

Übersicht

# NIS-2 Anforderungen mit gezielter Weiterbildung umsetzen.

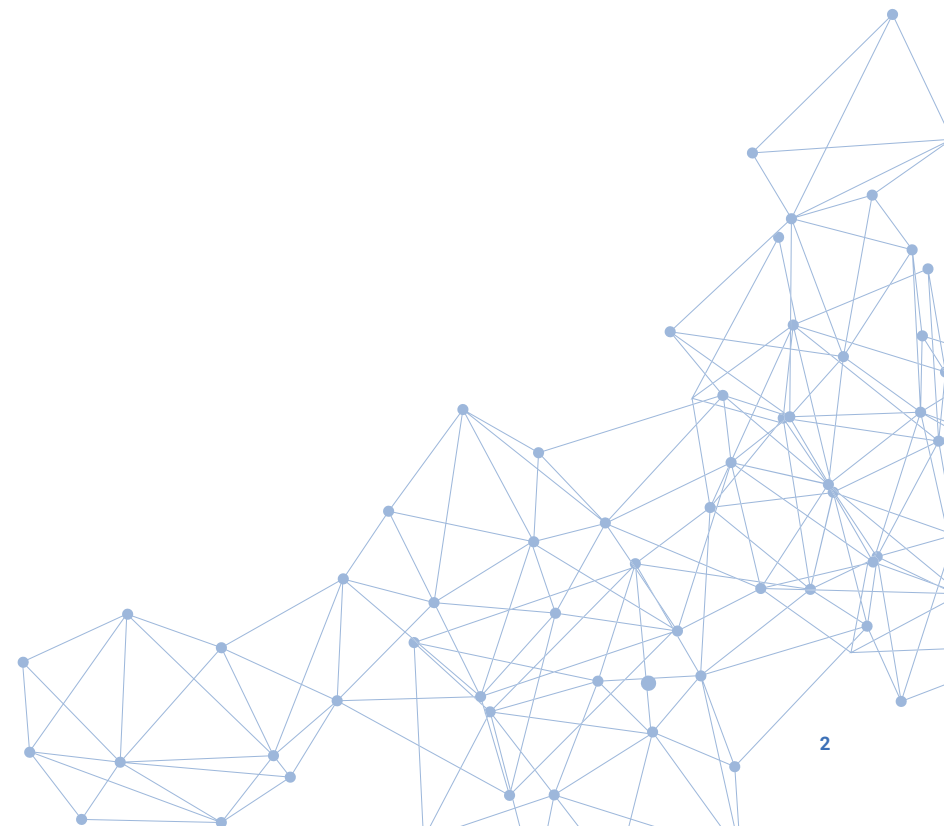
Kompetenz als zentraler Erfolgsfaktor  
für Ihre Compliance

# Einleitung

Mit der Umsetzung der europäischen NIS-2-Richtlinie in deutsches Recht verpflichtet das novellierte BSIG besonders wichtige und wichtige Einrichtungen zu einem strukturierten, dokumentierten und überprüfbaren Cyber-Risikomanagement.

- **§ 30 BSIG definiert einen verbindlichen Maßnahmenrahmen.**
- **§ 38 BSIG verankert die Verantwortung auf Leitungsebene.**

Die Wirksamkeit dieses Systems hängt maßgeblich von klar definierten Rollen und ausreichender Fachkompetenz ab. Gezielte Weiterbildung kann dazu beitragen, organisatorische Kompetenzlücken zu schließen und die gesetzlich geforderte Angemessenheit strukturiert umzusetzen.



# Mit diesen Schulungen werden Sie NIS-2-konform.

## § 38 BSIG macht deutlich:

Die Geschäftsleitung ist für Umsetzung und Überwachung der Maßnahmen verantwortlich und muss regelmäßig geschult werden.

