DSS connect GmbH
Gottlieb-Daimler Str. 40
74172 Neckarsulm

www.dss-connect.de
kontakt@dss-connect.de

Organize IT! 2024

Ihr zuverlässiger Partner für Datenschutz und IT-Sicherheit

AGENDA

22.10.2024

- **Sicher, dass sie sicher sind?**
- **Wie wird aus „ziemlich sicher“ ein bedarfsgerechtes und zertifizierbares Schutzkonzept ?**

AGENDA

- Sicher, dass sie sicher sind?
- Wie wird aus „ziemlich sicher“ ein bedarfsgerechtes und zertifizierbares Schutzkonzept ?

>> Sicherheit durch Transparenz

Datenschutz
IT-Sicherheit

„Wenn du alles unter Kontrolle hast, bist du zu langsam“

Mario Andretti

INFO #1

Begrifflichkeiten

„Sicherheit“ = die Situation, in der Entscheider das Ergebnis einer Aktion sicher vorhersagen kann.

Der englische Begriff **“Safety“** (= Gefahrlosigkeit) meint den Schutz der Umgebung vor einem Objekt.

Mit **“Security“** (= Schutz) wird der Schutz des Objektes vor der Umgebung beschrieben.

INFO #2

Sicherheit ist ein Zustand, bei dem bestimmte Gefahren beseitigt sind, und somit keine unvertretbaren Risiken bestehen.

oder einfacher, weil konkreter:

Wieviel Sicherheit braucht es, um definierte Schutzziele zu erreichen ?

INFO #3

- **Vertraulichkeit**
  Daten dürfen nur von berechtigten Personen eingesehen bzw. verarbeitet werden
- **Integrität**
  es muss sichergestellt sein, dass Daten nicht unerkannt bzw. unbemerkt verändert werden.
- **Verfügbarkeit**
  Zeitfenster der Systembereitschaft bzw. Minimierung des Risikos von Systemausfällen/ Downtime

INFO #4

Für welche Informationswerte benötigen wir Sicherheit ?

- HW ?
- SW?
- Kommunikationswege?
- Gebäude?
- MA-Wissen?
- Personenbezogene Daten?
- Firmengeheimnisse ?

CHECK #1

Fragen hierzu?

Datenschutz
IT-Sicherheit

REGEL #1

Jeder wird angegriffen.

Es gibt keine Ausnahmen!

Und keine 100% Sicherheit!

Datenschutz
IT-Sicherheit

REGEL #2

Früher oder später versagen ihre Schutzmaßnahmen !

Datenschutz
IT-Sicherheit

REGEL #3

Prävention ist wesentlich preiswerter als Reaktion !

CHECK #2

Ok ?
Einverstanden?

Dann auf zur Umsetzung…

SCHRITT #1

ANALYSE

- Erfassen Sie ihren IT-Verbund so präzise wie möglich (Asset-Management / CMDB)
- Stellen sie fest: wo, warum und wie lange liegen welche Daten (-Arten)
- Ermitteln sie die tatsächlichen Zugriffsrechte

Datenschutz
IT-Sicherheit

SCHRITT #2

BEWERTUNG (intern)

…… ihrer Kronjuwelen aus interner Sicht

- Ermitteln sie wie kritisch, sensibel bzw. schützenswert die gefundenen Daten sind
- Vergessen sie nicht die gesetzlichen Vorgaben (DSGVO, KRITIS, NIS2, Compliance…)
- Denken sie dabei in Geschäftsprozessen

Management Prozesse:
Strategie, Planung, Führung, Risiko-Mgnt., Qualitäts-Mgnt

Kernprozess**: Verkauf**

Kernprozess: **Service**

Kernprozess**: Produktion**

Support Prozesse:
Einkauf, IT, FiBu, Personalwesen,

SCHRITT #2

BEWERTUNG (extern)

…der Sicherheit aus der Angreifer-Perspektive

- Netzwerksicherheit
- Patchmanagement
- Verschlüsselung
- Malware-Infektionen
- Dataleaks im Kontext des Unternehmens

