

IT-Sicherheitsrechtstag 2026

Berlin, 24.09.2026

Geschäftsleitungsschulungen nach NIS-2/BSIG

Dr. Judith Nink, BSI

Agenda

- **01. Die Basics:**
 - Pflichten
 - rechtliche Grundlagen
- **02. Die Schulungspflicht im Detail**
- **03. Die gesellschaftsrechtliche Komponente**
- **04. Die wirtschaftliche Komponente**
- **05. Unterstützung des BSI**
- **06. Let`s Talk: Q&A**

01. Die Basics

Pflichten nach dem BSIG (NIS-2)

Was ist zu tun?

Pflichten für Einrichtungen, § 30 ff. BSIG

Risikomanagement

Meldepflicht

Registrierungspflicht

Pflichten für die Geschäftsleitung, § 38 BSIG

Umsetzung /
Überwachung



Schulungspflicht

Dokumentieren

Schulungspflicht für Geschäftsleitungen

Warum gibt es die Schulungspflicht?

„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“, § 38 Abs. 3 BSIG



§ 38 Abs. 1 BSIG

Verpflichtung Risikomanagementmaßnahmen umzusetzen und zu überwachen



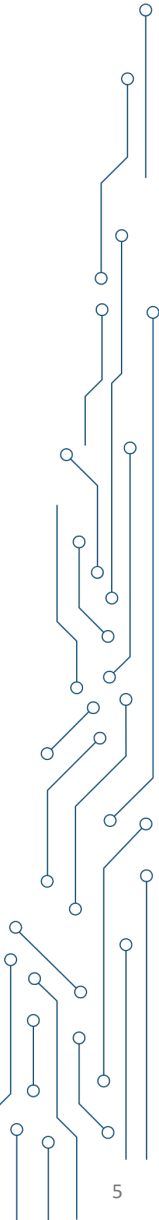
§ 38 Abs. 2 BSIG

Gesellschaftsrechtliche Binnenhaftung



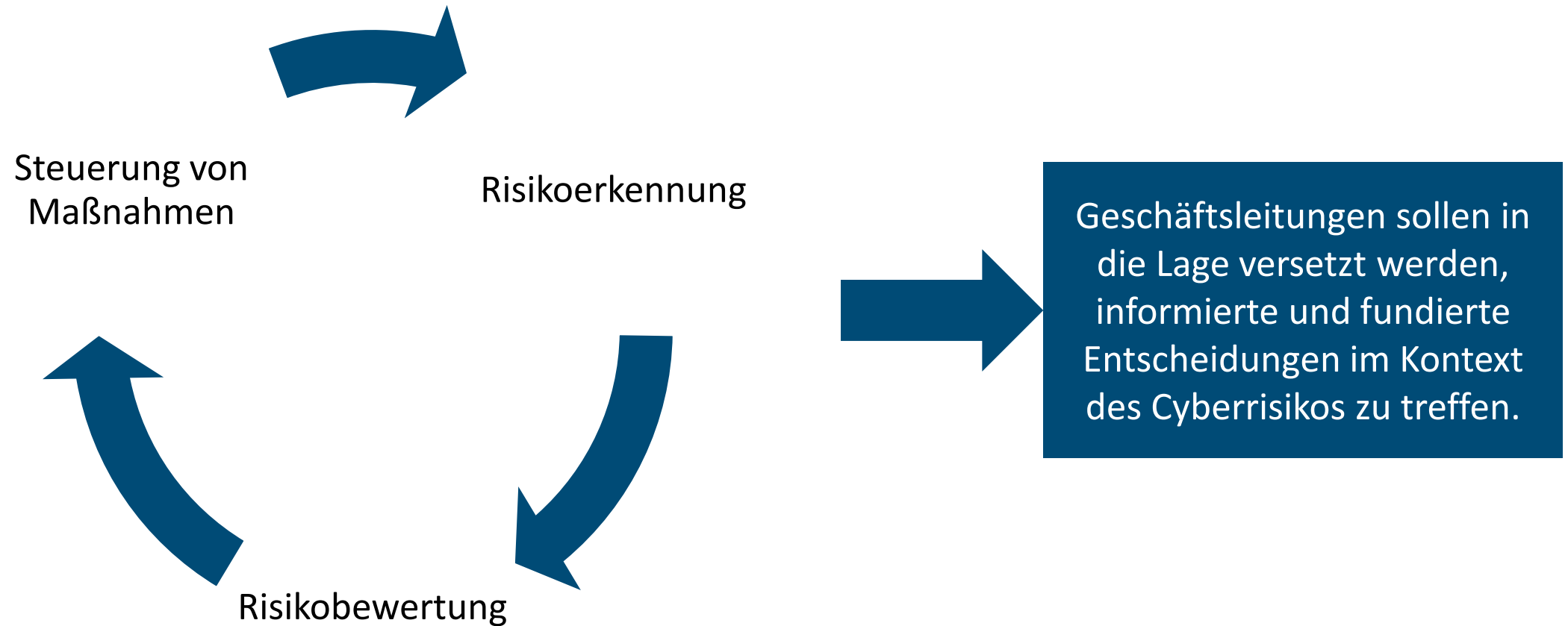
§ 38 Abs. 3 BSIG

Schulungspflicht für Geschäftsleitungen



Schulungspflicht für Geschäftsleitungen

Ziele des § 38 Abs. 1 BSIG



02. Die Schulungspflicht im Detail

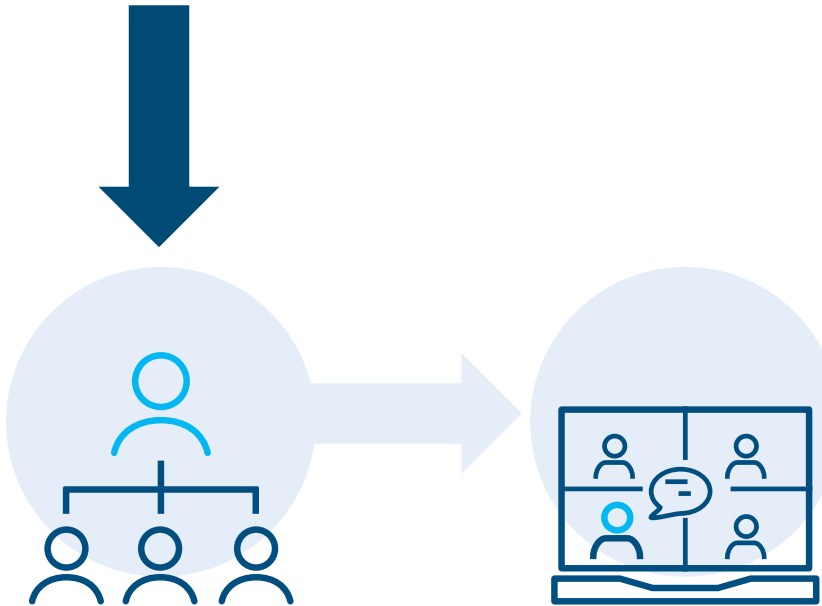
Wer muss sich schulen lassen?

Nicht nur Geschäftsführer und Geschäftsführerinnen

*„Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur **Führung der Geschäfte** und **zur Vertretung** einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung nach § 29 gelten nicht als Geschäftsleitung“, § 2 Abs. 13 BSIG.*

