Lizenzbestimmungen

2. Mapping: NIS-2 (BSIG n.F.) → VdS 10100

In diesem Artikel wird dokumentiert, wie die VdS 10100 die Anforderungen des BSIG n.F. umsetzt.

Der Artikel ist noch in Arbeit und wird nach und nach vervollständigt:

- Links zeigen noch ins Leere (die Verlinkungen deuten darauf hin, dass eine Kommentierung der VdS 10100 in Arbeit ist).
- Es sind noch nicht alle relevanten Paragrafen berücksichtigt.
- Es fehlen für § 30 Abs. 2 noch einige Mappings (mit dem Tag Fix Me! markiert).

§ 28 BSIG n.F. (Besonders wichtige Einrichtungen und wichtige Einrichtungen)

In Paragraf § 28 BSIG n.F. ist festgelegt, welche Einrichtungen von NIS-2 betroffen sind. Die VdS 10100 verweist auf diesen Paragrafen in Abschnitt 1.3.1 hin und fordert, dass die implementierende Organisation prüft, ob sie als „wichtige“ oder „besonders wichtige“ Einrichtung im Sinne von § 28 BSIG n.F. gilt.

§ 30 BSIG n.F. (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen)

§ 30, Abs. 1, Satz 1 BSIG n.F.

Gesetzestext	(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die in Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.
Umsetzung	Die VdS 10100 beschreibt ein vollständiges Informationssicherheitsmanagementsystem (ISMS) und leitet die implementierende Organisation an, die Informationsverarbeitung risikobasiert abzusichern. Der Geltungsbereich der VdS 10100 umfasst sämtliche informationstechnischen Systeme (IT-Infrastrukturen), Komponenten (IT-Ressourcen) und Prozesse, die von der jeweiligen Einrichtung für die Erbringung ihrer Dienste genutzt werden.

§ 30, Abs. 1, Satz 2 BSIG n.F.

Gesetzestext	Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind 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.
Umsetzung	Die entsprechenden Anforderungen des BSIG n.F. wurden wortwörtlich in die VdS 10100 übernommen: • Anhang A.2.4: In den Anforderungen an die Risikoanalyse fordert die VdS 10100, das Ausmaß der Risikoexposition, die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. • Anhang A.2.5: In den Anforderungen an die Risikobehandlung fordert die VdS 10100, die Größe der Einrichtung und die Umsetzungskosten zu berücksichtigen.

§ 30, Abs. 1, Satz 3 BSIG n.F.

Gesetzestext	Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

Umsetzung	Fix Me! Satz 1: Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die in Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Die Organisation muss die Einhaltung folgender Anforderungen dokumentieren: 1. die ergriffenen Maßnahmen sind geeignet, die angemessene Informationssicherheit zu gewährleisten ◦ Für die IT-Ressourcen der Klasse „standard“ (und höher) definiert die VdS 10100 technische und organisatorische Maßnahmen, die dem Stand der Technik entsprechen. Wenn die implementierende Organisation sich gegen die vollständige Umsetzung der Maßnahmen entscheidet, muss sie die dadurch entstehenden Risiken in das Risikomanagement aufnehmen. ◦ Für IT-Ressourcen der Klasse „wichtig“ und darüber fordert die VdS 10100 unter anderem ein individuelles Risikomanagement. 2. die ergriffenen Maßnahmen sind verhältnismäßig ◦ 3. die ergriffenen Maßnahmen sind wirksam, sie gewährleisten eine angemessene Informationssicherheit ◦ Die angemessene Sicherheit wird durch die IS-Leitlinie definiert und durch die IS-Richtlinien weiter spezifiziert ◦ Kapitel 21 fordert die strukturierte Erfassung von Kennzahlen anhand derer sich die Wirksamkeit ausgewählter Maßnahmen erkennen lässt (Stichproben) ◦ Die in der VdS 10100 an verschiedenen Punkten verankerte kontinuierliche Verbesserung sorgt für die Sicherstellung der Wirksamkeit der Maßnahmen ◦ Alle obigen Punkte werden dokumentiert (IS-Leitlinie, IS-Richtlinie, Bericht des ISB an das IST, Fortentwicklung der Verfahren, …) 1. die ergriffenen Maßnahmen sind geeignet, Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. 2. die ergriffenen Maßnahmen sind verhältnismäßig, Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. 3. die ergriffenen Maßnahmen sind wirksam, sie gewährleisten, dass Auswirkungen von Sicherheitsvorfällen möglichst gering sind.

§ 30, Abs. 2, Satz 1 BSIG n.F.

Gesetzestext	(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.

