sein.
Z2	Anhand der Dokumentation MUSS es fachlich versierten Personen möglich sein, folgende Punkte nachzuvollziehen:	übernehmen	Anhand der Dokumentation MUSS es fachlich versierten Personen möglich sein, folgende Punkte nachzuvollziehen:
Z2.1	1. wer für das IT-System verantwortlich ist	übernehmen	1. wer für das IT-System verantwortlich ist
Z2.2	2. wie und mit welchen Zugängen und Authentifizierungsmerkmalen der administrative Zugang zum IT-System möglich ist	übernehmen	2. wie und mit welchen Zugängen und Authentifizierungsmerkmalen der administrative Zugang zum IT-System möglich ist
Z2.3	3. welche grundlegenden Designentscheidungen bei der Installation getroffen wurden	übernehmen	3. welche grundlegenden Designentscheidungen bei der Installation getroffen wurden
Z2.4	4. welche Änderungen vorgenommen wurden	übernehmen	4. welche Änderungen vorgenommen wurden
Z2.5	5. wann sie vorgenommen wurden	übernehmen	5. wann sie vorgenommen wurden

Z2.6	6. wer sie vorgenommen hat	übernehmen	6. wer sie vorgenommen hat
Z2.7	7. warum sie vorgenommen wurden	übernehmen	7. warum sie vorgenommen wurden

10.5.7 Datensicherung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Alle kritischen IT-Systeme MÜSSEN über eine Datensicherung (siehe Abschnitt 16.6) verfügen.	kritisch → besonders sensibel	Alle kritischen IT-Systeme MÜSSEN über eine Datensicherung (siehe Abschnitt 16.6) verfügen.

10.5.8 Überwachung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Es MUSS überwacht werden, ob sich kritische IT-Systeme im Regelbetrieb befinden.	kritisch → besonders sensibel	Es MUSS überwacht werden, ob sich besonders sensible IT-Systeme im Regelbetrieb befinden.
Z2	Dabei MUSS sichergestellt werden, dass der Ausfall eines kritischen IT-Systems erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.	kritisch → besonders sensibel	Dabei MUSS sichergestellt werden, dass der Ausfall eines besonders sensiblen IT-Systems erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.
E1	*Darüber hinaus SOLLTEN die Ressourcen kritischer IT-Systeme überwacht werden, um Engpässe zu erkennen, bevor sie akut werden.*	kritisch → besonders sensibel	*Darüber hinaus SOLLTEN die Ressourcen besonders sensibler IT-Systeme überwacht werden, um Engpässe zu erkennen, bevor sie akut werden.*

10.5.9 Ersatzsysteme und -verfahren

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	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.	kritisch → besonders sensibel, leicht gekürzt	Wenn ein besonders sensibles IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, MUSS die Organisation über ein Ersatzsystem oder –verfahren verfügen, das es ermöglicht, die von ihm abhängigen zentralen Prozesse und Prozesse mit hohem Schadenspotential weiter zu betreiben.
E1	*Das Ersatzsystem oder –verfahren SOLLTE das Notbetriebsniveau (siehe Abschnitt 10.5.2) des kritischen IT-Systems sicherstellen.*	kritisch → besonders sensibel	*Das Ersatzsystem oder –verfahren SOLLTE das Notbetriebsniveau (siehe Abschnitt 10.5.2) des besonders sensiblen IT-Systems sicherstellen.*

10.5.10 Kritische Individualsoftware

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Die Organisation MUSS durch vertragliche und/oder organisatorische Regelungen sicherstellen, dass sie kritische Individualsoftware auch in Zukunft verwenden und ihren Bedürfnissen anpassen kann.	kritisch → besonders sensibel	Die Organisation MUSS durch vertragliche und/oder organisatorische Regelungen sicherstellen, dass sie kritische Individualsoftware auch in Zukunft verwenden und ihren Bedürfnissen anpassen kann.

11 Netzwerke und Verbindungen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Netzwerke und Verbindungen übertragen Informationen und vernetzen IT-Systeme miteinander. Deshalb ist es notwendig, sie angemessen abzusichern.		

11.1 Netzwerkplan

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Netzwerke der Organisation MÜSSEN so erfasst sein, dass fachlich versierte Personen folgende Punkte nachvollziehen können:		
G1.1	1. physikalische Netzwerkstruktur		
G1.1.a	a. aktive Netzwerkkomponenten und deren Verbindungen untereinander		
G1.1.b	b. physikalisches Medium der Verbindungen		
G1.2	2. logische Netzwerkstruktur		
G1.2.a	a. Netzwerksegmente (siehe Abschnitt 11.4.2), deren Einsatzzweck und deren Verbindungen untereinander		
G1.2.b	b. Fernzugänge (siehe Abschnitt 11.4.3)		
G1.2.c	c. Netzwerkkopplungen (siehe Abschnitt 11.4.4)		
G1.2.d	d. Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken (siehe Abschnitt		

	11.3)		

11.2 Aktive Netzwerkkomponenten

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Aktive Netzwerkkomponenten sind IT-Systeme und MÜSSEN gemäß Kapitel 10 behandelt werden.		