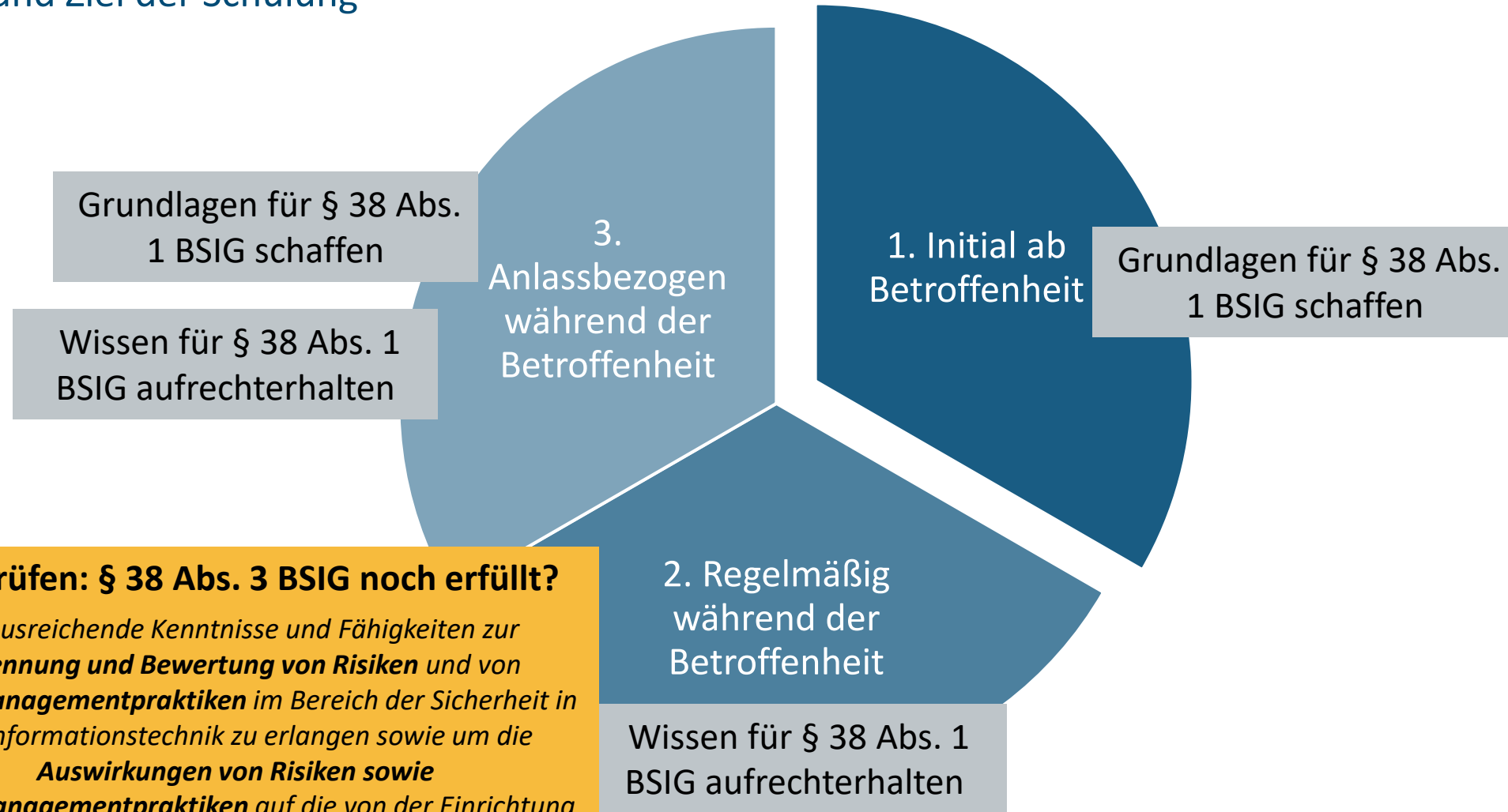
Das können bspw. folgende Rollen sein:

- Geschäftsführer / Geschäftsführerin, § 35 GmbHG, § 78 Abs. 1 AktG
- Vorstand / Vorständin
- Mitglied des Vorstands
- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Chief Operating Officer (COO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Komplementär / Komplementärin
- geschäftsführender Gesellschafter / geschäftsführende Gesellschafterin
- Prokurist, § 49 HGB
- ...