→ **Schulung der Geschäftsleitung nach §38 NIS-2**

## Mehrere Maßnahmenfelder des § 30 Abs. 2 BSIG:

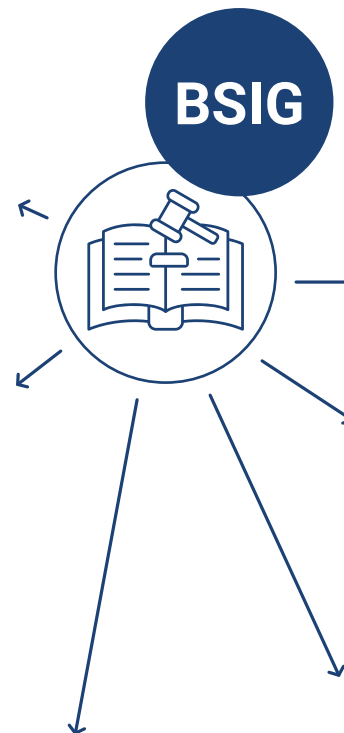
adressieren unmittelbar technische & organisatorische Sicherheitsanforderungen und erstrecken sich über ein breites Themenfeld.

- **Windows Server Hardening**
- **Active Directory Tiering**
- **Netzwerksicherheit**
- **Cloud Security**
- **Einführung in die Kryptographie**
- **Crypto Security Professional (TÜV)**
- **Post-Quanten-Kryptographie**
- **OWASP Security Champion**
- **T.I.S.P. – TeleTrust Information Security Professional**

## § 30 Abs. 2 Nr. 7:

verpflichtet ausdrücklich zu Cyberhygiene und Schulungen.

- **Cybersecurity-Awareness-Beauftragter (TÜV)**
- **Social Engineering**
- **IT Security Training: Angriff, Verteidigung & NIS-2 Compliance**



## § 30 Abs. 2 Nr.1:

Einführung eines wirksamen und angemessenen Risikomanagements für Informationssicherheit.

- **ISMS Foundation nach ISO/IEC 27001 (TÜV)**
- **ISMS Implementer nach ISO/IEC 27001 (TÜV)**
- **IT-Risikomanager:in nach ISO/IEC 27005 (TÜV)**
- **IT-Grundschutz-Praktiker**
- **IRCA ISMS ISO/IEC 27001:2022 Lead Auditor**

## § 30 Abs. 2 Nr. 2:

Bewältigung von Sicherheitsvorfällen.

- **Cyber Incident – First Response**
- **Cyber Threat Intelligence Training**
- **IT-Forensik – Grundlagen & Praxis**

## 30 Abs. 2 Nr. 3:

Sicherstellung der Aufrechterhaltung des Betriebs, einschließlich Backup-Management, Wiederherstellung nach Notfällen sowie Krisenmanagement.

- **BSI BCM-Praktiker**
- **Business Continuity Manager (TÜV)**
- **Build-your-BCM**
- **Backups – Professionelle Datensicherung**

# 1. Vom Maßnahmenkatalog zum Steuerungssystem

**§ 30 Abs. 2 Nr.1 verpflichtet Unternehmen zur Einführung eines wirksamen und angemessenen Risikomanagements für Informationssicherheit.**

Das Gesetz schreibt kein bestimmtes Zertifizierungsmodell vor. In der wirtschaftlichen Praxis haben sich jedoch strukturierte Managementansätze wie ISO/IEC 27001 oder BSI IT-Grundschutz als geeignete Umsetzungsrahmen etabliert. Beide Ansätze verfolgen das Ziel eines systematischen Informationssicherheitsmanagements, unterscheiden sich jedoch in Methodik und Struktur.

Maßgeblich entscheidend ist die strukturierte Fähigkeit eines Unternehmens:

- **Risiken systematisch zu identifizieren**
- **Maßnahmen risikobasiert abzuleiten**
- **Entscheidungen nachvollziehbar zu dokumentieren**
- **Wirksamkeit regelmäßig zu überprüfen**



## Hier setzen folgende Qualifizierungen an:

**ISMS Foundation nach ISO/IEC 27001 (TÜV)**

→ vermittelt die Systemlogik eines Informationssicherheitsmanagement-systems und eignet sich besonders als strukturierter Einstieg.