SCHRITT #3

MAßNAHMEN

- Definieren Sie technische und organisatorische Maßnahmen in Abhängigkeit des jeweiligen Schutzbedarfs
- Rollen Sie diese aus und ermitteln den Umsetzungsgrad
- Überprüfen Sie die Wirksamkeit der Maßnahmen (regelmäßig, PDCA)

CHECK #3

Da waren doch vorhin diese 3 Regeln…

REGEL #1

Jeder wird angegriffen.
Es gibt keine Ausnahmen!

- **Identifizieren Sie ihre Kronjuwelen**
- **Bewerten Sie ihre Risiko-Situation**
- **Sichern Sie ihre Systeme nach Stand der Technik ab**

REGEL #2

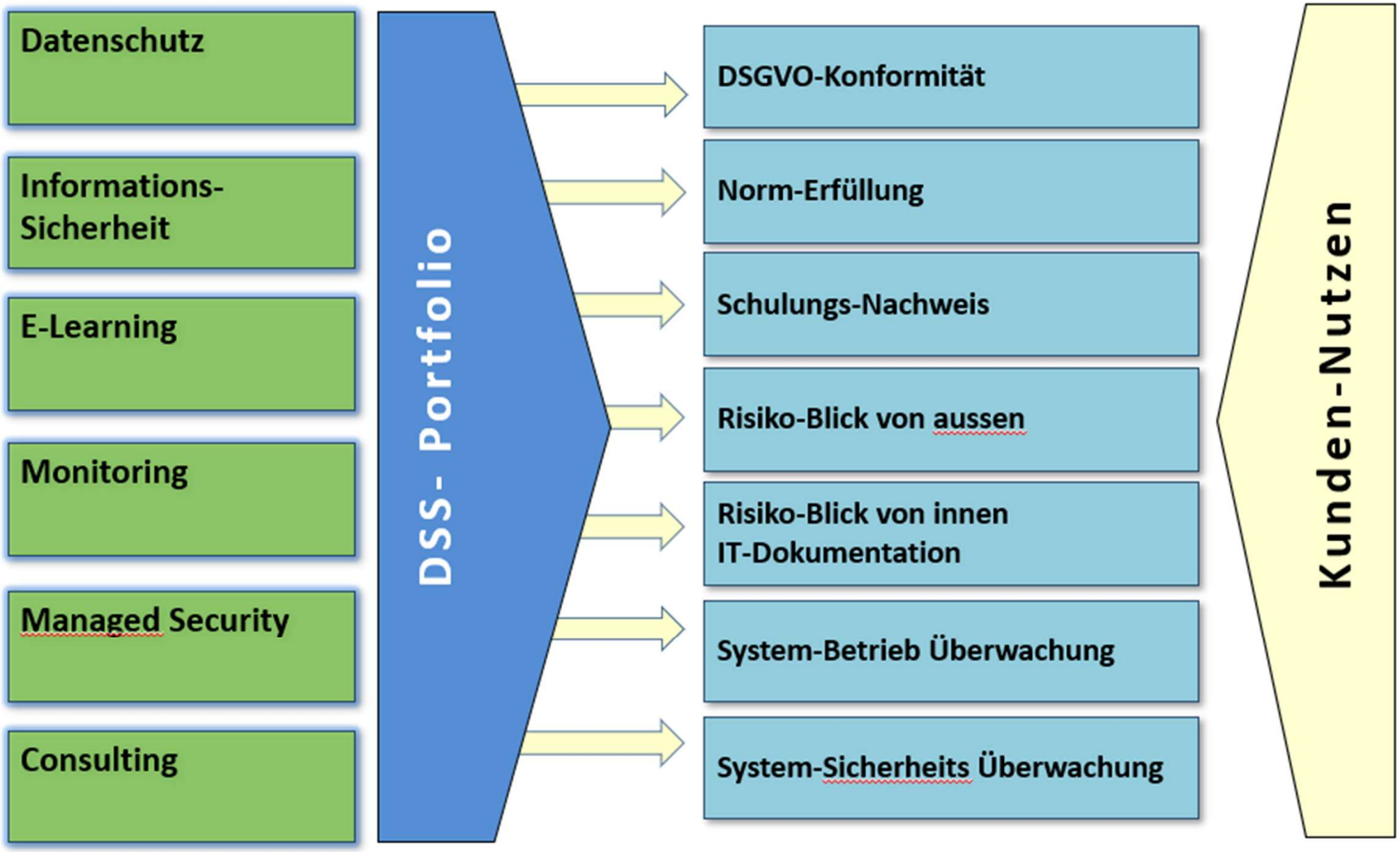
Früher oder später versagen ihre Schutzmaßnahmen!