11.3 Netzübergänge

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Folgende Maßnahmen MÜSSEN für alle Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken umgesetzt werden:		
B1.1	1. Der Netzwerkverkehr wird auf das für die Funktionsfähigkeit notwendige Minimum beschränkt.		
B1.2	2. Der Inhalt erlaubter Verbindungen wird auf Schadsoftware und Angriffe untersucht; erkannte Schadsoftware und Angriffe werden blockiert.		
B1.3	3. Hinweise auf Schadsoftware in der IT-Infrastruktur der Organisation und Angriffe aus der IT-Infrastruktur der Organisation heraus werden als Sicherheitsvorfall behandelt.		
B2	Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.		
E1	*Weitere Sicherheitsmaßnahmen SOLLTEN im Zuge einer Risikoanalyse und -behandlung (siehe Anhang A 2) ermittelt und umgesetzt werden.*		
G1	Die Konfiguration der Netzwerkkomponenten, die einen Netzwerkübergang zu weniger oder nicht vertrauenswürdigen Netzwerken implementieren, MUSS jährlich überprüft werden und folgende		

	Anforderungen erfüllen:		
G1.1	1. Für die sicherheitsrelevanten Einstellungen sind folgende Punkte dokumentiert:		
G1.1.a	a. wer sie implementiert hat		
G1.1.b	b. wann sie implementiert wurden		
G1.1.c	c. was sie bewirken		
G1.1.d	d. warum sie benötigt werden		
G1.2	2. Die angestrebten Verkehrsbeschränkungen werden wirksam umgesetzt.		

11.4 Basisschutz

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für alle Netzwerke implementiert werden.	„ sofern eine entsprechende Funktionalität gegeben ist“ gestrichen. NIS2 passt sich nicht der vorhandenen IT-Infrastruktur an.	Die Maßnahmen der folgenden Abschnitte MÜSSEN für alle Netzwerke implementiert werden.
		- 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 (…) - Auch in die VdS 10k aufnehmen? :-)	*Netzwerke KÖNNEN von der Umsetzung der Maßnahmen des Basisschutzes generell ausgenommen werden, ~~wenn sie die Kriterien der Risikoakzeptanz (siehe Abschnitt A 2.1) erfüllen.~~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*
E1	*Wenn eine entsprechende Funktionalität nicht gegeben ist, SOLLTE dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.*	Können wir so in NIS2 nicht übernehmen. Streichen.	
B2	Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung	übernehmen	Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang

	(siehe Anhang A 2) begegnet werden.		A 2) begegnet werden.

11.4.1 Netzwerkanschlüsse

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Dauerhaft nicht genutzte Netzwerkanschlüsse MÜSSEN vor unberechtigter Nutzung gesichert werden.		
E1	*Dies KANN bspw. durch eine Zutrittsbeschränkung, eine Deaktivierung der Netzwerkanschlüsse oder durch eine Netzwerkzugangskontrolle geschehen.*		

11.4.2 Segmentierung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Die Notwendigkeit einer Segmentierung der Netzwerke der Organisation MUSS geprüft und die Entscheidung dokumentiert werden.		
B2	Die Umsetzung der Segmentierung MUSS eine möglichst umfassende Beschränkung der Verbindungen sowie die Möglichkeit der Protokollierung von blockierten Verbindungen beinhalten.		

11.4.3 Fernzugang

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Der Zugang zu nichtöffentlichen Bereichen von IT-Systemen der Organisation über weniger oder nicht vertrauenswürdige Netzwerke MUSS abgesichert werden.		
B2	Dabei MÜSSEN folgende Anforderungen erfüllt werden:		
B2.1	1. Die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen wird geschützt.		

B2.2	2. Der Zugang wird so gestaltet, dass über ihn nur IT-Systeme erreichbar sind, die der jeweilige Nutzer für seine Aufgabenerfüllung benötigt.		
E1	*Darüber hinaus SOLLTEN folgende Anforderungen erfüllt werden:*		
E1.1	*1. 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.*		
E1.2	*2. Der Nutzer wird, vor allem wenn er umfangreiche Zugriffsrechte besitzt, mit Hilfe einer Mehr-Faktor-Authentifizierung authentifiziert, um die Gefahr eines unberechtigten Zugangs zu verringern.*		

11.4.4 Netzwerkkopplung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Die Kopplung von Netzwerken der Organisation über weniger oder nicht vertrauenswürdige Netzwerke hinweg MUSS abgesichert werden.		
B2	Dabei MÜSSEN die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen gewährleistet werden.		

11.5 Zusätzliche Maßnahmen für kritische Verbindungen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Für alle kritischen Verbindungen, MUSS eine Risikoanalyse und –behandlung (siehe Anhang A 2) etabliert werden.		