Häufigkeit / Intervall von Schulungen

Auslöser und Ziel der Schulung

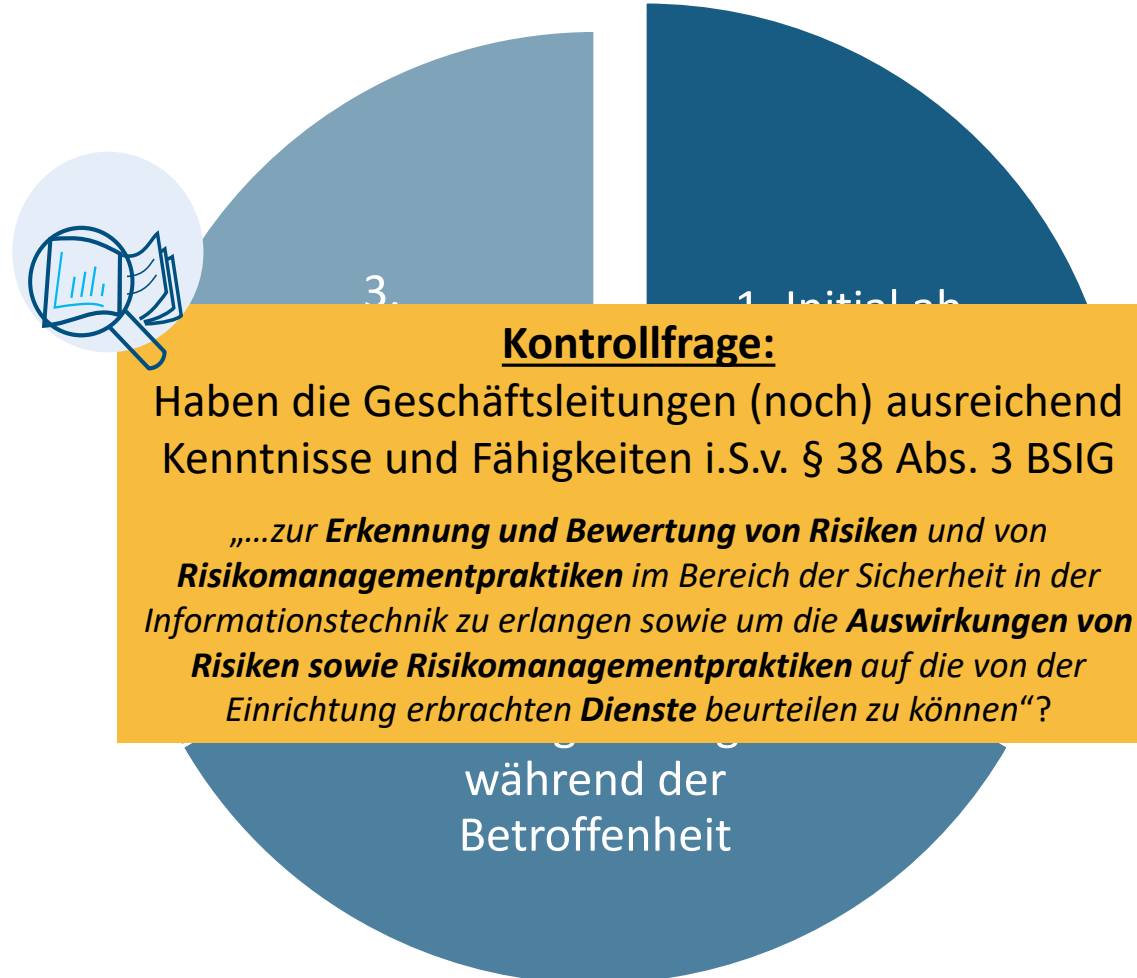


Prüfen: § 38 Abs. 3 BSIG noch erfüllt?

