Halderstone

Trainingsmodul

Informationssicherheits-Risikomanagem

Entscheidungen zur Risikobehandlung und Nachvollziehbarkeit zu Steuerungsmassnahmen und SoA beurteilen

Geht Ihr Audit über das Prüfen von Risikoregister hinaus und beurteilt auch Risikologik und Behand-lungsentscheidungen?

Überblick

ISO/IEC 27001 erwartet, dass Risikobeurteilung und Risikobehandlung das Informations-sicherheitsmanagementsystem (ISMS) steuern und nicht als eigenständige Dokumentation nebenher bestehen. In der Praxis treffen Auditoren oft auf allgemeine Assetlisten, wiederverwendete Bedrohungskataloge, inkonsistente Bewertungen und eine Erklärung zur Anwendbarkeit (SoA), die sich nicht auf konkrete Risiken und Behandlungsent-scheidungen zurückführen lässt.

Dieses normbezogene Auditmodul fokussiert darauf, wie das ISMS-Risikomanagement dort auditiert wird, wo die Informationssicherheitslogik entscheidend ist: Asset–Bedrohung–Schwachstellenlogik, Qualität der Behandlungsentscheidungen und Nachvollzieh-barkeit von Risiken zu ausgewählten Steuerungs-massnahmen (einschliesslich Anhang A) und zur SoA. Es vermittelt keine generischen Methoden des Risikomanagements und keine allgemeinen Audittechniken erneut; es wendet eine Auditbeurteilung auf die Anforderungen an das Risikomanagement nach ISO/IEC 27001 an.

Zielgruppe

- Angehende Auditierende, die ISO/IEC 27001 nach Best Practices auditieren wollen
- Praktizierende Auditierende von ISO/IEC 27001, die ihr Auditwissen, ihr Urteilsvermögen und ihre Wirksamkeit bei Audits stärken wollen

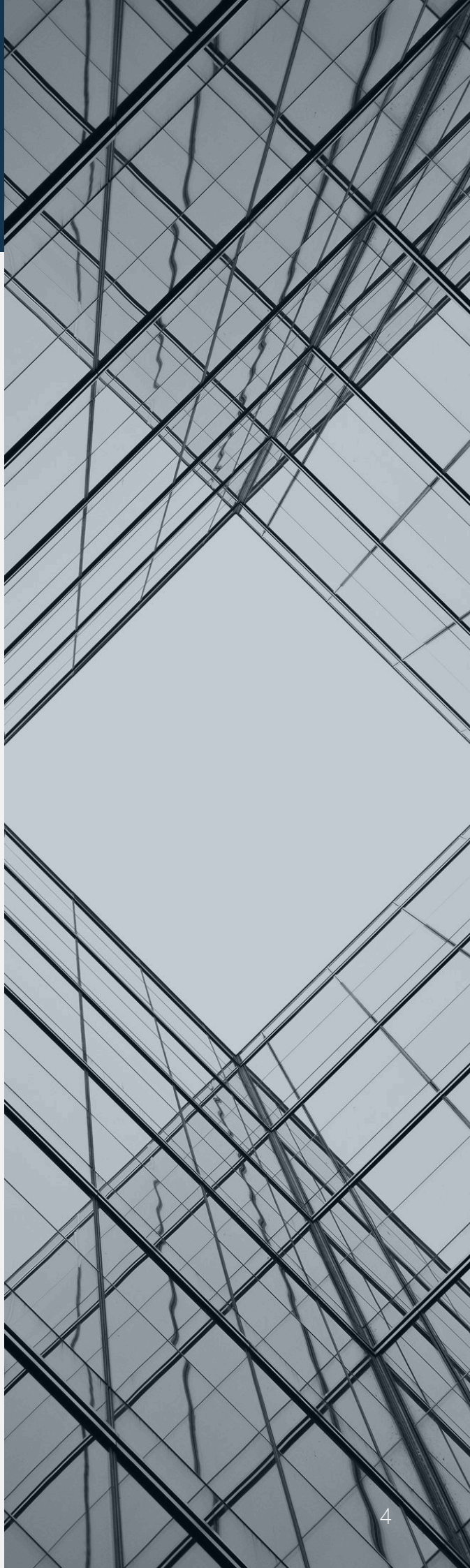
Ist dieses Modul für Sie das Richtige?

Es passt gut für Sie, wenn Sie...

- prüfen wollen, ob das ISMS-Risikomanagement Sicherheitsentscheidungen tatsächlich steuert.
- nicht nur die Vollständigkeit des Risikoregisters, sondern die Asset–Bedrohung–Schwachstellenlogik testen möchten.
- Risiken vom Kontext über Behandlungsentscheidungen bis zu Steuerungsmassnahmen und zur SoA nachverfolgen.
- Ihre Beurteilung von Risikoakzeptanz, Priorisierung und Nachvollziehbarkeit schärfen möchten.
- Auditfeststellungen suchen, die schwache Risikologik und systemische Lücken sichtbar machen.