Umsetzung	1. Stand der Technik ◦ Die VdS 10100 fordert, dass die IT-Ressourcen in die Schutzkategorien „nachrangig“, „standard“, „wichtig“ und „kritisch“ eingeteilt werden. Für die IT-Ressourcen der Schutzkategorie „standard“ und höher müssen grundlegende Sicherheitsmaßnahmen implementiert werden. Diese orientieren sich am Stand der Technik. Für die IT-Ressourcen der Schutzkategorie „wichtig“ und höher müssen individuelle Risikoidentifikationen und Risikoanalysen durchgeführt und die erkannten Risiken zeitnah und angemessen behandelt werden. Die Organisation muss dazu geeignete, verhältnismäßige und wirksame Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der erkannten Risiken definieren, dokumentieren und umsetzen. Die VdS 10100 empfiehlt, dass die Maßnahmen fortschrittlich und bereits in der Praxis erprobt und von Experten und Fachkreisen anerkannt sein sollten. Diese Eigenschaften sind Merkmale für den von geforderten „Stand der Technik“. 2. Berücksichtigung der einschlägigen europäischen und internationalen Normen ◦ Abschnitt 2.1: Die VdS 10100 empfehlen an verschiedenen Stellen die Umsetzung etablierter Regelwerke. Werden die Regelwerke nicht umgesetzt, schreiben die VdS 10100 die Umsetzung ausgewählter grundlegender Prinzipien und Maßnahmen dieser Regelwerke vor. In folgenden Bereichen der VdS 10100 findet dieses Prinzip Anwendung: ▪ Abschnitt 9.1 E2: ISO/IEC 27001 oder BSI-Standard 200-2 ▪ Abschnitt 9.3 E1: ISO 22301 oder BSI-Standard 200-4 ▪ Abschnitt 13.1 E1: VdS 2007 ▪ Abschnitt 13.3 E1: DIN EN 50173/4-Reihe ▪ Abschnitt 16.1 E1: BSI-Standard 200-2 unter Berücksichtigung der IT-Grundschutz-Bausteine des BSI ▪ Abschnitt 17.1 E1: BSI-Standard 200-4 oder DIN EN ISO 22301 ▪ Abschnitt 18.1 E1: BSI-Standard 200-4 oder DIN EN ISO 22301 ▪ Abschnitt 19.1 E1: ISO/IEC 27001 oder IT-Grundschutz-Baustein CON.1 des BSI ▪ Anhang A.1 E1: DIN EN ISO 9001 ▪ Anhang A.2.1 E1: BSI-Standard 200-3, ISO/IEC 27005 oder ISO 31000 3. gefahrenübergreifender Ansatz: Die VdS 10100 arbeitet gefahrenübergreifend. Gefahren und Gefährdungen werden systematisch identifiziert, analysiert und behandelt, unabhängig davon, ob sie technisch, organisatorisch, menschlich oder physisch verursacht sind. ◦ Abschnitt 3.1: Im Regelwerk werden Begriffe wie „Bedrohung“, „Gefährdung“ und „Gefahr“ generisch definiert und nicht auf Cyberangriffe verengt, sondern allgemein als Möglichkeit einer Schadwirkung bzw. Bedrohung über Schwachstellen auf Schutzobjekte verstanden. ◦ Anhang A.2: Die Richtlinie verlangt, bei unvollständiger Umsetzung von Maßnahmen und für wichtige IT-Ressourcen eine Risikoidentifizierung, -analyse und -behandlung der daraus entstehenden Risiken durchzuführen. Durch dieses Vorgehen wird sichergestellt, dass auch Ersatzmaßnahmen und andere Gefahrenarten einbezogen. ◦ Anhang A.2.3: Das Vorgehen für das Identifizieren von Risiken muss gewährleisten, dass umfassend nach möglichen Bedrohungen und Schwachstellen gesucht wird. ◦ Die VdS 10100 schreibt eine kontinuierliche Überprüfung und Anpassung der Gefährdungslage vor (jährliche Reviews, Nachbereitung von Störungen und Sicherheitsvorfällen, kontinuierlicher Verbesserungsprozess).

§ 30, Abs. 2, Satz 2 BSIG n.F.

Gesetzestext	Die Maßnahmen müssen zumindest Folgendes umfassen:
Umsetzung	• Abschnitt 1.1: In der Einleitung betonen die VdS 10100, dass sie Mindestanforderungen definieren. • Anhang A.2: Die Richtlinien verlangen an verschiedenen Stellen die Durchführung von Risikoidentifikationen, -analysen und -behandlungen. Dadurch wird die implementierende Organisation in die Lage versetzt, geeigneten Maßnahmen zu Erhaltung und Verbesserung der Informationssicherheit zu erkennen, selbst wenn diese nicht im BSIG n.F. oder der VdS 10100 explizit erwähnt werden. • Abschnitt 8.2: Die Richtlinien fordern ein Verfahren, mit dem regelmäßig aus verlässlichen Quellen Informationen über neue Bedrohungen und Schwachstellen und über mögliche Gegenmaßnahmen bezogen werden. Damit ist sichergestellt, dass die Organisation Kenntnis über Maßnahmen zu Erhaltung und Verbesserung der Informationssicherheit erhält, die nicht im BSIG n.F. oder den Richtlinien selbst aufgeführt sind.