12 Mobile Datenträger

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Mobile Datenträger sind aufgrund ihrer exponierten Nutzungsart besonders gefährdet. Deshalb ist es notwendig, die damit verbundenen Risiken angemessen zu behandeln.		

12.1 IS-Richtlinie

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit mobilen Datenträgern getroffen werden:		
G1.1	1. Es wird festgelegt, welche Informationen der Organisation auf mobilen Datenträgern gespeichert werden dürfen.		
G1.2	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.		
G1.3	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
E1	*Die auf den mobilen Datenträgern gespeicherten Informationen der Organisation SOLLTEN vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.*		

E2	*Der Schutz der Vertraulichkeit KANN z. B. durch eine Verschlüsselung der Datenträger erreicht werden.*		

12.3 Zusätzliche Maßnahmen für kritische mobile Datenträger

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Für alle kritischen mobilen Datenträger MUSS eine Risikoanalyse und –behandlung (siehe Anhang A 2) etabliert werden.		

13 Umgebung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Organisation MUSS ihre IT-Systeme und Datenleitungen gegen negative Umwelteinflüsse absichern.		
E1	*Dies SOLLTE auf Basis eines anerkannten Standards wie z. B. VdS 2007 erfolgen.*		
G2	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen (z. B. Patchfelder) MÜSSEN vor Beschädigung und unberechtigtem Zutritt geschützt werden.		
E1	*Dies KANN z. B. durch bauliche Maßnahmen (Serverraum) oder durch abschließbare Schränke (Server- oder Netzwerkschränke) umgesetzt werden.*		
E2	*Insbesondere SOLLTEN folgende Bedrohungen*		

	bewertet und behandelt werden:		
E2.1	*1. ungeeignete Umgebungsbedingungen (wie z. B. ungeeignete Temperatur oder Luftfeuchtigkeit, Staub oder Rauch)*		
E2.2	*2. negative Umwelteinflüsse (wie z. B. Feuer, Wasser, Blitzschlag)*		
E2.3	*3. unzuverlässige Stromversorgung (wie z. B. Unter- oder Überspannung, Spannungsspitzen, Unterbrechung)*		
E2.3.a	*Fest installierte Niederspannungsanlagen SOLLTEN gemäß gängiger Normen und Standards wie z. B. der DIN VDE 0100-Reihe errichtet sein.*		
E2.4	*4. Beschädigung und Verlust (wie z. B. Löschmittel, Vandalismus, Diebstahl)*		

13.2 Datenleitungen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
E1	*Sämtliche Datenleitungen SOLLTEN gemäß gängiger Normen und Standards wie z. B. DIN EN 50173/4-Reihe installiert werden.*		
G1	Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN fest installierte Datenleitungen durch entsprechende bauliche Maßnahmen vor Beschädigung geschützt werden.		
E2	*Dies KANN z. B. durch das Verlegen der Datenleitungen in Kabelkanälen umgesetzt werden.*		

13.3 Zusätzliche Maßnahmen für kritische IT-Systeme

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Im Zuge der Risikoanalyse und -behandlung (siehe Abschnitt 10.5.1) MÜSSEN für alle kritischen IT-Systeme folgende Bedrohungen behandelt werden:		
Z1.1	1. ungeeignete Umgebungsbedingungen (wie z. B. ungeeignete Temperatur oder Luftfeuchtigkeit,		

	Staub oder Rauch)		
Z1.2	2. negative Umwelteinflüsse (wie z. B. Feuer, Wasser, Blitzschlag)		
Z1.3	3. unzuverlässige Stromversorgung (wie z. B. Unter- oder Überspannung, Spannungsspitzen, Unterbrechung)		
Z1.4	4. Beschädigung und Verlust (wie z. B. Löschmittel, Vandalismus, Diebstahl)		
Z1.5	5. unautorisierter Zutritt		
Z1.6	6. Ausspähen vertraulicher Informationen		
E1	*Insbesondere SOLLTE geprüft werden, kritische IT-Systeme in zusätzlich abgesicherten Gebäuden oder Gebäudeteilen unterzubringen (Sicherheitszonen).*		

14 IT-Outsourcing und Cloud Computing

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Wenn IT-Ressourcen ausgelagert werden, ist es notwendig, dass die Sicherheitsinteressen der Organisation berücksichtigt werden.		

14.1 IS-Richtlinie

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Für Jedes Vorhaben, das zur Auslagerung von IT-Ressourcen führt, MÜSSEN folgende Punkte dokumentiert werden:		

G1.1	1. welche IT-Ressourcen ausgelagert werden sollen		
G1.2	2. welche betrieblichen, gesetzlichen und vertraglichen Bestimmungen, insbesondere in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität der ausgelagerten IT-Ressourcen, erfüllt werden müssen		
G1.3	3. ob die auszulagernden IT-Ressourcen kritisch sind		
G2	Wenn IT-Ressourcen ausgelagert werden, MUSS die Organisation darauf vorbereitet werden:		
G2.1	1. Kompetenzen für die Steuerung der auszulagernden IT-Ressourcen werden aufgebaut.		
G2.2	2. Die IT-Infrastruktur wird auf das Zusammenspiel mit den auszulagernden IT-Ressourcen vorbereitet.		