„...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.“

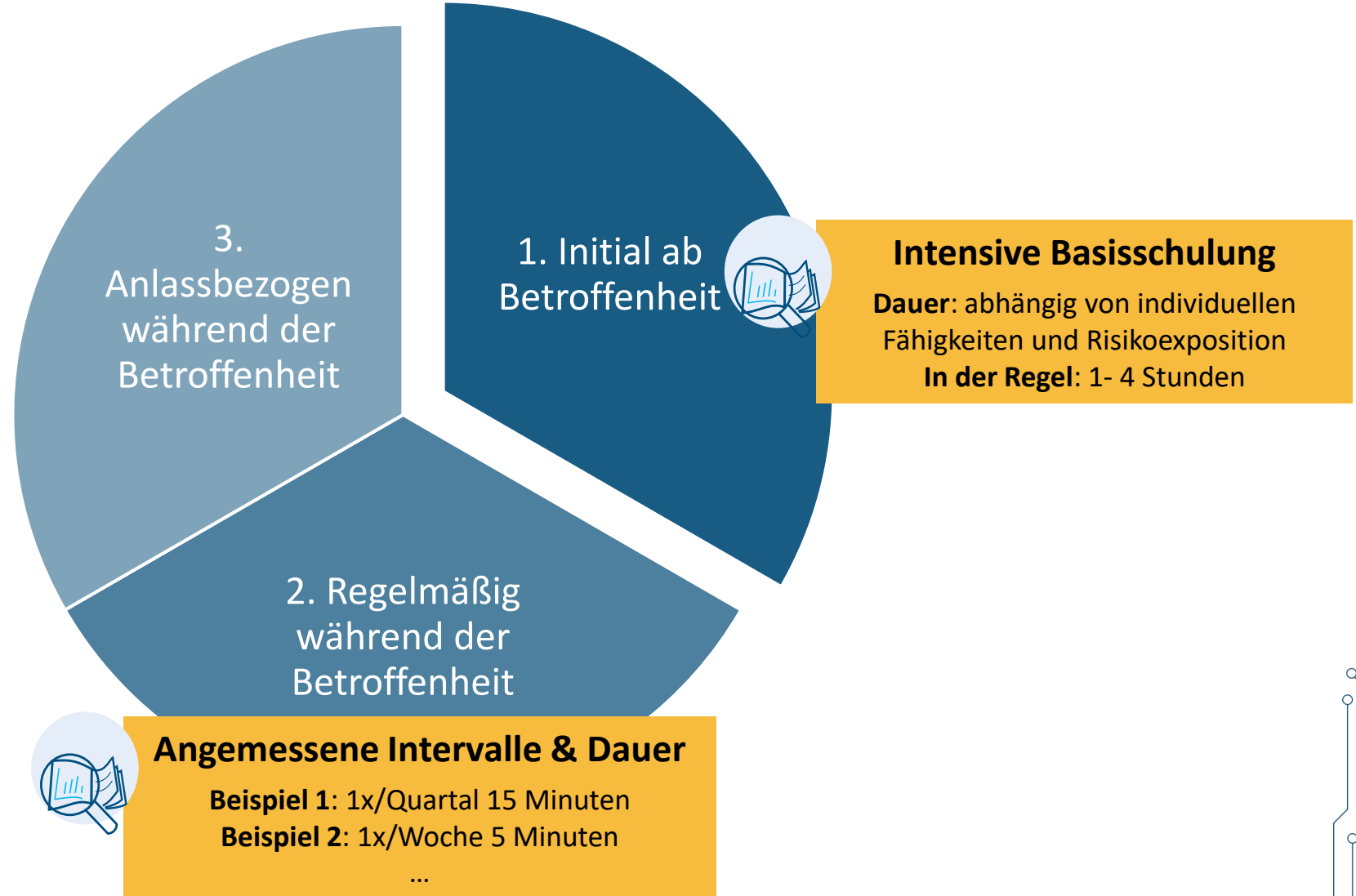
Dauer von initialen und regelmäßigen Schulungen