**ISMS Implementer nach ISO/IEC 27001 (TÜV)**

→ befähigt zur operativen Einführung und Steuerung.

**IT-Risikomanager:in nach ISO/IEC 27005 (TÜV)**

→ vertieft die Risikoanalyse im Kontext der ISO 27001.

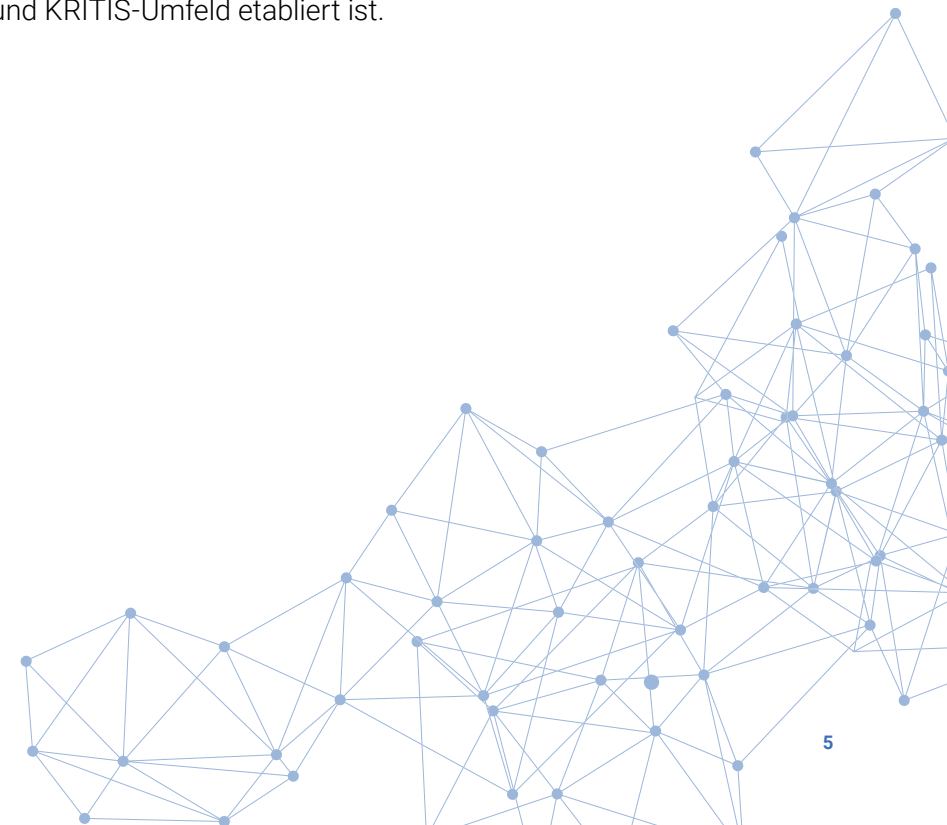
**IT-Grundschutz-Praktiker**

→ bietet eine national etablierte Umsetzungslogik, die besonders im deutschen Behörden- und KRITIS-Umfeld etabliert ist.

Dazu ergänzend werden in Abs. 7 „Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen“ gefordert. Diese Anforderungen lassen sich etwa im Rahmen interner Audits oder Management-Reviews operationalisieren. Dazu passend kann man in der Schulung

**IRCA ISMS ISO/IEC 27001:2022 Lead Auditor**

die Durchführung von internen und externen Audits erlernen.

