Online-Schulung · 7 Stunden · Bescheinigung

Risiken, über die man entscheiden kann.

Informationssicherheitsrisiken so formulieren, bewerten und behandeln, dass die Leitung entscheiden kann – für ISB, Risikoverantwortliche, IT-Leitung und Fachbereiche.

Die meisten Risikoregister scheitern nicht am Fachwissen, sondern an der Methodik: Stichwörter statt Szenarien, Stufen ohne beschriebene Skala, Maßnahmen, die angerechnet werden, ohne zu wirken – und eine Akzeptanz ohne Entscheider und ohne Frist. Diese Schulung vermittelt das Handwerk.

ISO/IEC 27001 verlangt eine festgelegte Risikobeurteilung und -behandlung (6.1.2 und 6.1.3); ISO/IEC 27005 und BSI-Standard 200-3 beschreiben das Vorgehen, DORA die regelmäßige Überprüfung des IKT-Risikomanagementrahmens.

Vom Szenario zur Entscheidung

- **Szenarien formulieren**
- **Bewerten mit Skalen**
- **Maßnahmen anrechnen**
- **Behandeln und vorlegen**

Risiken bewerten
7 Module
20 Lektionen
420 Minuten

- **Teilnahme-bescheinigung**
- **7 Begleit-unterlagen**
- **20 Infografiken**



Jede Stufe hat eine Folge im Verfahren. Lektion 3.3: die Matrix mit bewusst strenger Schnittführung oben links – und daneben, wer bei welcher Stufe entscheidet, was zusätzlich verlangt wird und wann neu bewertet werden muss.

Bewertungen, die vergleichbar sind

Beschriebene Skalen statt „gering, mittel, hoch“: Zwei Gruppen bewerten dasselbe Szenario und kommen zum selben Ergebnis.

Maßnahmen, die zählen

Angerechnet wird nur, was belegt wirkt – nicht, was vereinbart, beschafft oder geplant ist.

Restrisiken, die jemand trägt

Akzeptanz mit Entscheider, Begründung, Überwachung und Frist – prüffest dokumentiert.

7	20	60	420	7	75 %
Module	Lektionen	Quizfragen	Minuten Mindest-bearbeitungszeit	Begleitunterlagen	Bestehensgrenze

Schulung ansehen →

Angebot anfordern →

Herausgeber: Sachverständigenbüro Schulte, Düsseldorf. Die Schulung folgt der Struktur von ISO/IEC 27001, den Vorgehensbeschreibungen in ISO/IEC 27005 und BSI-Standard 200-3 sowie den Anforderungen der DORA-Verordnung. **Normtexte werden nicht wiedergegeben**; maßgeblich sind die gültigen Originaldokumente. Rechtsstand November 2026. Keine Rechtsberatung.

Woran Risikoregister scheitern.

Das Stichwort statt des Szenarios. „Cloud“, „Dienstleister“, „Cyberangriff“ – solche Einträge lassen sich nicht bewerten, weil jeder etwas anderes darunter versteht, und nicht behandeln, weil unklar bleibt, wogegen eine Maßnahme wirken soll.

Die Skala ohne Beschreibung. Stufen, die nur „gering, mittel, hoch“ heißen, messen nichts. Erst nachprüfbare Merkmale – Dauer, Aufwand, Außenwirkung – führen dazu, dass zwei Gruppen zum selben Ergebnis kommen.

Die Maßnahme, die nicht wirkt. „Vertraglich vereinbart“ ist nicht umgesetzt, „läuft seit Jahren“ ist nicht wirksam. Wer ohne Nachweis anrechnet, führt ein Register, das eine bessere Lage beschreibt als die tatsächliche.

Die Akzeptanz ohne Frist. Ein Risiko, das niemand namentlich trägt, das keine Überwachung hat und nie wieder bewertet wird, ist nicht akzeptiert, sondern unbearbeitet – mit einem freundlichen Namen.

Was die Schulung dagegen setzt

Eine durchgängige Methodik: Szenarien in der Form „weil … kann … sodass …“, beschriebene Skalen mit Betrachtungszeitraum, getrennte Brutto- und Nettobewertung, Maßnahmen nur mit Wirksamkeitsnachweis – und eine Entscheidungsvorlage, die beantwortet werden kann.

BEZUGSRAHMEN

ISO/IEC 27001 6.1.2 / 6.1.3 · **ISO/IEC 27005** · **BSI-Standard 200-3** · **DORA Art. 6** · **Risikoappetit** · **Akzeptanzkriterien**



Lektion 4.2: Ein Szenario vollständig durchgerechnet – welche Maßnahme welche Dimension senkt, was Geplantes zählt (nichts) und was die Differenz zwischen Brutto und Netto aussagt.