- **Erarbeiten Sie ein Notfallkonzept**
- **Befolgen Sie die Backup-Strategie**
- **Planen Sie die Inanspruchnahme ext. Unterstützung**
- **Schließen Sie eine Cyber-Versicherung ab**

REGEL #3

Prävention ist wesentlich preiswerter als Reaktion!

- **Überwachen Sie kontinuierlich ihre IT-Landschaft**
- **Schulen und sensibilisieren Sie ihre Mitarbeiter**
- **Messen Sie den Lernerfolg durch Phishing-Mails**


Datenschutz
Informations-Sicherheit
E-Learning
Monitoring
Managed Security
Consulting
DSS- Portfolio
DSGVO-Konformität
Norm-Erfüllung
Schulungs-Nachweis
Risiko-Blick von aussen
Risiko-Blick von innen
IT-Dokumentation
System-Betrieb Überwachung
System-Sicherheits Überwachung
Kunden-Nutzen

INFO #5

- Sicherheit ist Chefsache!
- Sorgen Sie für klare Zuständigkeiten!
- Reagieren sie bei Warnungen und Vorfällen!
- Üben Sie den Ernstfall!

DSS Datenschutz IT-Sicherheit

Datenschutz
IT-Sicherheit

Teil 2

Grundsätzliches zu NIS-2

Die NIS2-Richtlinie wurde am 27. 12 2022 im Amtsblatt der EU veröffentlicht und trat am 16.1.2023 in Kraft. Sie muss bis **Oktober 2024 in nationales Recht** umgesetzt werden.

Mit NIS2 wird der **Anwendungsbereich** des IT-Sicherheitsgesetz 2.0 bzgl. der betroffenen Sektoren und Branchen **erheblich erweitert**.

In der NIS2-Richtlinie wird zwischen „**wesentlichen** Unternehmen/Einrichtungen“ und „**wichtigen** Unternehmen/Einrichtungen“ unterschieden. Diese Unterscheidung wirkt sich auf die Verpflichtungen der Unternehmen und das Ausmaß der Sanktionen aus

Der Anforderungskatalog wurde erweitert und spezifiziert:
Betroffene Unternehmen und Organisationen müssen angemessene Maßnahmen u.a. in den Bereichen **Cyber-Risk-Management, Lieferkettensicherheit, Business-Continuity-Management, Penetrationstests, Incident Response, Wiederherstellung und zur Berichterstattung** an die Behörden ergreifen.

Die Regeln für die Durchsetzung werden verschärft (z. B. Erweiterung der **Haftung** auf die Management-Ebene und Verschärfung der **Sanktionen**)

