Halderstone

Trainingsmodul

Informationssicherheits-Risikomanagem

Informationssicherheitsrisiken systematisch beurteilen, behandeln und mit nachvollziehbaren Entscheidungen gemäss ISO/IEC 27001 dokumentieren

Führt Ihre Risikomanagementpraxis zu Artefakten, die Steuerungsentscheide nicht beeinflussen?

Überblick

Risikoregister und Bewertungsübungen stehen oft isoliert da und sind von der Auswahl von Steuerungsmassnahmen und den Akzeptanzentscheidungen getrennt.

Dieses Trainingsmodul zeigt, wie ISO/IEC 27001 Risikobeurteilung und Risikobehandlung rahmt, wie Risikokriterien und Risikovermerke definiert werden und wie Beurteilungsergebnisse so dokumentiert werden, dass sie die Behandlungsplanung und die Akzeptanz des Restrisikos unterstützen. Die Teilnehmenden lernen, stimmige Artefakte zur Risikobehandlung zu erstellen, die Risiken, Behandlungsoptionen, ausgewählte Steuerungsmassnahmen und die Erklärung zur Anwendbarkeit (SoA) miteinander verknüpfen. Im Zentrum stehen Nachvollziehbarkeit und Pflege statt die Mechanik von Bewertungsmodellen.

Zielgruppe

- Personen, die ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 entwerfen, aufbauen, betreiben oder verbessern
- Führungskräfte und Abteilungsleitende, die für die Wirksamkeit und Leistung eines ISMS verantwortlich sind
- Personen, die für Prozesse, Politiken, Assets, Risiken und Steuerungsmassnahmen im Bereich Informationssicherheit verantwortlich sind
- Auditierende von ISO/IEC 27001, die ihr Verständnis für managementseitige Best Practices vertiefen wollen (nicht Audittechnik)

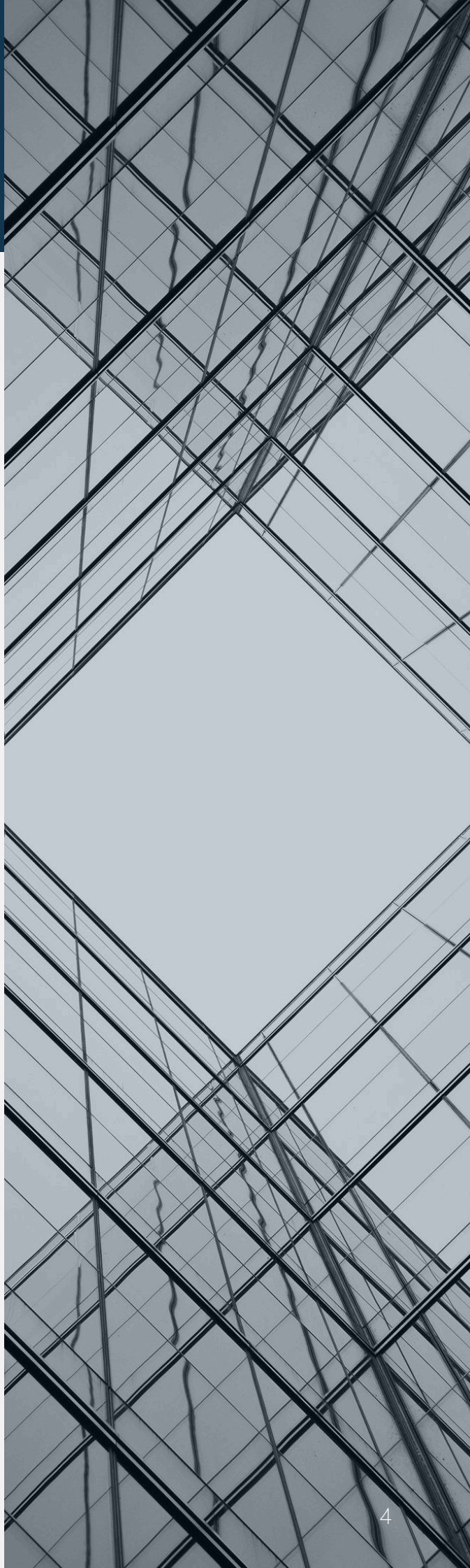
Ist dieses Modul für Sie das Richtige?

Es passt gut für Sie, wenn Sie...

- für Risikobeurteilung, Risikobehandlung oder Akzeptanzentscheidungen im ISMS verantwortlich sind.
- mit uneinheitlichen Risikokriterien, schwachen Risikovermerken oder unklaren Verantwortlichkeiten zu kämpfen haben.
- Risikobeiträge benötigen, die die Auswahl von Steuerungsmassnahmen und Entscheidungen zur SoA klar begründen.
- Artefakte zur Risikobehandlung erstellen müssen, die in Audits und der Managementbewertung Bestand haben.
- Risikomanagement als wiederholbaren Entscheidungsprozess statt als einmalige Übung etablieren wollen.