Punkt 1

Gesetzestext	1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,

Umsetzung	1. Konzepte in Bezug auf die Risikoanalyse: ◦ Abschnitt 3.1: Es werden grundlegende Begriffe wie „Gefahr“, „Bedrohung“, „Schwachstelle“, „Gefährdung“ und „katastrophaler Schaden“ definiert, damit die Organisation ein gemeinsames Verständnis für Risiken hat. ◦ Anhang A.2.4: Die VdS 10100 fordern, dass Risikoidentifikation, -analysen und -behandlungen nach einer definierten Vorgehensweise durchgeführt werden und stellt detaillierte Anforderungen. 2. Konzepte in Bezug auf die Sicherheit in der Informationstechnik: Die VdS 10100 setzt diese Anforderung um, indem sie als integrale Bestandteile eines ISMS eine Leitlinie und mehrere Richtlinien fordert. ◦ Kapitel 5: Das Topmanagement muss eine Leitlinie zur Informationssicherheit (IS-Leitlinie) erstellen, in Kraft setzen und veröffentlichen. In ihr werden die Ziele und der Stellenwert der Informationssicherheit in der Organisation festgelegt und die Verantwortlichkeiten zu Erreichung der Ziele definiert. ◦ Kapitel 6: Zur Unterstützung und Konkretisierung der IS-Leitlinie müssen IS-Richtlinien zu spezifischen Themen erstellt werden, wie Aufbau und Funktionsweise des ISMS (siehe Abschnitt 6.4), Regelungen für Nutzer (siehe Abschnitt 6.5), Mobile IT-Systeme (siehe Abschnitt Abschnitt 10.5.2), Mobile Datenträger (siehe Abschnitt Abschnitt 12.2), Beschaffung von IT-Ressourcen (siehe Abschnitt 14.2), Speicherorte (siehe Abschnitt 16.2), Sicherheitsvorfälle (siehe Abschnitt Abschnitt 17.2) und IT-Krisen (siehe Abschnitt Abschnitt 18.2).

Punkt 2

: Work in Progress

Gesetzestext	2. Bewältigung von Sicherheitsvorfällen,

Umsetzung	Für die Bewältigung von Sicherheitsvorfällen verlangt die VdS 10100 ein strukturiertes Incident- und Krisenmanagement. • Abschnitt 3.1: Die Begriffe „Sicherheitsvorfall“ und „erheblicher Sicherheitsvorfall“ sind in der VdS 10100 im Wortlaut der NIS-2-Richtlinie definiert. • : Vorbereitung: Es müssen Zuständigkeiten, Kommunikationswege, Meldewege und Verfahren für Vorfall- und Krisenmanagement vorab festgelegt und dokumentiert werden. • Erkennung: Vorgaben zur Überwachung und zum Erkennen von Sicherheitsvorfällen (Monitoring, Log-Auswertung, Meldewege für Mitarbeitende usw.). • Reaktion und Bewältigung: Beschriebene Schritte zur Eindämmung, Analyse, Beseitigung der Ursache und zum Wiederanlauf des Betriebs; explizit adressiert werden Krisenbewältigung und Wiederanlauf nach Notfällen. • Abschnitt 17.2: In einer IS-Richtlinie werden Verantwortlichkeiten definiert und Strukturen für das Melden, Untersuchen, Eskalieren und Kommunizieren von Sicherheitsvorfällen geschaffen. • Abschnitt 17.3: Die Organisation muss prüfen, welche Maßnahmen notwendig sind, um mögliche Sicherheitsvorfälle erkennen zu können. Das Ergebnis der Prüfung muss zusammen mit seiner Begründung dokumentiert werden. • Abschnitt 17.4: Die implementierende Organisation muss ein Verfahren für die Reaktion auf Sicherheitsvorfälle etablieren. Das Verfahren muss sicherstellen, dass die gesetzlichen Meldepflichten bei erheblichen Sicherheitsvorfällen (Erstmeldung, Bewertung des Sicherheitsvorfalls, Zwischenmeldungen auf Anfrage des BSI, ggf. Fortschrittsmeldungen und Abschlussmeldung) erfüllt und dabei die gesetzlichen Fristen eingehalten werden. • Abschnitt 17.4: Sicherheitsvorfälle müssen nachbereitet werden. Es müssen die Ursachen des Sicherheitsvorfalls ermittelt, die Bewältigung des Sicherheitsvorfalls bewertet und konkrete Verbesserungen erarbeitet werden.