There is no one-size fits all!



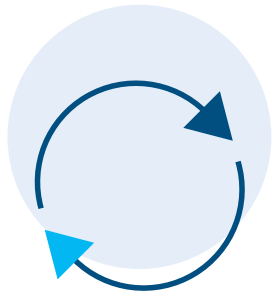
Dauer von initialen und regelmäßigen Schulungen

There is no one-size fits all!

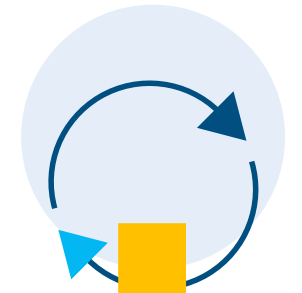


Häufigkeit / Intervall von Schulungen

Gründe für anlassbezogene Schulungen (Beispiele)



- Wechsel in der Geschäftsleitung
- Signifikante Änderungen in den Geschäftsprozessen
- Signifikante Änderungen der Risikoexposition
- Signifikante Änderungen der Bedrohungslage
- Signifikante Änderungen bei implementierten oder geplanten Risikomanagementmaßnahmen



Ad hoc!



Anlassgerecht!
Wenige Minuten
bis ...

Inhalte der Schulungen

Welche Kenntnisse sollten Schulungen an Geschäftsleitungen vermitteln

Kerninhalte

- Risikoanalyse
- Risikomanagementmaßnahmen
- Auswirkungen Risiken und Risikomanagementmaßnahmen

Unterstützende Inhalte

- Kontext der NIS-2-Regulierung
- Pflichten für Einrichtungen/GL übergreifend
- Sektor- und einrichtungsspezifische Inhalte
- Szenarien/Übungen/Fallstudien

Systematik von SOLL bzw. KANN-Empfehlungen

SOLL/SOLLEN:

- ✓ **zentrale Kenntnisse** werden **dringend** empfohlen.