14.3 Vertragsgestaltung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	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.		
E1	*Darüber hinaus SOLLTEN folgende Punkte sichergestellt sein:*		
E1.1	*1. Ansprüche aus Vertragsverletzungen können durchgesetzt werden, auch wenn sich der Anbieter nicht im gleichen Rechtsraum wie die Organisation befindet.*		
E1.2	*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 kritische IT-Ressourcen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Wenn kritische 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:		
Z1.1	1. Leistungen		
Z1.1.a	a. Die vom Anbieter zu erbringenden Leistungen werden definiert und deren Messung und Überwachung werden vereinbart.		
Z1.1.b	b. Die Standorte, an denen Leistungen erbracht werden, werden festgelegt.		
Z1.1.c	c. Die Sicherheitsmaßnahmen, die der Anbieter zum Schutz der ausgelagerten IT-Ressourcen treffen muss, werden vereinbart.		
Z1.1.d	d. Eine Beschreibung der Schnittstellen zwischen der IT-Infrastruktur der Organisation und den ausgelagerten IT-Ressourcen wird definiert.		
E1.1	*Es SOLLTEN Konsequenzen bei Nichteinhaltung der vertraglich vereinbarten Leistungen vereinbart werden.*		
Z1.2	2. Kommunikation		
Z1.2.a	a. Die Ansprechpartner auf Seiten der Organisation und des Anbieters werden benannt.		
Z1.2.b	b. Eine Vertraulichkeitsvereinbarung wird getroffen.		
Z1.2.c	c. Es wird vereinbart, ob und unter welchen Bedingungen der Anbieter dazu berechtigt ist, Daten an Dritte weiterzugeben.		
Z1.2.d	d. Eine Informationspflicht des Anbieters bei Sicherheitsvorfällen, die die ausgelagerten IT-Ressourcen betreffen, wird vereinbart.		
Z1.3	3. Leistungsänderungen und Vertragsauflösung		

Z1.3.a	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.		
Z1.3.b	b. Eine schriftliche Dokumentation und Meldung bei Änderungen an einem der oben genannten Punkte wird vereinbart.		
Z2	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	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:		
G1.1	1. Die jeweiligen Vorgänge werden vor ihrer Umsetzung beantragt, geprüft und genehmigt.		
G1.2	2. Zugänge und Zugriffsrechte werden nur genehmigt, wenn sie für die Aufgabenerfüllung des jeweiligen Nutzers oder für die betrieblichen Abläufe der Organisation notwendig sind.		

G1.3	3. Wenn ein Nutzer administrative Zugänge oder Zugriffsrechte erhalten soll, wird dies besonders begründet und vom IT-Verantwortlichen entschieden.		
G1.4	4. Antragssteller und Nutzer werden zeitnah über die erfolgte Durchführung informiert.		
E1.4	*Wenn Zugänge oder Zugriffsrechte entzogen werden, KANN auf das Informieren des Nutzers verzichtet werden.*		
G1.5	5. Vor dem Löschen eines Zugangs werden die Daten, die mit ihm verknüpft sind, weitergegeben, gelöscht oder gesichert bzw. archiviert.		
G1.6	6. Die jeweiligen Vorgänge werden dokumentiert.		

15.2 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	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.		
Z2	Nicht ordnungsgemäß angelegte Zugänge und Zugriffsrechte MÜSSEN als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.		

16 Datensicherung und Archivierung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	Daten können unbrauchbar werden oder verloren gehen. Deshalb ist es notwendig, durch eine Datensicherung die Integrität und Verfügbarkeit der Daten sicherzustellen.		
E1	*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.		
G1	Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN die Anforderungen folgender Abschnitte erfüllt werden.		

16.1 IS-Richtlinie

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie die Speicherorte für die Daten der Organisation festgelegt werden.		

16.2 Archivierung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Organisation MUSS prüfen, welche Daten archiviert werden müssen, um betrieblichen, gesetzlichen und vertraglichen Anforderungen zu genügen.		

16.3 Verfahren

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Für die Datensicherung, -wiederherstellung und -archivierung MÜSSEN Verfahren (siehe Anhang A 1) implementiert werden, die die folgenden Punkte sicherstellen:		
G1.1	1. Die gesicherten Daten werden bei Übertragung, Lagerung und Transport vor Änderungen, Beschädigung, Verlust und unberechtigter Einsichtnahme geschützt.		
E1.1	*Der Schutz der Vertraulichkeit KANN z. B. durch eine Verschlüsselung der Daten oder der Sicherungsmedien erreicht werden.*		
G1.2	2. Die gesicherten Daten werden nicht im gleichen Brandabschnitt wie die gesicherten IT-Systeme aufbewahrt.		