Punkt 3

Gesetzestext	3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,

Umsetzung	1. Aufrechterhaltung des Betriebs ◦ Trennung von wichtigen/kritischen IT-Systemen von und untereinander  ◦ Kapselung von wichtigen/kritischen IT-Systeme  ◦ Überwachung von IT-Systemen  2. Backup-Management ◦ Kapitel 16: Kapitel 16 der VdS 10100 behandelt Datensicherung und -wiederherstellung. Das Kapitel gliedert sich in sechs Abschnitte. ▪ Abschnitt 16.1 führt in die Materie ein und empfiehlt, die Datensicherung auf Basis eines anerkannten Standards wie z. B. BSI-Standard 200-2 unter Berücksichtigung der IT-Grundschutz-Bausteine des BSI zu implementieren. ▪ Abschnitt 16.2 fordert, die Speicherorte für die Daten der Organisation in einer IS-Richtlinie festzulegen. ▪ Abschnitt 16.3 verpflichtet die Organisation, Verfahren für die Datensicherung und -wiederherstellung zu implementieren. Die Verfahren müssen ▪ Abschnitt 16.4 stellt sicher, dass der ISB jährlich prüft, ob Änderungen an IT-Systemen sowie an gesetzlichen, vertraglichen und betrieblichen Rahmenbedingungen eine Anpassung der Sicherungs- und/oder Wiederherstellungsverfahren erforderlich machen und dass notwendige Anpassungen zeitnah implementiert werden. ▪ Abschnitt 16.5 schreibt vor, dass IT-Systeme für die Datensicherung und -wiederherstellung strukturiert vor unbefugtem Zugriff abgesichert werden müssen und welche Bereiche von Speicherorten, Servern, aktiven Netzwerkkomponenten und mobilen IT-Systemen in welchem Rhythmus gesichert werden müssen. Wenn einzelne Punkte dieses Abschnitts nicht umgesetzt werden, müssen die dadurch entstehenden Risiken in das Risikomanagement (siehe Anhang A.2) aufgenommen werden. ▪ Abschnitt 16.6 fordert zusätzliche Maßnahmen für wichtige IT-Systeme in Bezug auf die Datensicherung und -wiederherstellung. So müssen im Zuge des Risikomanagements der wichtigen IT-Systeme (siehe Abschnitt 10.6) die Folgen eines Datenverlusts analysiert und dabei der maximal tolerierbare Datenverlust (MTD) bestimmt werden. Wichtige IT-Systeme müssen vollständig gesichert werden. Dabei darf der MTD nicht überschritten werden. Die Wiederherstellung von wichtgen IT-Systemen muss innerhalb der MTA gewährleistet sein, sofern keine Ersatzsysteme oder -verfahren (siehe Abschnitt 10.6.8) verfügbar sind. 3. Wiederherstellung nach einem Notfall ◦ Abschnitt 16.3 Die Datensicherung und -wiederherstellung muss jährlich oder bei einer Änderung des Verfahrens getestet werden, indem ein betroffenes IT-System nach dem Zufallsprinzip ausgewählt, gemäß des Verfahrens gesichert und in einer Testumgebung wiederhergestellt wird. ◦ Abschnitt 17.5: Für jede wichtige IT-Ressource muss ein Wiederanlaufplan erstellt, die Abhängigkeiten der wichtigen IT-Ressourcen untereinander dokumentiert und dabei die Reihenfolge ihrer Wiederherstellung festgelegt werden. 4. Krisenmanagement ◦ Abschnitt 4.6 und Abschnitt 4.7: Das Topmanagement muss einen IT-Krisenmanager bestellen, der im Fall einer IT-Krise die Leitung des IT-Krisenmanagements übernimmt. Er wird durch und einen IT-Krisenstab unterstützt. ◦ Kapitel 18: Kapitel 18 der VdS 10100 behandelt IT-Krisen. Das Kapitel gliedert sich in fünf Abschnitte. ▪ Abschnitt 18.1 erläutert den Sinn einer strukturierte Vorbereitung auf Krisen die für oder durch die IT entstehen und empfiehlt das Implementieren eines Business Continuity Management (BCM) auf Basis eines anerkannten Standards. ▪ Abschnitt 18.2 fordert, dass in einer IS-Richtlinie Regelungen für den Umgang mit IT-Krisen getroffen werden. ▪ Abschnitt 18.3 fordert, dass ein generische Vorgehensweise in Form eines Verfahrens (siehe Anhang A.1) für die Bewältigung von IT-Krisen implementiert wird (genereller IT-Krisenplan). ▪ Abschnitt 18.4 fordert das Identifizieren der und die strukturierte Vorbereitung auf die wahrscheinlichsten IT-Krisen. Wenn einzelne Punkte dieses Abschnitts nicht umgesetzt werden, müssen die dadurch entstehenden Risiken in das Risikomanagement (siehe Anhang A.2) aufgenommen werden. ▪ Abschnitt 18.5 fordert, dass für den IT-Krisenfall Kommunikationskanäle in der Organisation zur Verfügung stehen, die auch bei einer Störung oder einem Ausfall der IT-Infrastruktur genutzt werden können.