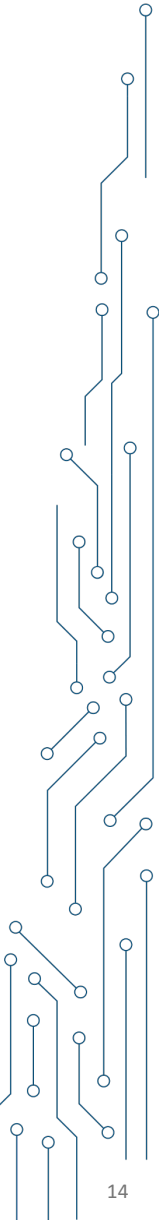
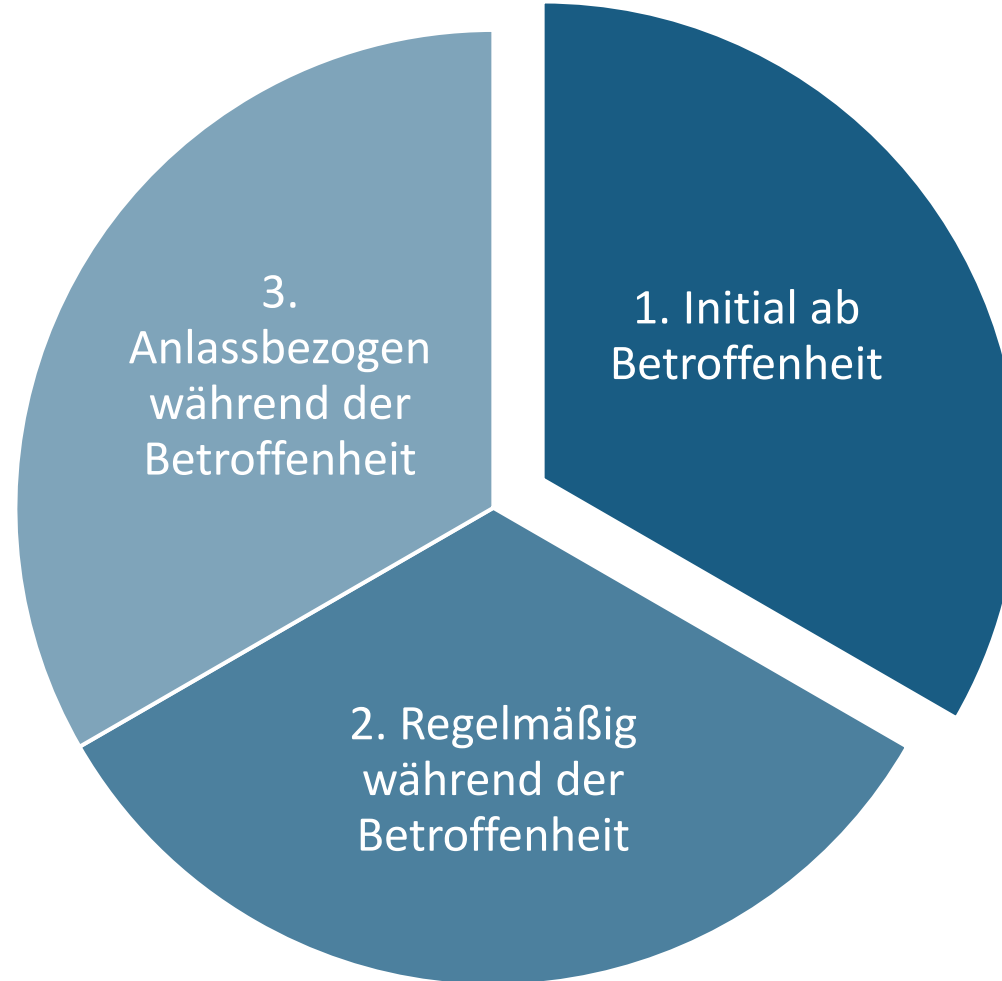
KANN/KÖNNEN:

- ✓ **ergänzende Kenntnisse** werden **fakultativ** empfohlen

Empfehlungen sind abstrakt und müssen durch Schulungsanbieter je Einrichtung und beschulter Zielgruppe in konkrete Schulungsinhalte übersetzt werden.

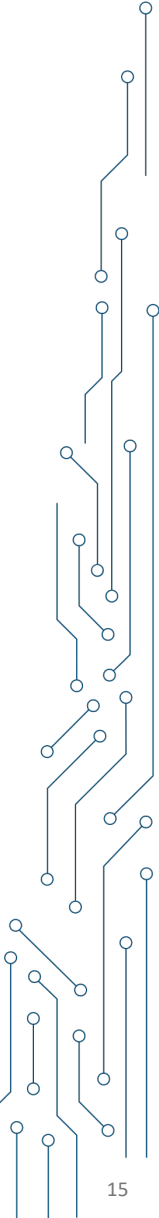
Formate von Schulungen

There is no one-size fits all!



Formate von Schulungen

There is no one-size fits all!



Formate von Schulungen

Beispiele



KI-generiert.

Externe vs. interne Anbieter von Schulungen

Wer kann/soll Schulungen anbieten können?