Grundsätzliches zu NIS-2
> Anforderungen gem. §30 BSIG-E

- Betroffen sind Unternehmen aus definierten Sektoren mit 10 - 50 Mio € Jahresumsatz und 50 - 249 MA.
- NIS2 unterteilt Infrastrukturen in besonders wichtige und wichtige Unternehmen. Es sind grundsätzlich die Anbieter öffentlicher Kommunikationsnetze, Vertrauensdienste und Namensregister der obersten Domäne (inkl. DNS-Diensteanbieter) betroffen.
- Ebenso Sektoren mit hoher Kritikalität (Anhang I): Energie, Verkehr, Bank- und Finanzwesen, Gesundheitswesen, Wasserversorgung, Digitale Infrastruktur, ITK-Dienste, Öffentliche Verwaltung, Weltraum
- Sonstige kritische Sektoren (Anhang II): Post- und Kurierdienste, Abfallwirtschaft, Chemie, Ernährung, Herstellung von Waren, Digitale Dienste, Forschung
- Risikomanagement ist ein Grundpfeíler der NIS2-Umsetzung inkl. notwendigem ISMS , ISB und vor allem entsprechende Prozessen…..

Übersicht der Unternehmens-Zuordnung zu Wirtschafts-zweigen (Sektoren) Quelle: https://ec.europa.eu/eurostat/de