E1.2	*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.*		
G1.3	3. 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.		
E1.3	*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.*		
G1.4	4. Die Durchführung und die Ergebnisse der Tests werden dokumentiert.		
E2	*Die Verfahren SOLLTEN darüber hinaus die folgenden Punkte sicherstellen:*		
E2.1	*1. Einzelne Datensicherungen werden in festen zeitlichen Abständen (z. B. wöchentlich) an einen entfernten Standort ausgelagert, damit die gesicherten Daten auch bei größeren Schadensereignissen verfügbar bleiben.*		
E2.2	*2. Die Datensicherung wird nach dem Mehr-Generationen-Prinzip durchgeführt, um die Wahrscheinlichkeit eines umfangreichen Datenverlusts weiter zu verringern.*		

16.4 Weiterentwicklung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	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.		
G2	Notwendige Anpassungen MÜSSEN zeitnah implementiert werden.		

16.5 Basisschutz

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für Speicherorte (siehe Abschnitt 16.1), Server, aktive Netzwerkkomponenten und mobile IT-Systeme implementiert werden.	„ sofern eine entsprechende Funktionalität gegeben ist“ gestrichen. NIS2 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.
	-	- 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 (…) - Auch in die VdS 10k aufnehmen? :-)	*Speicherorte, Server, aktive Netzwerkkomponenten und mobile IT-Systeme KÖNNEN von der Umsetzung der Maßnahmen des Basisschutzes generell ausgenommen werden, ~~wenn sie die Kriterien der Risikoakzeptanz (siehe Abschnitt A 2.1) erfüllen.~~wenn die Verletzung ihrer Vertraulichkeit, Verfügbarkeit und Authentizität nur zu einem vernachlässigbaren Schaden führen kann (Risikoakzeptanzgrenze, siehe Anhang A 2).*
E1	*Wenn eine entsprechende Funktionalität nicht gegeben ist, SOLLTE dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.*	Können wir so in NIS2 nicht übernehmen. Streichen.	
B2	Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.	übernehmen	Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

16.5.1 Speicherorte

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Speicherorte MÜSSEN so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand nicht älter als 24 Stunden ist.		

16.5.2 Server

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Server MÜSSEN so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand (Systemsoftware, Konfigurationen, Anwendungssoftware, Anwendungs-, Logdaten, usw.) nicht älter als 24 Stunden ist.		

16.5.3 Aktive Netzwerkkomponenten

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Systemsoftware und Konfiguration der aktiven Netzwerkkomponenten MÜSSEN nach jeder Änderung gesichert werden.		

16.5.4 Mobile IT-Systeme

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
B1	Es MUSS eine Vorgehensweise für die Datensicherung von einem Administrator vorgegeben werden.		

16.6 Zusätzliche Maßnahmen für kritische IT-Systeme

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Jedes kritische IT-System MUSS über eine Datensicherung verfügen, die in Ergänzung zu Abschnitts 16.5 folgende Anforderungen erfüllt.		

16.6.1 Risikoanalyse

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Die Verfahren zur Datensicherung und -wiederherstellung MÜSSEN in Ergänzung zu Abschnitt 16.3 folgende Punkte sicherstellen:		
Z1.1	1. Kritische IT-Systeme werden vollständig gesichert (Systemsoftware, Konfigurationen, Anwendungssoftware, Anwendungs-, Logdaten, usw.).		
Z1.2	2. Der MTD wird nicht überschritten.		
Z1.3	3. Die Wiederherstellung innerhalb der MTA wird gewährleistet, sofern keine Ersatzsysteme oder –verfahren verfügbar sind (siehe Abschnitt 10.5.9).		

17 Sicherheitsvorfälle

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

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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
T1	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.		

E1	*Zu diesem Zweck SOLLTE die Organisation ein Business Continuity Management (BCM) auf Basis eines anerkannten Standards wie BSI-Standard 100-4 oder DIN EN ISO 22301 implementieren.*		
G1	Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN die Anforderungen folgender Abschnitte erfüllt werden.		