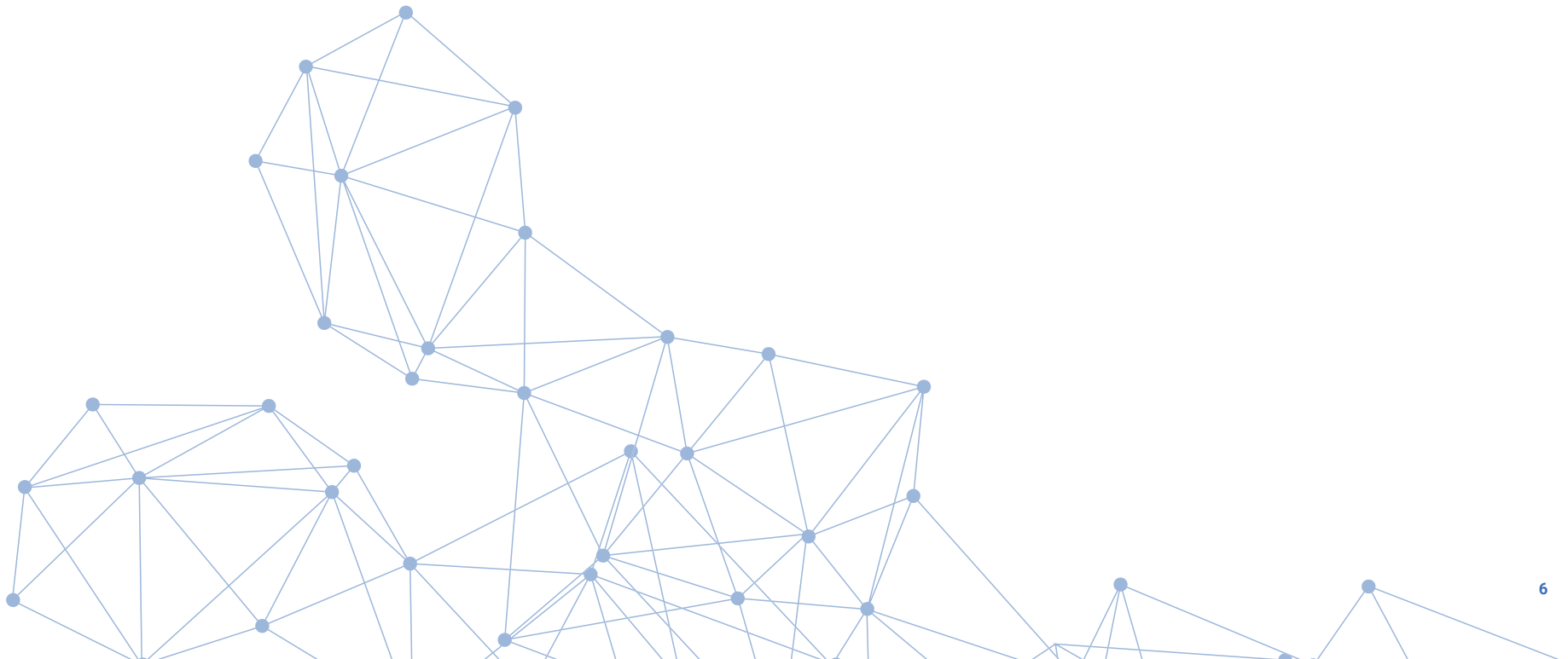


## 2. Incident Handling und Meldewege

**§ 30 Abs. 2 Nr. 2 fordert die Bewältigung von Sicherheitsvorfällen.**

**Die konkreten Meldepflichten ergeben sich aus § 32 BSIG.**

Ein funktionierendes Incident-Management erfordert somit klare Entscheidungslogiken und trainierte Eskalationswege. Schulungen können dazu beitragen, die tatsächliche organisatorische Befähigung zur sachgerechten Vorfallbewältigung zu verbessern.



## Passende Schulungen für die Bewältigung von Sicherheitsvorfällen:

### Cyber Incident – First Response

→ vermittelt strukturierte Erstreaktion und betriebliche Modelle der Incidentbewältigung.

### Cyber Threat Intelligence Training

→ unterstützt die Bewertung der Bedrohungslage.

### IT-Forensik – Grundlagen und Praxis

→ trainiert die forensische Analyse und Dokumentation.