ISSN 1977-0383

eurostat
Methodologies and Working papers

NACE Rev. 2

Statistische Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft

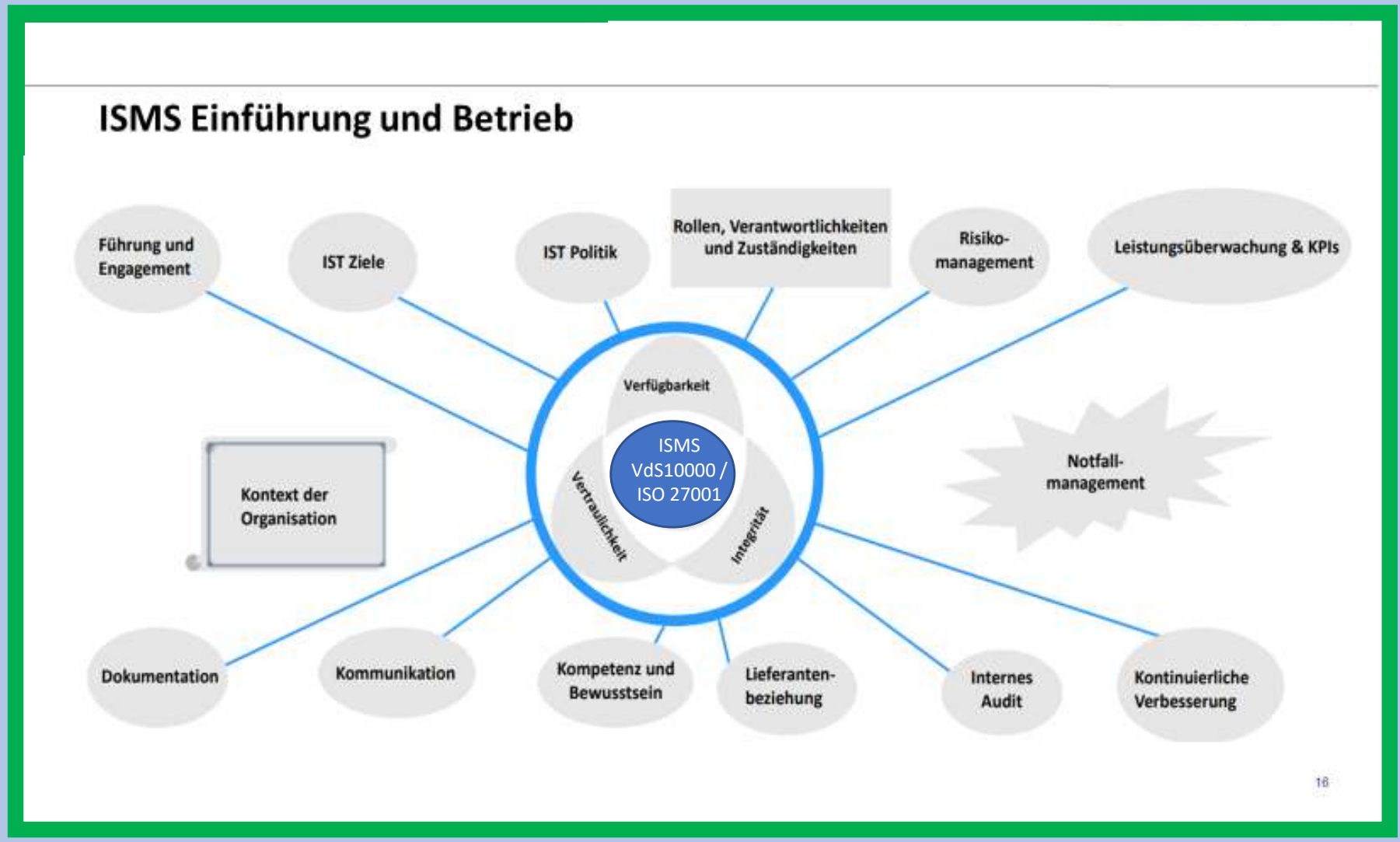
Grobe Struktur der NACE Rev. 2

Abschnitt	Überschrift
A	Land- und Forstwirtschaft, Fischerei
B	Bergbau und Gewinnung von Steinen und Erden
C	Verarbeitendes Gewerbe/Herstellung von Waren
D	Energieversorgung
E	Wasserversorgung; Abwasser- und Abfallentsorgung und Umweltverschmutzungen
F	Baugewerbe/Bau

	28.15	Herstellung von Lagern, Getrieben, Zahnrädern und Antriebselementen	2814
28.2		Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen	
	28.21	Herstellung von Öfen und Brennern	2815
	28.22	Herstellung von Hebezeugen und Fördermitteln	2816
	28.23	Herstellung von Büromaschinen (ohne Datenverarbeitungsgeräte und periphere Geräte)	2817
	28.24	Herstellung von handgeführten Werkzeugen mit Motorantrieb	2818
	28.25	Herstellung von kälte-und lufttechnischen Erzeugnissen, nicht für den Haushalt	2819*
	28.29	Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen a. n. g.	2819*
28.3		Herstellung von land-und forstwirtschaftlichen Maschinen	
	28.30	Herstellung von land-und forstwirtschaftlichen Maschinen	2821
28.4		Herstellung von Werkzeugmaschinen	
	28.41	Herstellung von Werkzeugmaschinen für die Metallbearbeitung	2822*

„NIS-2 (Mindest)Maßnahmen“

- Risikoanalyse, Bewertung und Behandlung
- Sicherheitsvorfälle bewältigen
- Sicherheit des Personals
- Verschlüsselte Übertragung
- Multi-Faktor Authentifizierung
- Backup, Recovery, Notfallplan