Internes Personal

- IT-Sicherheits- bzw. IT Verantwortliche im Unternehmen

Dienstleister

- Externe Bestands-IT-Sicherheitsdienstleister
- Beratung und ggf. Betrieb von IT(-Sicherheit)-Systemen

Schulungsanbieter

- Anbieter von IT-Sicherheitsschulungen
- Dezierte NIS-2-GL-Schulungen



Kennt
internen
Aufbau

Kapazität,
fehlende
Erfahrung bei
Schulungen



Kennt internen
Aufbau

Ggf. Interessen-
konflikte,
fehlende
Erfahrung bei
Schulungen



Erfahrung

Interner
Aufbau bei
Einrichtungen
unbekannt

03. Die gesellschaftsrechtliche Komponente

Verantwortlichkeit der Geschäftsleitung

§ 38 Abs. 2 BSIG i.V.m. § 93 Abs. 1, 2 S. 1 AktG / § 43 Abs. 1, 2 GmbHG

KI-generiert



Legalitätspflicht und Risikomanagement

Rechtliche Pflichten – persönliche Haftung der Geschäftsleitung – Bedeutung von Risikomanagement

Gesetzliche Grundlage



Pflicht zur Einrichtung eines **Risikomanagements** zur Vermeidung von Rechtsverstößen.

i Aus § 93 AktG und § 43 GmbHG.

Business Judgement Rule



Business Judgement Rule
(§ 93 Abs. 1 S. 2 AktG)



Keine Entlastung bei Legalitätspflicht

Die Abwägung, ob Maßnahmen zu teuer sind, ist **ausgeschlossen**. **Gesetzliche Pflichten** müssen eingehalten werden.

Haftung der Geschäftsleitung



- ✓ Pflichtverletzung (schuldhaft)
- ✓ Schaden der Einrichtung
- ✓ adäquate Kausalität

✓ Nur bei **organspezifischen Pflichten**.

Beispiel: Bußgeld



z. B. bei unzureichend umgesetzten Risikomanagementmaßnahmen (§ 65 Abs. 2 Nr. 2 BSIG).



Persönliche Haftung der Geschäftsleitung, wenn schuldhaft.

Voraussetzungen nach § 38 Abs. 2 BSIG

- 1 Umsetzungs- und/oder Überwachungspflichten
- 2 schuldhaft verletzt
- 3 Schaden der Einrichtung
- 4 adäquate Kausalität



Gilt nur für § 38 Abs. 1 BSIG (nicht für Fortbildungspflichten).

Fazit



Ohne Risikomanagement **keine Entscheidungsgrundlage** – mit **persönlicher Haftung** bei Pflichtverletzungen.