17.1 IS-Richtlinie

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit Sicherheitsvorfällen getroffen werden:		
G1.1	1. Der Begriff „Sicherheitsvorfall“ wird klar definiert.	Definition „erheblicher Sicherheitsvorfall“ in Kap. 3 aufnehmen.	1. Die Begriffe „Sicherheitsvorfall“ und „erheblicher Sicherheitsvorfall“ werden klar definiert.
E1	*Hierbei SOLLTE aufgezählt werden, welche Auffälligkeiten zur Meldung eines möglichen Sicherheitsvorfalls führen müssen.*		
G1.2	2. Jeder Mitarbeiter meldet mögliche Sicherheitsvorfälle über die dafür vorgesehenen Meldewege.		
G1.3	3. Administratoren untersuchen, ggf. in Zusammenarbeit mit den jeweiligen Prozessverantwortlichen, dem IT-Verantwortlichen und dem ISB, Sicherheitsvorfälle vordringlich.		3. Die Verantwortlichen untersuchen, ggf. in Zusammenarbeit mit den jeweiligen Prozessverantwortlichen, den IT-Verantwortlichen und dem ISB, Sicherheitsvorfälle vordringlich.
G1.4	4. Es wird definiert, in welchen Fällen das Topmanagement über Sicherheitsvorfälle informiert wird.		
G1.5	5. Es wird definiert, wie die Organisation intern und nach außen über akute und bewältigte Sicherheitsvorfälle kommuniziert.		
			6. Es wird definiert, ab wann ein Sicherheitsvorfall als ein erheblicher Sicherheitsvorfall eingestuft wird.

17.2 Erkennen

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
E1	*Es SOLLTEN Maßnahmen implementiert werden, die es ermöglichen, Sicherheitsvorfälle zu erkennen, wie z. B.:*	MÜSSEN bei der VdS 10100?	
E1.1	*1. Intrusion Detection Systeme (IDS)*		
E1.2	*2. Integritätsprüfungen auf Prüfsummenbasis*		
E1.3	*3. Sensor-Systeme (Honeypots)*		
E1.4	*4. Überwachen der Zugriffe auf besonders sensible Dateien*		
E1.5	*5. Erfassen und Auswerten von Logmeldungen*		
E2	*Das Melden von Sicherheitsvorfällen SOLLTE durch eine positive Fehlerkultur und/oder anonyme Meldewege gefördert werden.*		

17.3 Reaktion

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das beim Auftreten eines Sicherheitsvorfalls folgende Reaktionen zeitnah sicherstellt:		
G1.1	1. Es wird ein Überblick über die Situation gewonnen.		
G1.2	2. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen.		
G1.3	3. Der Schaden wird durch Sofortmaßnahmen eingedämmt.		
G1.4	4. Der Schaden wird dokumentiert.		
G1.5	5. Beweismittel werden gesichert.		
G1.6	6. Der Schaden wird behoben und der Regelbetrieb wieder aufgenommen.		
G1.7	7. Es findet eine Nacbhbereitung 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.		
E1	*Bei geringfügigen Störungen oder Ausfällen KÖNNEN einzelne Punkte ausgelassen und/oder das Verfahren vorzeitig beendet werden.*		
	-	Ggf. in die VdS 10000 aufnehmen?! Organisationen sind z. B. auch ohne NIS2 verpflichtet, Informationen an Dritte (z. B. an Versicherungen, Datenschutz-Aufsichtsbehörden usw.) weiterzugeben,	Zusätzlich MUSS das Verfahren bei einem erheblichen Sicherheitsvorfall die folgenden Punkte sicherstellen:
	-	Grundlage für die Zusammenarbeit mit dem BSI legen.	1. Der Sicherheitsvorfall wird fortlaufend so dokumentiert, so dass die Organisation ihre Informationspflichten erfüllen kann.
	-	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?!	2. Einem Mitarbeiter mit entsprechender Fachkompetenz wird die Verantwortlichkeit zugeordnet, mit dem BSI zu kommunizieren.
	-		*Diese Verantwortlichkeit KANN z. B. der ISB wahrnehmen.*
	-	BSIG § 32 Abs. 1,2 und 3	3. 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.	4. Auf Anweisung des BSI werden die Empfänger der betroffenen Dienste unverzüglich über den Sicherheitsvorfall unterrichtet; hierzu werden entsprechende Inhalte, Empfängerlisten und Kommunikationswege vorbereitet, die auch bei einer Störung oder einem Ausfall der IT-Infrastruktur genutzt werden können.
	-	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	5. 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

		die Empfehlung aufgenommen werden, auch für die interne Kommunikation entsprechende Vorkehrungen zu treffen.	Schutzmaßnahmen mitgeteilt, hierzu werden entsprechende Inhalte vorbereitet, die im Bedarfsfall nur noch angepasst werden müssen.
	-	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 kritische IT-Systeme

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Folgende Maßnahmen MÜSSEN zusätzlich für alle kritischen IT-Systeme umgesetzt werden.		

17.4.1 Wiederanlaufpläne

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Für jedes kritische IT-System MUSS ein Verfahren (siehe Anhang A 1) für den Wiederanlauf implementiert werden (Wiederanlaufplan), das folgende Anforderungen erfüllt:		
Z1.1	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.		
Z1.2	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.		
Z1.3	3. Er enthält eine Aufstellung der für die Wiederherstellung zwingend benötigten Ressourcen, wie z. B. Mitarbeiter und deren Kontaktdaten, Hardware, Software, Netzwerke, Dienste und Authentifizierungsmerkmale.		
Z1.4	4. Er ist verständlich und übersichtlich strukturiert.		
Z1.5	5. Er ist im Bedarfsfall schnell verfügbar.		
Z1.6	6. Er wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.		