Ergänzend spielt Kommunikation eine zentrale Rolle:

### Krisenkommunikation bei Cyberangriffen

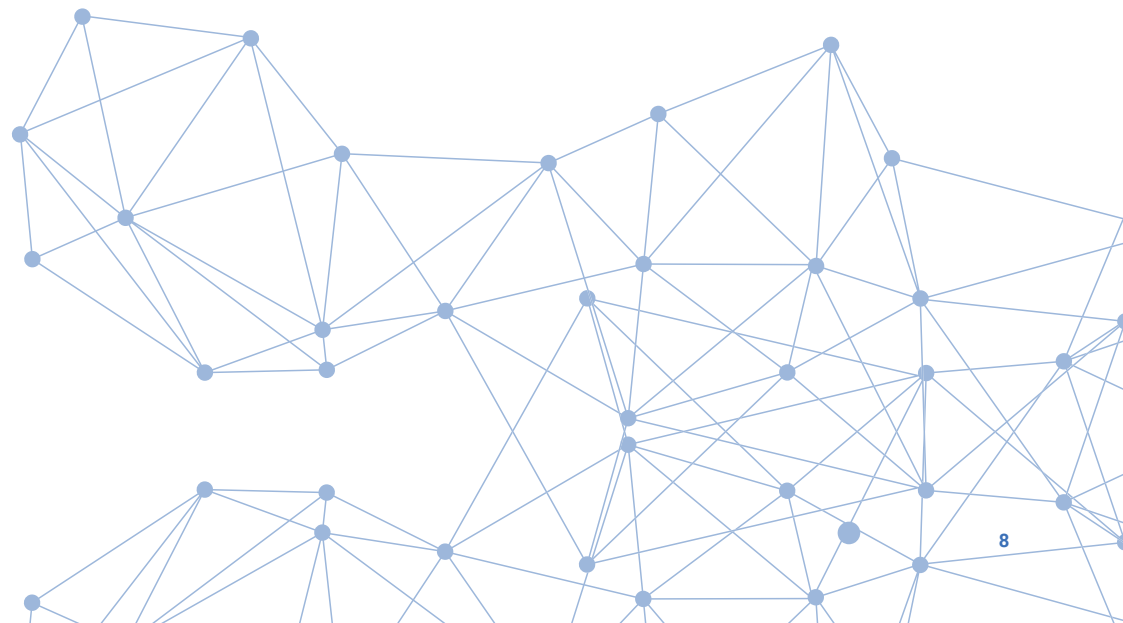
strukturiert interne und externe Informationsflüsse. Denn technische Eindämmung allein genügt nicht: Reputation, Stakeholdervertrauen und regulatorische Transparenz sind integraler Bestandteil professioneller Incident-Bewältigung.



# 3. Resilienz und Business Continuity

**§ 30 Abs. 2 Nr. 3 BSIG verpflichtet besonders wichtige und wichtige Einrichtungen zur Sicherstellung der Aufrechterhaltung des Betriebs, einschließlich Backup-Management, Wiederherstellung nach Notfällen sowie Krisenmanagement.**

Für die strukturierte Umsetzung haben sich insbesondere zwei Rahmenwerke etabliert: **die ISO 22301 als internationaler Standard für Business Continuity Management sowie der BSI-Standard 200-4**, der BCM eng mit dem IT-Grundschutz verzahnt und im behördlichen Umfeld weit verbreitet ist. **Ergänzend bietet die ISO/IEC 27031 Leitlinien zur Sicherstellung der Verfügbarkeit von Informations- und Kommunikationstechnologien** und konkretisiert damit insbesondere die IT-seitige Wiederherstellungs- und Kontinuitätsplanung im Rahmen eines ganzheitlichen BCM-Ansatzes.



## Passende Schulungen zum Aufbau von Cyber-Resilienz:

### BSI BCM-Praktiker

→ orientiert sich am BSI-Standard 200-4 und vermittelt die strukturierte Einführung eines BCM-Systems im Kontext des IT-Grundschutzes.