Fragen, die Prüfer und Aufsicht stellen

1. Wie sind Ihre Skalen definiert und wer hat sie freigegeben?
2. Worauf beruht die Häufigkeitsangabe dieses Risikos?
3. Welche Maßnahme senkt das Risiko – und woran ist ihre Wirksamkeit belegt?
4. Wer hat dieses Restrisiko akzeptiert, mit welcher Begründung und bis wann?
5. Wann wurde zuletzt neu bewertet, und was hat sich dabei geändert?

Die Schulung beantwortet jede dieser Fragen mit einer Vorlage – und mit geschulten Beteiligten, deren Teilnahme dokumentiert ist.

Die Differenz ist der Ertrag

Wenn zwei Gruppen dasselbe Szenario verschieden bewerten, fehlt Wissen – nicht Einigkeit. Genau dort liegt der Befund.

Übertragen heißt nicht loswerden

Eine Versicherung ersetzt Geld, keinen stehenden Prozess – Verantwortung und Meldepflichten bleiben.

Häufung wird sichtbar gemacht

Vier akzeptierte mittlere Risiken mit derselben Ursache sind in Wahrheit eines mit hohem Ausmaß.

Ablauf, Nutzen und Inhalte

Die sieben Module

1 Rahmen und Zuständigkeiten
Geltungsbereich, Risikoeigentümer und Entscheidungswege; Risikoappetit und Akzeptanzkriterien. · 35 Min.

2 Risiken identifizieren
Szenarien formulieren, vier Zugänge zur Identifikation, Risikoregister aufbauen und verknüpfen. · 60 Min.

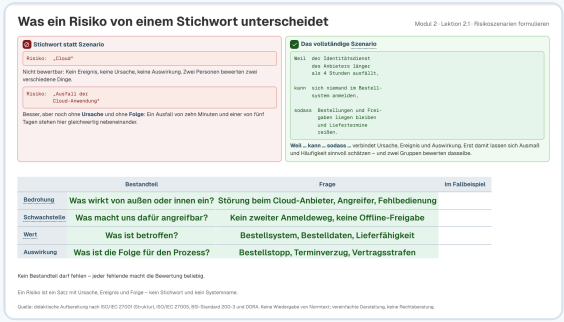
3 Risiken bewerten
Skalen und Betrachtungszeitraum, Ausmaß und Eintritt schätzen, Risikomatrix, Brutto und Netto. · 75 Min.

4 Bestehende Maßnahmen bewerten
Vorhanden, eingerichtet, durchgeführt, wirksam – und ein Szenario vollständig durchgerechnet. · 55 Min.

5 Risiken behandeln
Vermeiden, vermindern, übertragen, akzeptieren; Maßnahmen planen und verfolgen, Restrisiko dokumentieren. · 60 Min.

6 Fallstudie
Fünf Szenarien: unabhängig bewerten, Differenzen auflösen, Maßnahmen anrechnen, priorisieren und der Leitung vorlegen. · 105 Min.

7 Berichten und Abschluss
Managementbericht und Kennzahlen, Neubewertung nach Turnus und Anlass. · 30 Min.



Lektion 2.1: Was ein Risiko von einem Stichwort unterscheidet – die Satzform „weil … kann … sodass …“ mit Bedrohung, Schwachstelle, Wert und Auswirkung.

Durchgängiger Fall

Ein geschäftskritischer Bestellprozess mit Cloud-Anwendung, externem Identitätsdienst und IT-Dienstleister. Fünf Szenarien werden von zwei Gruppen unabhängig bewertet, die Differenzen aufgelöst, Maßnahmen angerechnet und die Restrisiken der Leitung vorgelegt.

Für wen

Informationssicherheitsbeauftragte, Risiko- und Prozessverantwortliche, IT-Leitung, Compliance und Fachbereiche, die Risiken mitbewerten. Grundkenntnisse eines ISMS sind hilfreich, aber nicht erforderlich.

Sieben Begleitunterlagen – die vollständige Arbeitsmappe

Bewertungsmethodik mit Skalen — B1

Modul 1/3

Geltungsbereich, Rollen, Skalen, Matrix, Risikoappetit und Akzeptanzkriterien – von der Leitung freizugeben.

Leitfaden Risikoszenarien — B2

Modul 2

Von der Idee zum bewertbaren Satz: Bedrohung, Schwachstelle, Wert, Auswirkung, Schutzziel.