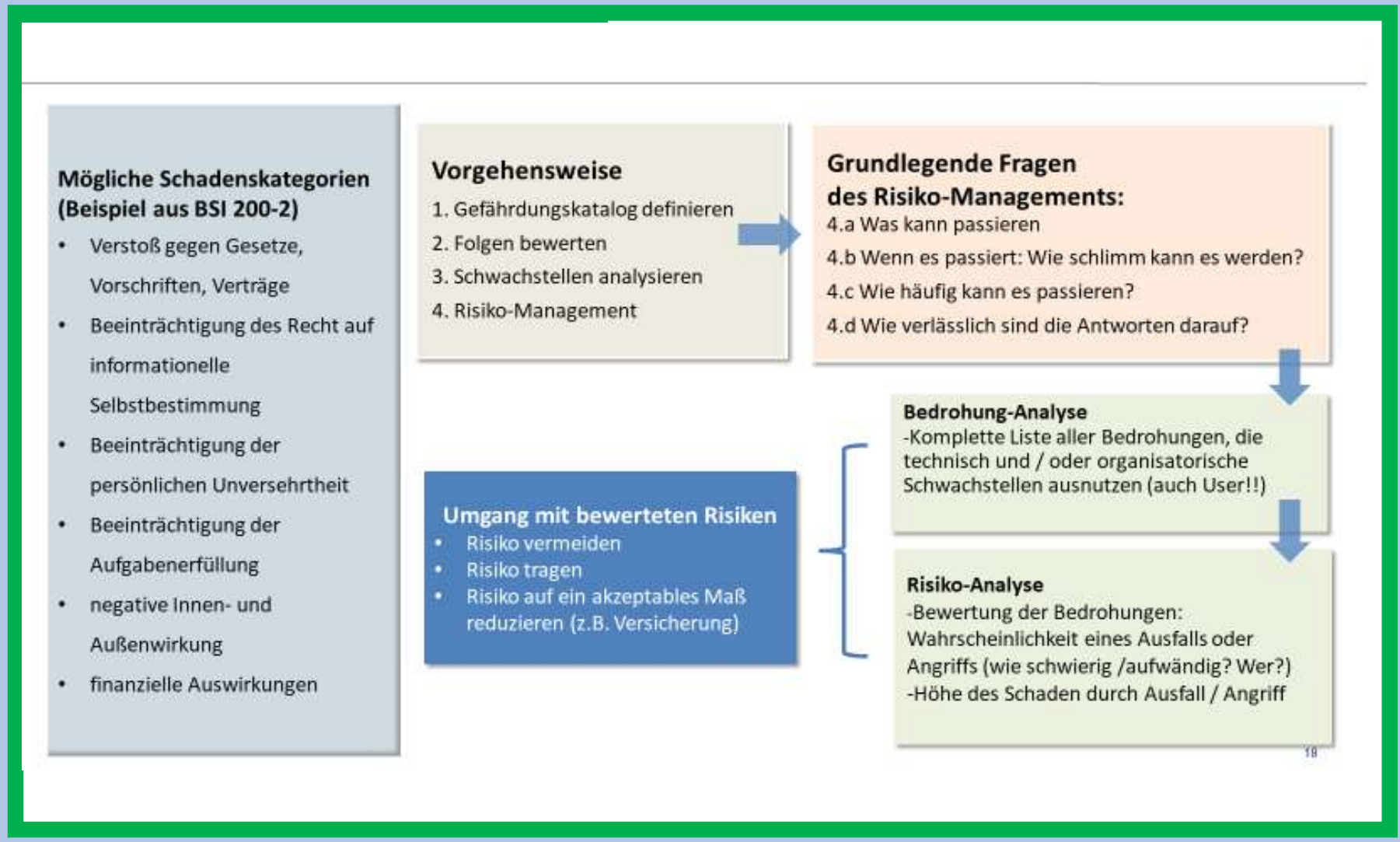

ISMS Einführung und Betrieb
Führung und Engagement
IST Ziele
IST Politik
Rollen, Verantwortlichkeiten und Zuständigkeiten
Risiko-management
Leistungsüberwachung & KPIs
Verfügbarkeit
ISMS VdS10000 / ISO 27001
Vertraulichkeit
Integrität
Kontext der Organisation
Notfall-management
Dokumentation
Kommunikation
Kompetenz und Bewusstsein
Lieferanten-beziehung
Internes Audit
Kontinuierliche Verbesserung
18