### Business Continuity Manager (TÜV)

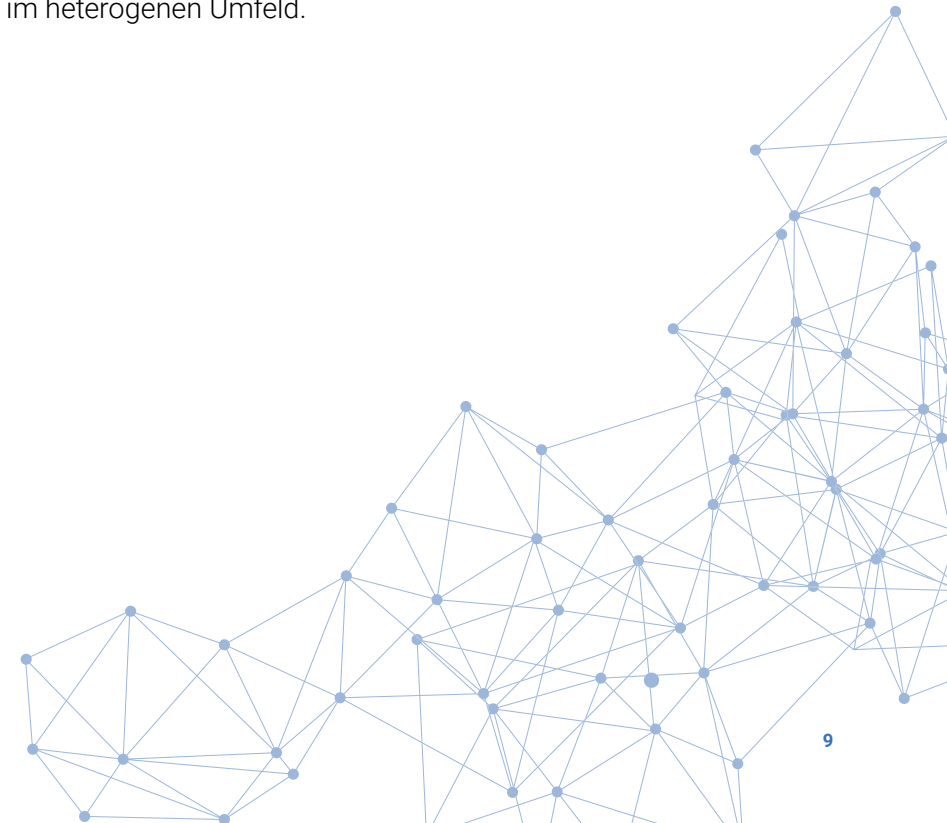
→ integrieren BCM strategisch in Managementprozesse. Die Schulung bietet einen ganzheitlicheren Blick auf das Themenfeld (ISO 22301, ISO 27031 & BSI 200-4).

### „Build-your-BCM“: Tabletop Übung

→ nutzt Gamification-Ansätze und trainiert die Entscheidungsfähigkeit unter Realbedingungen.

### Backups – Professionelle Datensicherung

→ adressiert herstellerunabhängig die technische Grundlage der Wiederherstellungsfähigkeit im heterogenen Umfeld.



# 4. Technische & organisatorische Mindestmaßnahmen

Mehrere Maßnahmenfelder des **§ 30 Abs. 2 BSIG** adressieren unmittelbar **technische & organisatorische Sicherheitsanforderungen** und erstrecken sich über ein breites Themenfeld.

Diese Maßnahmen sind nicht als isolierte Einzelvorgaben zu verstehen, sondern als integraler Bestandteil eines risikobasierten Sicherheitskonzepts. Gefordert werden unter anderem:

- **Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen**
- **Lieferkettensicherheit**
- **Kryptografie**
- **Zugriffskontrolle**
- **Multi-Faktor-Authentifizierung**
- **gesicherte Kommunikation**

## Fachliche Vertiefungen können beispielsweise erfolgen in den Bereichen...

### ...Administration

#### Windows Server Hardening

→ technisches Konfigurationsmanagement („Systemhärtung“) von Windows-Server Umgebungen

#### Active Directory Tiering

→ vermittelt die strukturierte Trennung administrativer Ebenen gemäß dem bewährten Tier-Modell.