Punkt 4

Gesetzestext	4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
Umsetzung	• Abschnitt 3.1: Die VdS 10100 fasst informationstechnische Systeme (IT-Infrastrukturen), informationstechnischen Komponenten (IT-Ressourcen) und Prozesse die von externen Stellen wie z. B. Lieferanten, Partnern oder Verbänden eingekauft oder zur Verfügung gestellt werden unter dem generischen Begriff „externe IT-Ressource“ zusammen. • Kapitel 14: Mit den Lieferanten externer IT-Ressourcen müssen Verträge geschlossen werden, die die externen IT-Ressourcen spezifizieren und die Lieferanten zur Erfüllung der vereinbarten Leistungen verpflichten. Für wichtige externe IT-Ressourcen müssen die Anforderungen an deren Informationssicherheit im Rahmen einer Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) ermittelt und die Leistungen, Sicherheitsmaßnahmen sowie die Kommunikation und die Mitwirkungspflichten bei Leistungsänderungen und Vertragsauflösung vertraglich vereinbart werden. Wenn einzelne Punkt nicht vertraglich vereinbart werden können, müssen die dadurch entstehenden Risiken in das Risikomanagement (siehe Anhang A.2) aufgenommen werden.

Punkt 5

Gesetzestext	5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,

Umsetzung	1. Sicherheitsmaßnahmen bei Erwerb von... 1. ...informationstechnischen Systemen (IT-Infrastrukturen), informationstechnischen Komponenten (IT-Ressourcen) und Prozessen: ■ Abschnitt 3.1: Die VdS 10100 fasst informationstechnische Systeme (IT-Infrastrukturen), informationstechnischen Komponenten (IT-Ressourcen) und Prozesse die von externen Stellen wie z. B. Lieferanten, Partnern oder Verbänden eingekauft oder zur Verfügung gestellt werden unter dem generischen Begriff „externe IT-Ressource“ zusammen. ■ Kapitel 14: Mit den Lieferanten externer IT-Ressourcen müssen Verträge geschlossen werden, die die externen IT-Ressourcen spezifizieren und die Lieferanten zur Erfüllung der vereinbarten Leistungen verpflichten. Für wichtige externe IT-Ressourcen müssen die Anforderungen an deren Informationssicherheit im Rahmen einer Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) ermittelt und die Leistungen, Sicherheitsmaßnahmen sowie die Kommunikation und die Mitwirkungspflichten bei Leistungsänderungen und Vertragsauflösung vertraglich vereinbart werden. Wenn einzelne Punkt nicht vertraglich vereinbart werden können, müssen die dadurch entstehenden Risiken in das Risikomanagement (siehe Anhang A.2) aufgenommen werden. ■ Abschnitt 14.3 und Abschnitt 14.4.2: Die VdS 10100 empfiehlt für alle externen IT-Ressourcen das Management und die Offenlegung von Schwachstellen vertraglich festzulegen. Für wichtige IT-Ressourcen ist diese Maßnahme verpflichtend. 2. Sicherheitsmaßnahmen bei Entwicklung von informationstechnischen Systemen (IT-Infrastrukturen), informationstechnischen Komponenten (IT-Ressourcen) und Prozessen: ◦ Abschnitt 4.12: Projektverantwortliche müssen den ISB bei allen Projekten mit Auswirkung auf die Informationsverarbeitung konsultieren, um sicherzustellen, dass sicherheitsrelevante Aspekte ausreichend beachtet werden. ◦ Kapitel 20: Wenn IT-Ressourcen entwickelt oder angepasst werden muss der Projektverantwortliche sicherstellen, dass in der Planungsphase die Anforderungen an deren Informationssicherheit festgelegt werden, ein entsprechendes Sicherheitskonzept definiert und im Laufe des Projekts umgesetzt wird. 3. Sicherheitsmaßnahmen bei Wartung von, informationstechnischen Systemen (IT-Infrastrukturen), informationstechnischen Komponenten (IT-Ressourcen) und Prozessen: Kapitel 20 - Fix Me!

Punkt 6

Gesetzestext	6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,

Umsetzung	• Abschnitt 4.4: Der ISB muss jährlicher an das Informationssicherheitsteam (IST) über den aktuellen Stand der Informationssicherheit, insbesondere über Mängel, Risiken und Sicherheitsvorfälle berichten. Zu diesem Zweck müssen strukturiert Kennzahlen ermittelt werden (siehe Kapitel 21). • Abschnitt 8.3: Die VdS 10100 empfiehlt, Schulungs- und Sensibilisierungsmaßnahmen von den Teilnehmern bewerten zu lassen, um ihren Inhalt, ihre Form und ihren Ablauf zu verbessern. • Abschnitt 17.4 und Abschnitt 18.3: Im Zuge der Bewältigung von Sicherheitsvorfällen und IT-Krisen findet eine Nachbereitung statt, bei der die Ursachen ermittelt, ihre Bewältigung bewertet und konkrete Verbesserungen erarbeitet werden. • Kapitel 21: Die VdS 10100 fordert, dass die Wirksamkeit und Effizienz der Sicherheitsmaßnahmen für die Verantwortlichen transparent zu gemacht wird, damit frühzeitig Probleme und Verbesserungspotential erkannt werden können. Hierzu fordert sie, dass strukturiert Kennzahlen aus den Bereichen Sicherheitsvorfälle, Verfügbarkeit der IT-Infrastruktur, Ergebnisse von Audits und von sonstigen Überprüfungen, Awareness und Verhalten der Mitarbeiter, Management und kontinuierliche Verbesserung , Funktionieren des ISMS und Risikomanagement erhoben und im Zuge des jährlichen Berichts des ISB an das IST (siehe Abschnitt 4.4) vorgestellt werden. • Anhang A.1: Umsetzung, Angemessenheit und Effektivität von Verfahren werden jährlich bei einem Drittel der Verfahren überprüft.