Es passt möglicherweise weniger gut für Sie, wenn Sie...

- vor allem Risikobeurteilungs- oder Behandlungsverfahren entwerfen oder verbessern wollen.
- generische Risikomanagementframeworks oder Bewertungsmodelle erwarten.
- sich auf die Moderation von Workshops oder die Erstellung von Risikodokumentation fokussieren.
- nicht bereit sind, formell vollständige, aber fachlich schwache Risikobegründungen zu hinterfragen.



Lernergebnisse

Zentrale Lernergebnisse

- Beurteilen, ob die Asset–Bedrohung–Schwachstellenlogik glaubwürdig und für Entscheidungen im ISMS geeignet ist
- Innere Stimmigkeit von Risikobeurteilungsergebnissen mit praktischen Auditchecks und gezielten Stichprobenheuristiken prüfen
- Beurteilen, ob Entscheidungen zur Risikobehandlung nachvollziehbar, autorisiert und überprüfbar sind

Zusätzliche Fähigkeiten

- Durchgängige Nachvollziehbarkeit von Risiken zu Steuerungsmassnahmen und zur Erklärung zur Anwendbarkeit (SoA) verifizieren
- Häufige systemische Schwachstellen im Risikomanagement nach ISO/IEC 27001 erkennen und Frühwarnsignale lesen
- Wirksame Nachweiswege und Nachweisanfragen aufbauen, die Risikodokumentation mit der operativen Realität der Steuerungsmassnahmen verbinden

Agenda

Was ISMS-Risikomanagement auditfähig macht

Wie das Risikomanagement als Entscheidungs- und Nachvollzugssystem funktioniert und nicht nur ein Risikoregister existiert oder «vollständig» wirkt

Zusammenspiel von Assets, Bedrohungen und Schwachstellen testen

Wie die Plausibilität von Assets im Geltungsbereich, realistische Bedrohungswege und sinnvolle Schwachstellen geprüft werden, einschliesslich Grenz- und Abhängigkeitsrisiken aus gemeinsam genutzten Diensten, Cloud, Lieferanten und Schattenassets

Risikobeurteilungsergebnisse, die im Audit standhalten

Wie die innere Stimmigkeit zwischen Geltungsbereich, Assets, Sicherheitsvorfällen, Schwachstellen und Ergebnissen geprüft und mit gezielten Stichproben schwache oder bequemkeitsgetriebene Begründungen offengelegt werden

Entscheidungen zur Risikobehandlung beurteilen

Wie beurteilt wird, ob Behandlungsentscheidungen (reduzieren, behalten, vermeiden, teilen) stimmig, autorisiert und dokumentiert sind und ob die Risikoakzeptanz in Bezug auf Kompetenz, Begründung, Restrisiko und Auslöser für Überprüfungen glaubwürdig ist

Nachvollziehbarkeit zu Steuerungsmassnahmen und zur Erklärung zur Anwendbarkeit (SoA)

Wie die Nachvollziehbarkeit von Risiken zur Auswahl von Steuerungsmassnahmen und zur Begründung der Anwendbarkeit überprüft und die Vollständigkeit der SoA sowie Hinweise auf «Control Theatre» getestet werden

Nachweiswege von der Dokumentation zur Umsetzung

Wie der Nachweis von Behandlungsentscheidungen über Projekte und die Umsetzung von Steuerungsmassnahmen bis zur gelebten Praxis verfolgt und Brüche zwischen Plänen, Massnahmen und dem tatsächlichen Betrieb erkannt werden

Praxisworkshop mit Auditsimulation

Anwendung der erlernten Konzepte, Methoden und Ansätze in einem realistischen Praxisfall

Enthaltene Unterlagen

Lernunterlagen

- Foliensatz
- Workbook für Teilnehmende

Vorlagen & Werkzeuge

- Tool für die Planung von Auditgesprächen
- Checkliste für dokumentierte Informationen
- Stichprobentool
- Arbeitsblätter für die Auditanalyse
- Bibliothek typischer Schwachstellen
- KI-Prompt-Sammlung

Bestätigung

- Teilnahmebestätigung

Vorbereitungshinweise

Vorausgesetzter Hintergrund

Dieses Modul setzt voraus, dass die Teilnehmenden bereits mit Auditnachweisen und beruflichem Urteilsvermögen arbeiten können und über Grundkenntnisse der ISO/IEC 27001-ISMS-Terminologie verfügen, einschliesslich der Erklärung zur Anwendbarkeit.