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

- eine allgemeine Einführung in Informationssicherheitsrisiken suchen.
- quantitative Risikomodellierung oder fortgeschrittene Risikoanalysen erwarten.
- eine werkzeugspezifische oder vorlagengetriebene Einführung in die Risikobeurteilung wünschen.
- bereits einen konsistenten, gut verstandenen und überprüfbaren ISMS-Risikoprozess betreiben.



Lernergebnisse

Zentrale Lernergebnisse

- ISO/IEC 27001-Anforderungen an Risikobeurteilung und Risikobehandlung praxisnah einordnen
- Dokumentierte Elemente wie Kriterien, Vermerke und Entscheidungsaufzeichnungen für konsistente Risikomethoden definieren
- Artefakte zur Risikobehandlung erstellen, die Entscheide und die Akzeptanz des Restrisikos belegen

Zusätzliche Fähigkeiten

- Nachvollziehbarkeit von Risiken über Behandlungsentscheide bis zu Steuerungsmassnahmen und zur Erklärung zur Anwendbarkeit sicherstellen
- Typische Schwachstellen in Risikobeurteilung und Risikobehandlung erkennen, die zu reiner Papierarbeit führen
- Pflegeroutinen und Auslöser für Überprüfungen festlegen, damit Risikoregister aktuell und nützlich bleiben

Agenda

Rolle des Risikomanagements im ISMS

Wie ISO/IEC 27001 Risikomanagement nutzt, um nachvollziehbare Entscheide statt Papierarbeit zu ermöglichen, und wie die Risikaarbeit mit Geltungsbereich, Zielen, Steuerungsmassnahmen und Managementbewertung zusammenhängt

Risikoterminologie und erforderliche Definitionen nach ISO/IEC 27001

Wie Risikokonzepte der Informationssicherheit in der Norm verwendet werden, einschliesslich Risikoverantwortliche, Akzeptanz und Restrisiko, und was als Risikomethode definiert und gepflegt werden muss, ohne sie neu zu erklären

Risikokriterien und Anforderungen an die Konsistenz

Wie Vorgaben der Governance in brauchbare Kriterien für Auswirkung, Eintrittswahrscheinlichkeit und Akzeptanz übersetzt werden und warum schlecht gestaltete Kriterien bei Konsistenz und Nachweisbarkeit scheitern

Ergebnisse der Risikobeurteilung, die Behandlungsentscheide unterstützen

Wie gute Risikovermerke im ISMS in der Praxis aussehen, einschliesslich Klarheit, Verantwortlichkeit und betroffener Informationen oder Prozesse, und welche Minimalangaben nötig sind, um verwaiste Risiken und nicht belastbare Schlussfolgerungen zu vermeiden

Erwartungen an die Risikobehandlung und die Artefakte

Wie ISO/IEC 27001 Behandlungsoptionen und die Belegung von Entscheiden definiert und wie eine verhältnismässige Behandlungsplanung mit Verantwortlichkeiten, Terminen, Abhängigkeiten und dem Umgang mit dem Restrisiko aussieht

Nachvollziehbarkeit zu Steuerungsmassnahmen und Schnittstelle zur SoA

Wie Behandlungsentscheide die Auswahl und Begründung von Steuerungsmassnahmen steuern und wie die Erklärung zur Anwendbarkeit für jede einbezogene oder ausgeschlossene Steuerungsmassnahme eine belastbare Begründung mit Bezug zur Risikobehandlung zeigen muss

Pflege der Risikoinformationen über die Zeit

Wie Änderungen, Sicherheitsvorfälle und Leistungsindikatoren Risikoupdates auslösen und wie Risiko- und Behandlungsartefakte mit der operativen Realität und den Inputs für die Managementbewertung im Einklang bleiben

Praxisworkshop

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

Enthaltene Unterlagen

Lernunterlagen

- Foliensatz
- Workbook für Teilnehmende

Vorlagen & Werkzeuge

- Prozess für Informationssicherheits-Risikomanagement
- Beispiel für ein Risikoregister für Informationssicherheitsrisiken
- Checkliste zur Qualität von Risikokriterien
- Protokoll zu Risikobehandlungsentscheiden
- Vorlage für den Risikobehandlungsplan
- KI-Prompt-Sammlung für typische Anwendungsfälle

Bestätigung

- Teilnahmebestätigung

Vorbereitungshinweise

Vorausgesetzter Hintergrund

Dieses Modul setzt voraus, dass Teilnehmende bereits mit allgemeinen Risikokonzepten und der grundlegenden Logik von Managementsystemen arbeiten können.