17.4.2 Abhängigkeiten

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
Z1	Es MÜSSEN die Abhängigkeiten der kritischen IT-Systeme untereinander dokumentiert werden.		
E1	*Darüber hinaus SOLLTEN die Abhängigkeiten der kritischen IT-Systeme von sämtlichen kritischen IT-Ressourcen dokumentiert und dabei die Notwendigkeit weiterer Wiederanlaufpläne geprüft werden.*		
Z2	Die Dokumentation MUSS folgende Anforderungen erfüllen:		
Z2.1	1. Aus ihr geht eindeutig hervor, in welcher Reihenfolge die kritischen IT-Systeme wiederhergestellt werden müssen.		
Z2.2	2. Sie ist verständlich und übersichtlich strukturiert.		
Z2.3	3. Sie ist im Bedarfsfall schnell verfügbar.		
Z2.4	4. Sie wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.		

Kapitel 18 der VdS 10000 entfällt in Zukunft.

Anhang A

A 1 Verfahren

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Organisation MUSS die in diesen Richtlinien geforderten Verfahren planen, steuern und stetig verbessern.		
E1	*Dies SOLLTE im Rahmen eines Qualitätsmanagements auf Basis eines anerkannten Standards wie z. B. DIN EN ISO 9001 geschehen.*		
G2	Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN folgende Anforderungen erfüllt werden:		
G2.1	1. Es wird definiert, wer für die Durchführung verantwortlich ist.		
G2.2	2. Verfahren werden in einer für die jeweilige Zielgruppe zugänglichen und verständlichen Form dokumentiert und bekannt gegeben.		
G2.3	3. Verfahren werden verbessert, wenn Mängel in ihrer Umsetzung, Angemessenheit oder Effektivität erkannt werden.		
G2.4	4. 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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Die Organisation MUSS die in diesen Richtlinien geforderten Risikoanalysen durchführen und erkannte Risiken zeitnah und angemessen	Achtung! Risikomanagement! Muss umformuliert werden,	

	behandeln.		
E1	*Dies SOLLTE im Rahmen eines Risikomanagements auf Basis eines anerkannten Standards wie BSI-Standard 200-3, ISO/IEC 27005 oder ISO 31000 erfolgen.*	übernehmen	*Dies SOLLTE im Rahmen eines Risikomanagements auf Basis eines anerkannten Standards wie BSI-Standard 200-3, ISO/IEC 27005 oder ISO 31000 erfolgen.*
G2	Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.	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

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
	-	neu	Die Vorgehensweisen für die Risikoidentifikation, -analyse und -behandlung MÜSSEN festgelegt sein.
	-	neu	Es MÜSSEN Kriterien für die Bewertung der Schadenshöhe und der Eintrittswahrscheinlichkeit festgelegt werden, anhand derer Risiken bewertet werden und anhand derer zuverlässig festgestellt werden kann, ob ein Risiko akzeptiert werden kann (Risikoakzeptanzgrenze).
	-	neu	Die Kriterien für die Bewertung der Schadenshöhe MÜSSEN konkrete Anforderungen an die Vertraulichkeit, Verfügbarkeit und Integrität des Gegenstands der Risikoanalyse beinhalten.
	-	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 Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen.“* *- ISO 31010 in Kap. 2 aufgenommen.*	*Die Auswahl der Vorgehensweisen SOLLTE auf Basis eines anerkannten Standards wie z. B. ISO 31010 erfolgen.*

A 2.2 Risikoanalyse

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Eine Risikoanalyse MUSS folgende Anforderungen erfüllen:	übernehmen	Eine Risikoanalyse MUSS folgende Anforderungen erfüllen:
G1.1	1. Ihre Dokumentation beinhaltet das Vorgehen für das Identifizieren und Bewerten von Risiken.	Alternativ: 1. Die Dokumentation beinhaltet das Vorgehen für das Identifizieren und Bewerten von Risiken sowie deren Ergebnisse.	1. Ihre Durchführung und ihre Ergebnisse werden dokumentiert.
G1.2	2. Die Vorgehensweise gewährleistet, dass Bedrohungen und Schwachstellen zuverlässig erkannt werden können.	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“ <u>ACHTUNG!</u> Als Grundlage der Risikoidentifikation benötigen wir konkrete Anforderungen an die Verfügbarkeit, Integrität und Vertraulichkeit von Prozessen (9.1), Informationen (9.2) und IT-Ressourcen (9.3). Dabei sollten die Anforderungen an Informationen und IT-Ressourcen von denen der Prozesse vereerbt werden. Noch unklar!	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.
	-	- Für die Umsetzung eines schlagkräftigen Risikomanagements ist es sicher hilfreich, das Rad nicht neu erfinden zu müssen. Es bestehen verschiedene Sammlungen von Bedrohungen bzw. Gefährdungen, die hinzugezogen werden können. - ENISA Thread Taxonomy, ISO 27005 und/oder die Aufstellung „Elementare Gefährdungen“ des BSI in Kapitel 2 aufnehmen.	*Dabei SOLLTEN entsprechende Kataloge wie z. B. ENISA Thread Taxonomy, der Annex der ISO 27005 oder die Aufstellung „Elementare Gefährdungen“ des BSI berücksichtigt werden.*
G1.3	3. Die Bewertung von Risiken erfolgt auf Basis der potentiellen Schäden und deren Eintrittswahrscheinlichkeit.	übernehmen	3. Die Bewertung von Risiken erfolgt auf Basis der potentiellen Schäden und deren Eintrittswahrscheinlichkeit.
G1.4	4. Das Ergebnis der Risikoanalyse ermöglicht eine Priorisierung bei der Risikobehandlung.	übernehmen	4. Das Ergebnis der Risikoanalyse ermöglicht eine Priorisierung bei der Risikobehandlung.