Punkt 7

Gesetzestext	7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,

Umsetzung	Die VdS 10100 setzt diese Anforderung von NIS-2 über ein eigenes Kapitel zu Schulung und Sensibilisierung um, das über begleitende Anforderungen an Qualifikation der Mitarbeiter, Wissensaktualisierung und kontinuierliche Verbesserung in der Organisation verankert ist: • Abschnitt 8.3: Abschnitt 8.3 fordert, dass Mitarbeitende in Informationssicherheit geschult und sensibilisiert werden und dies zielgruppenorientiert und in regelmäßigen Abständen geschieht. • Abschnitt 4.10: Aus Abschnitt 4.10 kann abgelesen werden, dass die Vorgesetzten auf die Durchführung der Schulungs- und Sensibilisierungsmaßnahmen achten müssen. • Abschnitt 7.3: Abschnitt 7.3 fordert, dass Mitarbeitende im Zuge der Aufnahme ihrer Tätigkeit in die IS-Leitlinie und in sämtliche für sie relevante Regelungen zur Informationssicherheit (wie z. B. in die Inhalte entsprechender Richtlinien und Verfahren) eingewiesen werden. • Abschnitt 8.2: In Abschnitt 8.2 wird gefordert, dass regelmäßig aus verlässlichen Quellen Informationen über neue Bedrohungen und Schwachstellen und über mögliche Gegenmaßnahmen bezogen werden und die jeweils Verantwortlichen über relevante Entwicklungen zeitnah informiert werden. Daraus ist die Aktualisierung und Anpassung der Schulungs- und Sensibilisierungsmaßnahmen gewährleistet. • Abschnitt 21.2: Zusätzlich wird gefordert, dass die Awareness und Verhalten der Mitarbeiter anhand von Kennzahlen gemessen wird, damit die Wirksamkeit und Effizienz der Schulungs- und Sensibilisierungsmaßnahmen für die Verantwortlichen transparent gemacht und um frühzeitig Probleme und Verbesserungspotential erkannt werden. • Anhang A.1: Die Maßnahmen der Abschnitte 8.3, 8.2 und 7.3 werden in Form von Verfahren (siehe Anhang A.1) definiert und unterliegen damit der kontinuierlichen Verbesserung.

Punkt 8

Gesetzestext	8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,

Umsetzung	• Abschnitt 10.5.3: Mit einer Risikoidentifizierung, -analyse und -behandlung muss untersucht werden, welche Informationen auf mobilen IT-Systemen durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden. • Abschnitt 10.6.6: Im Zuge der Risikoidentifizierung, -analyse und -behandlung für wichtige IT-Systeme (siehe Abschnitt 10.7.1) muss untersucht werden, welche Informationen auf wichtigen IT-Systemen durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden. • Abschnitt 11.5.4 und Abschnitt 11.5.5: Der Zugang zu nichtöffentlichen Bereichen von IT-Systemen und die Kopplung von Netzwerken der Organisation über weniger oder nicht vertrauenswürdige Netzwerke muss abgesichert werden. Dabei müssen die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen geschützt werden. Die VdS 10100 gibt hier die Empfehlung zum Einsatz von kryptografischen Maßnahmen. • Abschnitt 12.3: Für alle wichtigen mobilen Datenträger muss eine Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) etabliert werden. Dabei muss festgelegt werden, welche Informationen auf mobilen Datenträgern durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden. • Abschnitt 17.5.1: Für alle wichtigen IT-Systeme muss ein Wiederanlaufplan erstellt werden, der u. a. eine Aufstellung der für die Wiederherstellung zwingend benötigten Ressourcen beinhaltet. In dieser Aufstellung müssen die Schlüssel für kryptografische Maßnahmen beinhaltet sein. • Kapitel 19: Kapitel 19 der VdS 10100 behandelt Kryptografie als zentrale Komponente der Informationssicherheit. Das Kapitel gliedert sich in drei Abschnitte. ◦ Abschnitt 19.1 erläutert die Rolle der Kryptografie beim Schutz von Vertraulichkeit, Integrität und Authentizität ◦ Abschnitt 19.2 verpflichtet die umsetzende Organisation, ausreichend sichere kryptografische Maßnahmen und Betriebsparameter zu wählen. Wenn kryptografischen Maßnahmen als unsicher erkannt werden, müssen sie zeitnah verbessert oder ersetzt werden. Zusätzlich stellt die VdS 10100 detaillierte Anforderungen an das Management der notwendigen Schlüssel. Die Anforderungen umfasst u. a. die Generierung, Verteilung, Speicherung und Rotation der Schlüssel, um Kompromittierungen zu vermeiden. ◦ Abschnitt 19.3 fordert, dass für kritische Informationen (siehe Abschnitt 9.4) festgelegt wird, wie kritische Informationen im Ruhezustand als auch bei der Übertragung durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden. Hierzu empfiehlt die VdS 10100 die Durchführung einer entsprechenden Risikoidentifizierung, -analyse und -behandlung.