Risikoregister — B3

Modul 2/3

Eine Zeile je Szenario – mit Brutto, Netto, Annahmen, Maßnahmen und Stand.

Maßnahmenplan — B4

Modul 5

Was genau, welche Wirkung, wer, bis wann und woran die Erledigung erkennbar ist.

Risikoakzeptanz — B5

Modul 5

Die sechs Pflichtangaben – mit Prüfung auf Pflichten, Schäden Dritter und Häufung.

Managementbericht — B6

Modul 7

Lage, Entscheidungen, Fortschritt, Restrisiken, Unsicherheiten – mit Entscheidungsfrage.

Checkliste Neubewertung — B7

Modul 7

Turnus und Anlässe im Blick: Annahmen prüfen, Wirksamkeit prüfen, Änderung begründen.

Lernkontrollen und Abschluss — Quiz

Nach jeder Lektion

60 Fragen mit Erläuterung. Abschlussprüfung über alle Module, bestanden ab 75 Prozent.

So läuft es ab

1 Plätze buchen
Sie teilen uns die Zahl der Teilnehmenden mit; wir richten Ihr Unternehmen im Schulungsportal ein.

2 Einladen
Teilnehmende werden im Portal angelegt und erhalten ihren persönlichen Zugang per E-Mail.

3 Lernen
Sieben Module mit Infografiken und Begleitunterlagen, Lernkontrollen nach jeder Lektion.

4 Fall bearbeiten
Modul 6 führt durch fünf Szenarien bis zur Entscheidungsvorlage an die Leitung.

5 Nachweisen
Abschlussprüfung ab 75 Prozent, Bescheinigung als PDF, Auswertung im Portal.

Was Sie erhalten

Zugang je Teilnehmer
Persönlicher Link, Fortschritt wird gespeichert, Bearbeitung in mehreren Sitzungen möglich.

Teilnahmebescheinigung
PDF mit fortlaufender Nummer, Inhalten, Dauer und Prüfadresse zur Online-Verifikation.

Sieben Begleitunterlagen
Bewertungsmethodik, Szenarienleitfaden, Risikoregister, Maßnahmenplan, Risikoakzeptanz, Managementbericht, Checkliste Neubewertung.

Auswertung im Portal
Stand je Teilnehmer, Abschlüsse, Bescheinigungen und Wiederholungsintervalle auf einen Blick.

Anbindung an Ihr ISMS

Abschlüsse lassen sich automatisch als Schulungsnachweise in das ISMS-Werkzeug **Vercora** übertragen – mit Bescheinigungsnummer, Datum und Prüfadresse.

Ihr Ansprechpartner

Herausgeber

Heinrich Markus Schulte

IT-Sachverständiger · CISA, CISM, CIPP/E, CEH
Schwerpunkte: NIS-2, DORA, CRA, ISMS

> *„Ein Risiko ist erst dann gesteuert, wenn jemand mit Namen darüber entschieden hat – mit Begründung, Überwachung und Frist. Genau dieses Handwerk vermittelt die Schulung.“*

Angebot anfordern →

Schulung ansehen →

Sachverständigenbüro Schulte
Grünberger Weg 9 · 40627 Düsseldorf
+49 211 93375777
sachverstaendiger@itschulte.de
itschulte.de

Weitere Schulungen aus demselben Haus

Interne ISMS-Audits — 420 Min.
ISO/IEC 27001 Abschnitt 9.2 · ISO 19011
Audits planen, Nachweise bewerten und Feststellungen schreiben, die standhalten.

NIS-2-Geschäftsleitungsschulung — 180 Min.
§ 38 Abs. 3 BSIG · BSI-Curriculum
Die gesetzlich geforderte Schulung der Geschäftsleitung zu Risikomanagement, Pflichten und Haftung.

Incident Response & Playbooks — 420 Min.
NIST SP 800-61 · ISO/IEC 27035 · § 32 BSIG
Vorfälle erkennen, melden, eindämmen und auswerten – mit fünf szenariobasierten Playbooks.

Notfallmanagement & BCM — 120 Min.
BSI-Standard 200-4 · DER.4
BCM aufbauen und üben – anschlussfähig zur ISO 22301.

Die Schulung vermittelt Methodik des Risikomanagements. **Normtexte werden nicht wiedergegeben**; maßgeblich sind die jeweils gültigen Originaldokumente und die Vorgaben Ihrer Organisation. Die Bescheinigung bestätigt die Teilnahme; sie ist keine Zertifizierung und kein Prüftestat. Rechtsstand November 2026. Keine Rechtsberatung.