A 2.3 Risikobehandlung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100
G1	Identifizierte Risiken MÜSSEN angemessen, zeitnah und priorisiert behandelt werden, indem geeignete Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der Risiken (z. B. durch den Abschluss einer Versicherung) definiert, dokumentiert und umgesetzt oder indem Risiken akzeptiert werden.		Identifizierte Risiken MÜSSEN angemessen, und priorisiert behandelt werden.
		§ 30 (1): „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen“ → Text der VdS 10k entsprechend angepasst	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.
		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.*
	Identifizierte organisatorische Maßnahmen SOLLTEN in IS Richtlinien (siehe Kapitel 6) oder in Verfahren (siehe Anhang A 2.1) aufgenommen werden.	Organisatorische Maßnahmen in RL und Verfahren verankern: SOLLTE oder MUSS? Kann in die VdS 10k als SOLLTE aufgenommen werden.	Identifizierte organisatorische Maßnahmen SOLLTEN in IS-Richtlinien (siehe Kapitel 6) oder in Verfahren (siehe Anhang A 2.1) aufgenommen werden.
		§ 30 Abs. 1 („Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.“)	Die Dokumentation der Maßnahmen MUSS beinhalten, warum sie als geeignet, verhältnismäßig und wirksam angesehen werden.
G2	Die Umsetzung der Maßnahmen MUSS kontrolliert und auf Wirksamkeit geprüft werden.	übernehmen	Die Umsetzung der Maßnahmen MUSS kontrolliert und auf Wirksamkeit geprüft werden.
			Hierzu SOLLTEN erhebliche Risiken einzelnen Mitarbeitern (Risk Owner) zugeordnet und konkrete zeitliche Vorgaben für deren Behandlung definiert werden.
G3	Wenn Risiken nicht angemessen behandelt werden können, MÜSSEN sie vom Topmanagement akzeptiert und dies dokumentiert werden.	übernehmen	Wenn Risiken nicht angemessen behandelt werden können, MÜSSEN sie vom Topmanagement akzeptiert und dies dokumentiert werden.

A 2.4 Wiederholung und Anpassung

Ref	VdS 10000	Kommentar / ToDo	VdS 10100

G1	Risikoanalysen MÜSSEN jährlich auf ihre Aktualität geprüft und bei Bedarf wiederholt werden.	übernehmen	Risikoanalysen MÜSSEN jährlich auf ihre Aktualität geprüft und bei Bedarf wiederholt werden.
G2	Sie MÜSSEN darüber hinaus zeitnah überarbeitet werden, wenn eine der folgenden Faktoren auftritt:	Änderung: Risikoanalysen → Sie (Diese Änderung bitte auch in die VdS 10k aufnehmen), ansonsten: übernehmen	Sie MÜSSEN darüber hinaus zeitnah überarbeitet werden, wenn eine der folgenden Faktoren auftritt:
G2.1	1. Der Gegenstand der Risikoanalyse hat sich wesentlich verändert (z. B. die Hardware, die Software oder die Konfiguration eines IT-Systems).	übernehmen	1. Der Gegenstand der Risikoanalyse hat sich wesentlich verändert (z. B. die Hardware, die Software oder die Konfiguration eines IT-Systems).
G2.2	2. Der Einsatzzweck des untersuchten Gegenstands hat sich wesentlich geändert.	übernehmen	2. Der Einsatzzweck des untersuchten Gegenstands hat sich wesentlich geändert.
G2.3	3. Die Gefährdungslage hat sich erhöht (z. B. wenn eine neue Gefährdung bekannt wurde oder sich eine bestehende Gefährdung wesentlich erhöht hat).	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

	VdS 10000	Kommentar / ToDo	VdS 10100
G1		§ 38 (1): Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.	Die Maßnahmen des Risikomanagements MÜSSEN jährlich vom Topmanagement geprüft und gebilligt werden.