#### Netzwerksicherheit

→ vermittelt umfassende Grundkenntnisse zu aktuellen Netzwerktechnologien und deren Absicherung.

#### Cloud Security Associate (TÜV)

→ behandelt neben Governance zentrale Sicherheitsmaßnahmen wie Identitäts- und Zugriffsmanagement von Cloud-Diensten.

### ...Kryptographie

#### Einführung in die Kryptographie

→ Grundlagen sicherer Verschlüsselung

#### Crypto Security Professional (TÜV)

→ vermittelt ein ganzheitliches Verständnis moderner kryptografischer Verfahren

### ...Software-Entwicklung

#### OWASP Security Champion

→ vermittelt wie Sicherheitsanforderungen von Beginn an in den Software-Entwicklungsprozess integriert werden können

#### T.I.S.P. – TeleTrusT Information Security Professional

→ vermittelt darüber hinaus ein umfassendes, interdisziplinäres Verständnis technischer und organisatorischer Informationssicherheit.



# 5. Awareness – Der menschliche Faktor als Risikodimension

§ 30 Abs. 2 Nr. 7 verpflichtet ausdrücklich zu Cyberhygiene und Schulungen.

Damit erkennt der Gesetzgeber an, dass menschliches Verhalten eine zentrale Risikokomponente darstellt.

## Passende Schulungen:

Cybersecurity-Awareness-Beauftragte:r (TÜV)

Social Engineering und Phishing Awareness Training

IT-Security Training:  
Angriff, Verteidigung & NIS-2 Compliance

- befähigt zur strukturierten Gestaltung von Awareness-Programmen.
- reduzieren operative Risiken durch das Trainieren der häufigsten „Einfalllöcher“.
- vermittelt für ein fachfremdes Publikum umfassende Bewertungskompetenzen für defensive & offensive Strategien der Cybersicherheit.

# 6. Geschäftsleitung und Governance

**§ 38 BSIG** macht deutlich: Die Geschäftsleitung ist für Umsetzung und Überwachung der Maßnahmen verantwortlich und muss regelmäßig geschult werden. Als „regelmäßig“ im Sinne dieser Vorschrift gelten Schulungen, die mindestens alle drei Jahre angeboten werden.

Schulung der Geschäftsleitung nach §38 NIS-2

→ orientiert sich hierbei an der offiziellen BSI Handreichung und adressiert die Erkennung und Bewertung von Risiken.

# Exkurs: Die Rolle des Informations- sicherheitsbeauftragten

Das BSIG schreibt keine konkrete Rollenbezeichnung wie „Informationssicherheitsbeauftragter“ zwingend vor. Es verlangt jedoch eine klare organisatorische Verantwortungszuordnung.

In der Praxis übernimmt diese Koordinationsfunktion häufig der ISB bzw. der CISO mit folgenden Aufgaben:

- Steuerung des ISMS
- Koordination der Risikoanalyse
- Vorbereitung von Managemententscheidungen
- Begleitung von Audits
- Schnittstelle zu Incident- und BCM-Strukturen