Hilfreiche Vorkenntnisse sind:

- Verständnis von Risikoterminologie sowie von Bewertungs- und Behandlungsansätzen
- Vertrautheit mit Rollen im Managementsystem, dokumentierten Informationen und Steuerungsroutinen
- Grundlegende Kenntnisse der Informationssicherheit

Vorbereitungsmodule

Grundlagen (je nach Vorwissen)

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

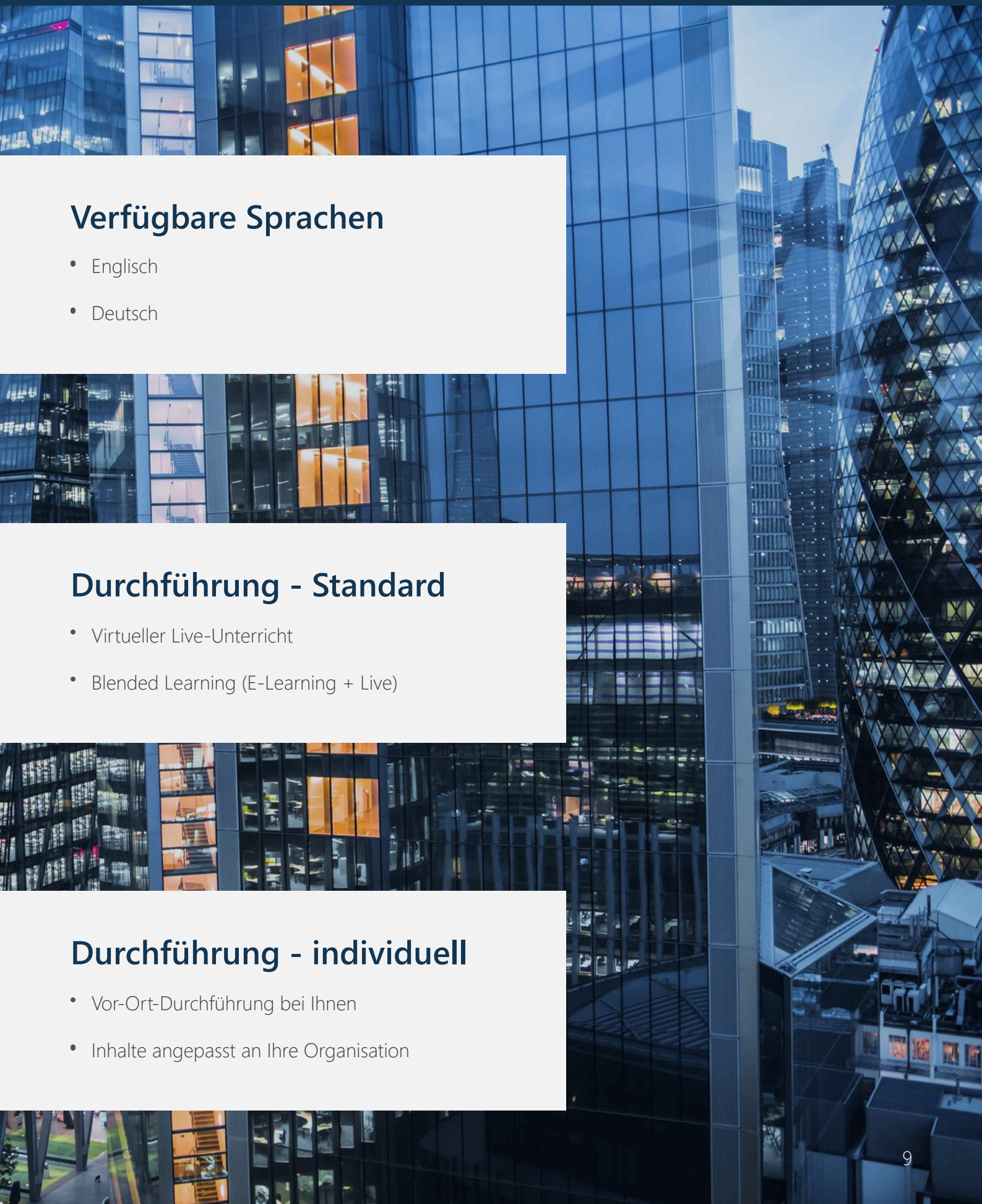
- Risikomanagement

Unterstützend (optional)

Hilfreich, aber nicht erforderlich, um wirksam teilnehmen zu können

- Kontext & Geltungsbereich

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