Hilfreicher Hintergrund umfasst:

- Verständnis der allgemeinen Logik zur Behandlung von Risiken und Chancen (Methoden werden hier nicht erneut vermittelt)
- Fähigkeit, dokumentierte Absicht von Nachweis der Umsetzung zu unterscheiden
- Vertrautheit mit typischen sicherheitsrelevanten Assets und Abhängigkeiten (zum Beispiel Identitäten, Endgeräte, cloudbasierten Diensten, kritischen Datenflüssen)

Vorbereitungsmodule

Grundlagen (je nach Vorwissen)

Hilfreich, wenn Sie mit den zugrunde liegenden Konzepten noch wenig vertraut sind

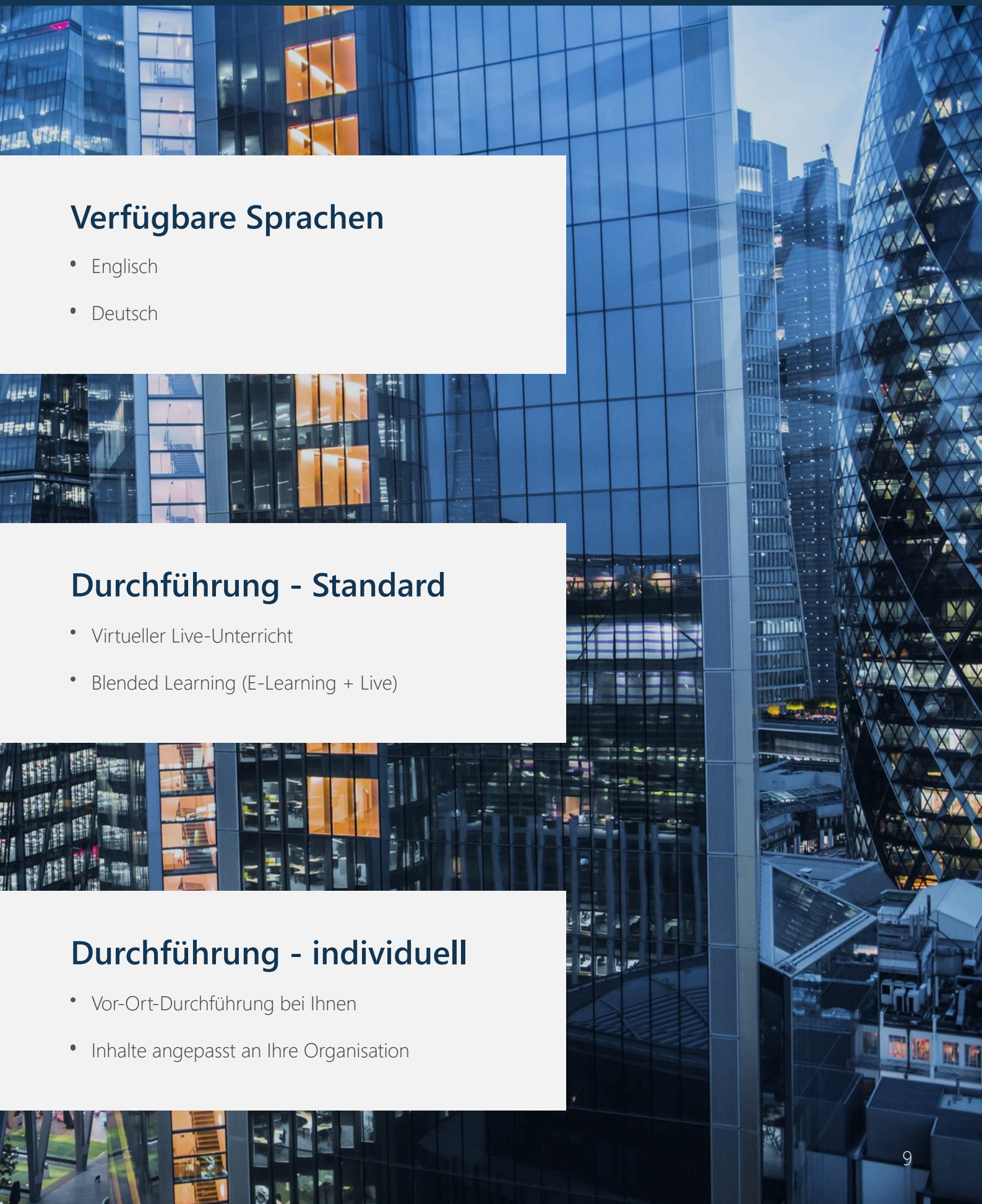
- Audit-Grundsätze

Unterstützend (optional)

Hilfreich, aber nicht erforderlich, um wirksam teilnehmen zu können

- Risikomanagement auditieren
- Risikomanagement

Organisatorisches



Verfügbare Sprachen

- Englisch
- Deutsch

Durchführung - Standard

- Virtueller Live-Unterricht
- Blended Learning (E-Learning + Live)

Durchführung - individuell

- Vor-Ort-Durchführung bei Ihnen
- Inhalte angepasst an Ihre Organisation

Halderstone

Halderstone by Langer & Co
Zürcherstrasse 2
CH-8852 Altendorf
Schweiz
info@halderstone.com
www.halderstone.com