Punkt 9

Gesetzestext	9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,

Umsetzung	1. Konzepte für die Sicherheit des Personals ◦ Abschnitt 7.2 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. ◦ Abschnitt 7.3 Vor Aufnahme der Tätigkeit müssen Mitarbeiter sich zur Vertraulichkeit verpflichten. Sie müssen in die IS-Leitlinie und in sämtliche für sie relevante Regelungen zur Informationssicherheit eingewiesen und im Umgang mit den für sie relevanten Sicherheitsmaßnahmen geschult werden. Danach erhalten Sie die benötigten IT-Ressourcen, Zugänge, Zugriffsrechte sowie Authentifizierungsmerkmale wie Schlüssel, Transponder, Zertifikate etc. und werden in deren Nutzung geschult. ◦ Abschnitt 7.4 Bei Beendigung oder Wechsel der Tätigkeit eines Mitarbeiters werden Mitarbeiter, Kunden sowie relevante externe Stellen über die Änderungen informiert und die zur Verfügung gestellten IT-Ressourcen, Zugänge, Zugriffsrechte sowie Authentifizierungsmerkmale wie Schlüssel, Transponder, Zertifikate etc. umgehend überprüft und bei Bedarf angepasst. 2. Konzepte für die Zugriffskontrolle ◦ Abschnitt 7.3: Strukturiertes Vorgehen bei Aufnahme einer Tätigkeit, dabei strukturierte Vergabe der Zugriffsrechte und Authentifizierungsmerkmale. ◦ Abschnitt 7.4: Strukturiertes Vorgehen bei Beendigung oder Wechsel der Tätigkeit eines Mitarbeiters, dabei strukturierte Anpassung der Zugänge, Zugriffsrechte und Authentifizierungsmerkmale. ◦ Abschnitt 10.3.2: Schutz der Informationen vor unrechtmäßigem Zugriff bei Ausmusterung und Wiederverwendung von IT-Systemen, indem die Informationen z. B. zuverlässig gelöscht, überschrieben, aus dem IT-System entfernt werden oder indem das IT-System insgesamt zerstört wird. ◦ Abschnitt 10.4.2: Sämtliche Zugriffsrechte und Privilegien der Anwendungssoftware SOLLTEN auf ein Mindestmaß reduziert werden. ◦ Abschnitt 10.4.8: Der Zugang zu allen nichtöffentlichen Bereichen der IT-Systeme MUSS durch geeignete Anmeldeverfahren abgesichert werden, die eine Authentifizierung verlangen. ◦ Abschnitt 10.4.9: Für jeden Zugang sollten die Prinzipien „Need-to-Know“, „Least-Privileges“ und „Least-Functionality“ umgesetzt werden. ◦ Abschnitt 11.5.4: Der Zugang zu nichtöffentlichen Bereichen von IT-Systemen über weniger oder nicht vertrauenswürdige Netzwerke MUSS abgesichert werden. Dabei müssen Fernzugriffe zeitlich begrenzt, innerhalb festgelegter Zeitfenster erfolgen und protokolliert werden. ◦ Kapitel 15: Die VdS 10100 fordert die strukturierte Vergabe, Anpassung und Entzug von sämtlichen Zugänge und Zugriffsrechte sowie von ausgesuchten Zutrittsrechten. Sämtliche Zugänge und Zugriffsrechte, Zutrittsrechte zu Serverräumen, Server- oder Netzwerkschränken sowie sämtliche Zutrittsrechte zu kritischen IT-Systemen dürfen nur genehmigt werden, wenn sie für die Aufgabenerfüllung notwendig sind. Zusätzlich müssen alle Zugänge und Zutrittsrechte zu kritischen IT-Systemen und sämtliche Zugriffsrechte auf kritische Informationen jährlich erfasst und daraufhin überprüft werden, ob sie gemäß der Verfahren aus Abschnitt 15.2 angelegt wurden und benötigt werden. Nicht ordnungsgemäß angelegte oder entzogene Zugänge, Zugriffsrechte oder Zutrittsrechte müssen als Sicherheitsvorfall (siehe Kapitel 17) behandelt werden. ◦ Abschnitt 20.2: Wenn IT-Ressourcen entwickelt oder angepasst werden für sie ein Sicherheitskonzept definiert und umgesetzt werden. Die VdS 10100 empfiehlt, in den Sicherheitskonzepten die Autorisierung der nutzenden Instanzen (Zugriffskontrolle) zu berücksichtigen. 3. Konzepte für die Verwaltung von IKT-Systemen (IT-Infrastrukturen)  4. Konzepten für die Verwaltung von IKT-Produkten (IT-Ressourcen)  5. Konzepten für die Verwaltung von IKT-Prozessen 