INFORMATIONSSICHERHEITS-MANAGEMENT-SYSTEM

Punkt	Reifegrad	Beschreibung	Anforderung	Erfordernis	Priorität	Verantwortlicher	Status	Aufgaben	Dokumente	Risiko
Kontext der Organisation										
4.1		Verstehen der Organisation und ihres Ko…	Die Organisation muss externe und intern…	MUSS	A	Goebes Martin	0/3	1	0	0
4.2		Verstehen der Erfordernisse und Erwartu…	Die Organisation muss:a) die interessiert…	MUSS	A	Goebes Martin	0/3	1	0	0
4.3		Festlegen des Anwendungsbereichs des …	Die Organisation muss die Grenzen und …	MUSS	A	Goebes Martin	0/3	1	0	0
4.4		Informationssicherheitsmanagementsystem	Die Organisation muss entsprechend den…	MUSS	A	Goebes Martin	0/3	1	0	0
Führung										
5.1		Führung und Verpflichtung	Die oberste Leitung muss in Bezug auf d…	MUSS			0/3	0	0	0
5.2		Politik	Die oberste Leitung muss eine Informatio…	MUSS			0/3	0	0	0
5.3		Rollen, Verantwortlichkeiten und Befugnis…	Die oberste Leitung muss sicherstellen, d…	MUSS			0/3	0	0	0
Planung										
6.1.1		Maßnahmen zum Umgang mit Risiken un…	Bei der Planung für das ISMS muss die O…	MUSS			0/3	0	0	0
6.1.2		Maßnahmen zum Umgang mit Risiken un…	Die Organisation muss einen Prozess zur…	MUSS			0/3	0	0	0
6.1.3		Maßnahmen zum Umgang mit Risiken un…	Die Organisation muss einen Prozess für …	MUSS			0/3	0	0	0
6.2		Informationssicherheitsziele und Planung…	Die Organisation muss Informationssiche…	MUSS			0/3	0	0	0

„NIS-2 (Mindest)Maßnahmen“

- Sicherheit in der Lieferkette
- Schutzmaßnahmen für Systeme, Prozesse, Daten
- Wirksamkeit der Maßnahmen , PDCA-Zyklus
- Sensibilisierung und Schulung der MA
- Richtlinie kryptografische Verfahren, Verwendungszweck


Mögliche Schadenskategorien (Beispiel aus BSI 200-2)
• Verstoß gegen Gesetze, Vorschriften, Verträge
• Beeinträchtigung des Recht auf informationelle Selbstbestimmung
• Beeinträchtigung der persönlichen Unversehrtheit
• Beeinträchtigung der Aufgabenerfüllung
• negative Innen- und Außenwirkung
• finanzielle Auswirkungen
Vorgehensweise
1. Gefährdungskatalog definieren
2. Folgen bewerten
3. Schwachstellen analysieren
4. Risiko-Management
Grundlegende Fragen des Risiko-Managements:
4.a Was kann passieren
4.b Wenn es passiert: Wie schlimm kann es werden?
4.c Wie häufig kann es passieren?
4.d Wie verlässlich sind die Antworten darauf?
Bedrohung-Analyse
-Komplette Liste aller Bedrohungen, die technisch und / oder organisatorische Schwachstellen ausnutzen (auch User!!)
Risiko-Analyse
-Bewertung der Bedrohungen: Wahrscheinlichkeit eines Ausfalls oder Angriffs (wie schwierig /aufwändig? Wer?)
-Höhe des Schaden durch Ausfall / Angriff
Umgang mit bewerteten Risiken
• Risiko vermeiden
• Risiko tragen
• Risiko auf ein akzeptables Maß reduzieren (z.B. Versicherung)
19

Gemäß Art. 20 können das Management zur Verantwortung gezogen werden, wenn betroffene Unternehmen gegen die Anforderungen von Artikel 21 verstoßen.
Der derzeitige Referentenentwurf (NIS2UmsuCG) sieht darüber hinaus sogar vor, dass Management-Organe (insbesondere bei fahrlässigen Verfehlungen) mit ihrem privaten Vermögen für solche Verstöße haften müssen.

Die Sanktionen der NIS2-Richtlinie sehen vor, dass die Mitgliedstaaten die maximalen Geldbußen nur bis zu einer bestimmten Höhe begrenzen dürfen. Bei wesentlichen Einrichtungen müssen die maximalen Geldbußen bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Umsatzes betragen – je nachdem, welcher Betrag höher ist.
Bei wichtigen Einrichtungen liegt die minimale Obergrenze bei 7 Millionen Euro oder 1,4 Prozent des weltweiten Umsatzes.
Auch für diese Bußgelder müssen die Managementorgane mit ihren privaten Vermögen haften, soweit der Referentenentwurf in seiner jetzigen Fassung umgesetzt wird.

Datenschutz
IT-Sicherheit