Schulungen wie **Informationssicherheitsbeauftragte:r (TÜV)**

deutsch und englisch oder

**Chief Information Security Officer (CISO) (TÜV)**

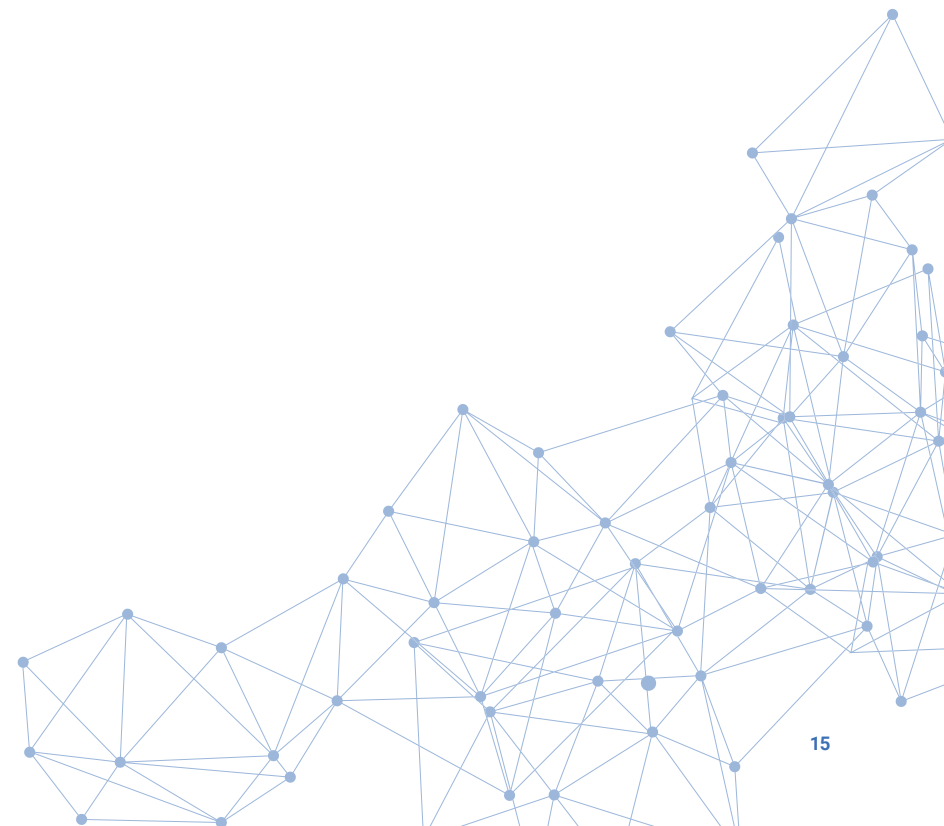
bereiten Teilnehmer auf die rollenspezifischen Herausforderungen vor.

# Fazit

**NIS-2 verlangt kein einzelnes Tool, keine einzelne Zertifizierung und keine isolierte Maßnahme.**

Gefordert ist ein integriertes, überprüfbares und wirksames Steuerungssystem für Informationssicherheit. Dort, wo passende Kompetenzen systematisch aufgebaut werden, wird die nachhaltige Umsetzung der NIS-2 Anforderungen gelingen.

Unternehmen, die ihre Umsetzung strukturiert angehen möchten, sollten daher prüfen, in welchen Rollen gezielte Kompetenzentwicklung erforderlich ist und wie sich diese in ein nachhaltiges Sicherheitskonzept integrieren lässt.



## Impressum

### isits AG International School of IT Security

HuestraÙe 30  
D-44787 Bochum

**Tel** +49 (0)234 927 898-0

**E-Mail** [info@is-its.org](mailto:info@is-its.org)

#### Disclaimer

Dieses Whitepaper dient der fachlichen Information und stellt keine Rechtsberatung dar. Es basiert auf dem Stand der gesetzlichen Anforderungen des BSIG im Kontext der NIS-2-Umsetzung zum Zeitpunkt der Veröffentlichung.

Die dargestellten Interpretationen und Umsetzungsempfehlungen ersetzen keine individuelle rechtliche oder organisatorische Prüfung. Unternehmen sollten ihre spezifische Betroffenheit sowie die Angemessenheit von Maßnahmen unter Berücksichtigung ihrer individuellen Risikolage eigenständig oder mit geeigneter rechtlicher Beratung bewerten.

Die hier gezeigten Schulungen sind keine gesetzliche Pflicht, helfen jedoch bei der strukturierten Umsetzung der gesetzlichen Anforderungen.

[www.is-its.org](http://www.is-its.org)