Rechtskonform handeln



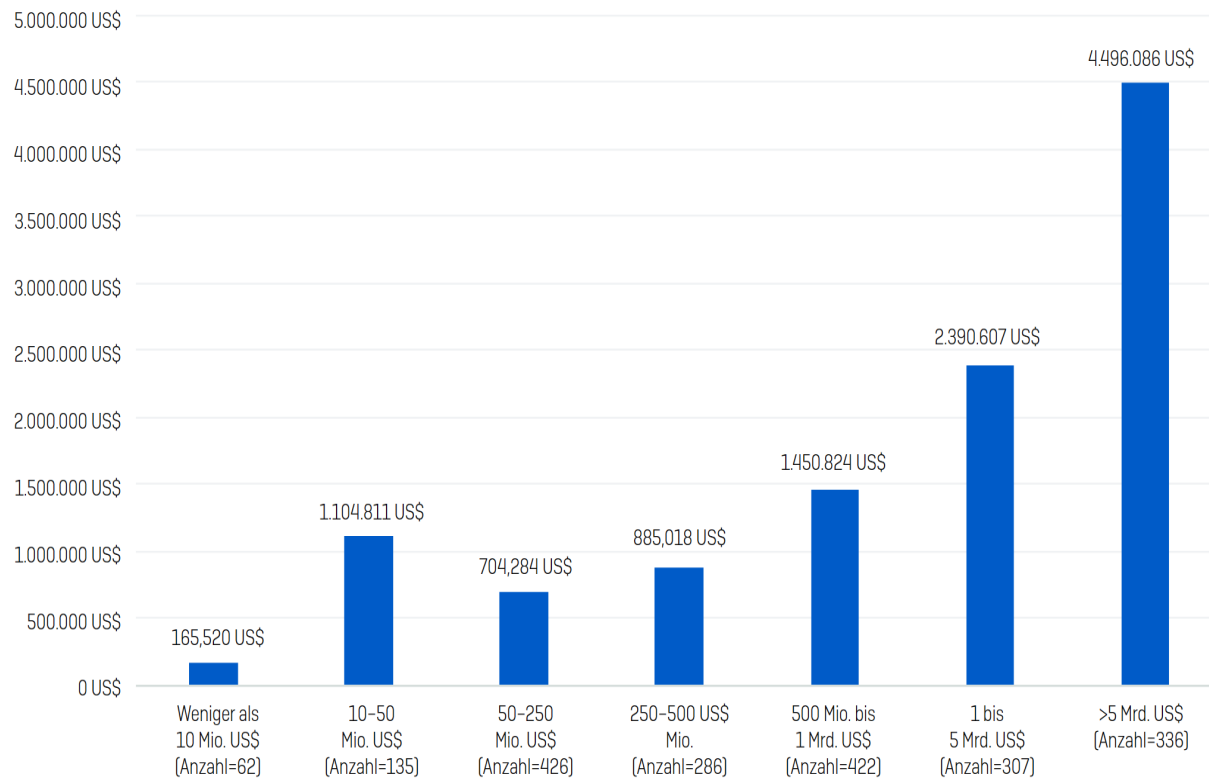
Risiken erkennen und steuern



Persönliche Verantwortung

04. Die wirtschaftliche Komponente

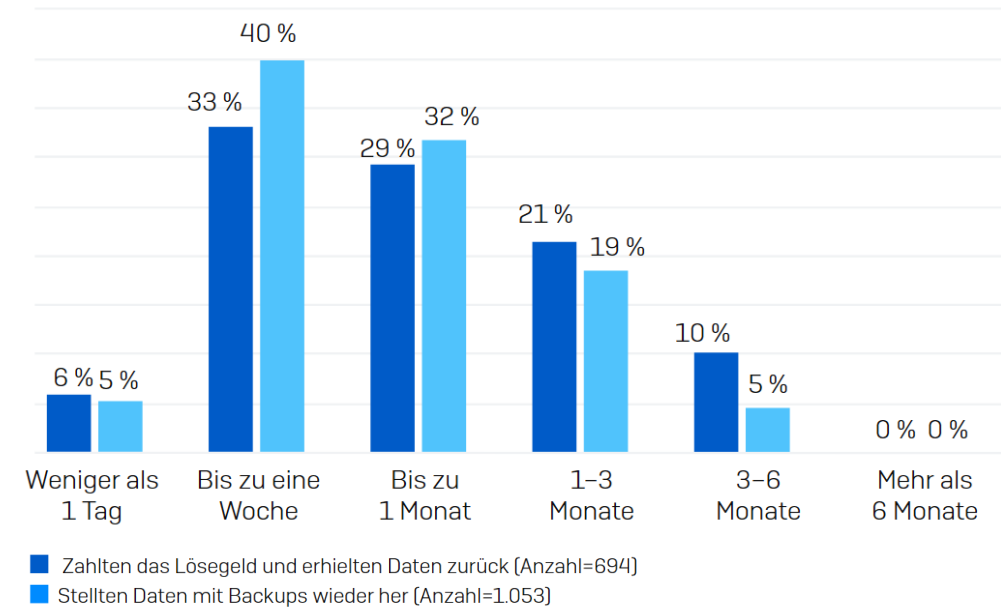
Cybersicherheit rechnet sich! Beispiel Ransomware



Durchschn. Bereinigungskosten nach Umsatz

Zahlen das Lösegeld und erhielten Daten zurück	Stellen Daten mit Backups wieder her
750.000 US\$ Mittelwert	375.000 US\$ Mittelwert
2,6 Mio. US\$ Durchschnitt	1,62 Mio. US\$ Durchschnitt

Wiederherstellungskosten nach Methode



Ausfallzeiten nach Methode der Datenwiederherstellung

Cybersicherheit ist Chefinnen- und Chefsache!



05. Unterstützung des BSI

Geschäftsleitungsschulung gemäß BSIG

Konkrete Hilfestellungen



1. BSI, **Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen**, abrufbar unter: <https://www.bsi.bund.de/dok/nis-2-schulung-geschaeftsleitung>
2. *In Arbeit*: ACS Mitgliedsunternehmen, **Guideline Schulungen & Checkliste Schulungsinhalte**
3. BSI, **NIS-2-regulierte Unternehmen**: Infomaterialien, Checklisten, Empfehlungen, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html

Leitfragen für Geschäftsleitungen

Wie können Geschäftsleitungen das Wissen anwenden und ihren Verantwortungen nachkommen?



Leitfrage

Warum diese Frage wichtig ist

Hilfreiche Antwort

Antwort, die weitere
Nachfragen erfordert

Link: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/NACD/toolkit_management_cyber_risiken_de.html

06. Let's Talk: Q&A

Vielen Dank für Ihre Aufmerksamkeit

Dr. Judith Nink

Fachbereichsleiterin Cybersicherheit bei Unternehmen

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 87

53175 Bonn

www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