Punkt 10

Gesetzestext	10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.
Umsetzung	1. Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung ◦ Abschnitt 10.4.8 Die VdS 10100 fordert den Einsatz von Mehr-Faktor-Authentifizierung oder kontinuierliche Authentifizierung bei allen IT-Systemen, die dazu technisch in der Lage sind. Die unvollständige Umsetzung dieser Anforderung bei IT-Systemen, die technisch dazu in Lage sind muss als Risiko in das Risikomanagement (siehe Anhang A.2) aufgenommen werden (Prinzip Basisschutz). 2. gesicherte Sprach-, Video- und Textkommunikation ◦ Abschnitt 3.1 Die VdS 10100 betrachtet Sprach-, Video- und Textkommunikation als Verbindung. ◦ Abschnitt 11.6 Für wichtige Verbindungen wird ein Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) gefordert, in der die Bedrohungen Ausfall, unsichere Protokolle, unzureichende Authentisierung der Kommunikationspartner und unberechtigte Nutzung untersucht werden. 3. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung (Organisation) ◦ Abschnitt 18.5: Für den IT-Krisenfall müssen Kommunikationskanäle zur Verfügung stehen, die auch bei einer Störung oder einem Ausfall der IT-Infrastruktur genutzt werden können.

§ 32 BSIG n.F. (Meldepflichten)

Abschnitt 17.4:

§ 33 BSIG n.F. (Registrierungspflicht)

In Paragraf § 33 BSIG n.F. ist festgelegt, wie sich betroffene Einrichtungen registrieren und welche Informationen sie dabei übermitteln müssen. Die VdS 10100 verweisen auf diesen Paragrafen in Abschnitt 1.3.1. Sie fordern ein Verfahren mit dem sichergestellt ist, dass bei positiver Prüfung der Betroffenheit das Registrierungsverfahren gem. § 33 BSIG n.F. durchlaufen und dabei die dort gesetzten Fristen eingehalten wird.

§ 34 BSIG n.F. (Besondere Registrierungspflicht für bestimmte Einrichtungsarten)

§ 38 BSIG n.F. (Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen)

§ 38, Abs. 1, Satz 1 BSIG n.F.

Gesetzestext	(1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.
Umsetzung	• Abschnitt 4.3: Das Topmanagement muss sich zur Übernahme der Gesamtverantwortung für die Informationssicherheit verpflichten, insbesondere gem. § 38 BSIG n.F. für die Umsetzung und Überwachung des Risikomanagements und der Maßnahmen für die Informationssicherheit. • Abschnitt 4.4: Der Informationssicherheitsbeauftragte (ISB) muss jährlich an das Informationssicherheitsteam (IST) über den aktuellen Stand der Informationssicherheit, insbesondere über Mängel, Risiken und Sicherheitsvorfälle berichten. Zu diesem Zweck müssen strukturiert Kennzahlen ermittelt werden (siehe Kapitel 21). • Abschnitt 4.5: Das Topmanagement ist persönlich oder durch einen Repräsentanten im IST vertreten.

§ 38, Abs. 3, Satz 1 BSIG n.F.

Gesetzestext	(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Umsetzung	• Abschnitt 8.3: Abschnitt 8.3 der VdS 10100 fordert, dass ein Verfahren (siehe Anhang A.1) für Schulungs- und Sensibilisierungsmaßnahmen implementiert wird. Das Verfahren muss u. a. sicherstellen, dass das Topmanagement alle drei Jahre sowie bei Bedarf an speziellen Schulungen teilnimmt. Die Schulungen müssen ausreichende Kenntnisse und Fähigkeiten im Bereich der Informationssicherheit vermitteln, damit das Topmanagement seine gesetzliche Verantwortung gem. § 38 BSIG n.F. für die Umsetzung und Überwachung des Risikomanagements und der Maßnahmen für die Informationssicherheit nachkommen kann. Die VdS 10100 empfiehlt, dass die Inhalte der Schulung sich an den Vorgaben im Dokument „NIS-2-Geschäftsleitungsschulung“ des BSI orientieren.

§ 60 BSIG n.F. (Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten)

Fix Me!

Ich möchte...
...etwas in diesem Artikel kommentieren.☐
Ihre Kontaktdaten (für Rückfragen, optional)

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Name (optional) Ihre Mailadresse (optional)
Wir möchten wissen, dass Sie ein Mensch sind

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Geben Sie hier die Zahl 'zwanzig minus elf' als Ziffer ein. *
Ihr Feedback

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Wie finden Sie diesen Artikel? * bitte wählen
Was fanden Sie besonders gut? (optional)

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Was sollte besser werden? (optional)

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Feedback absenden