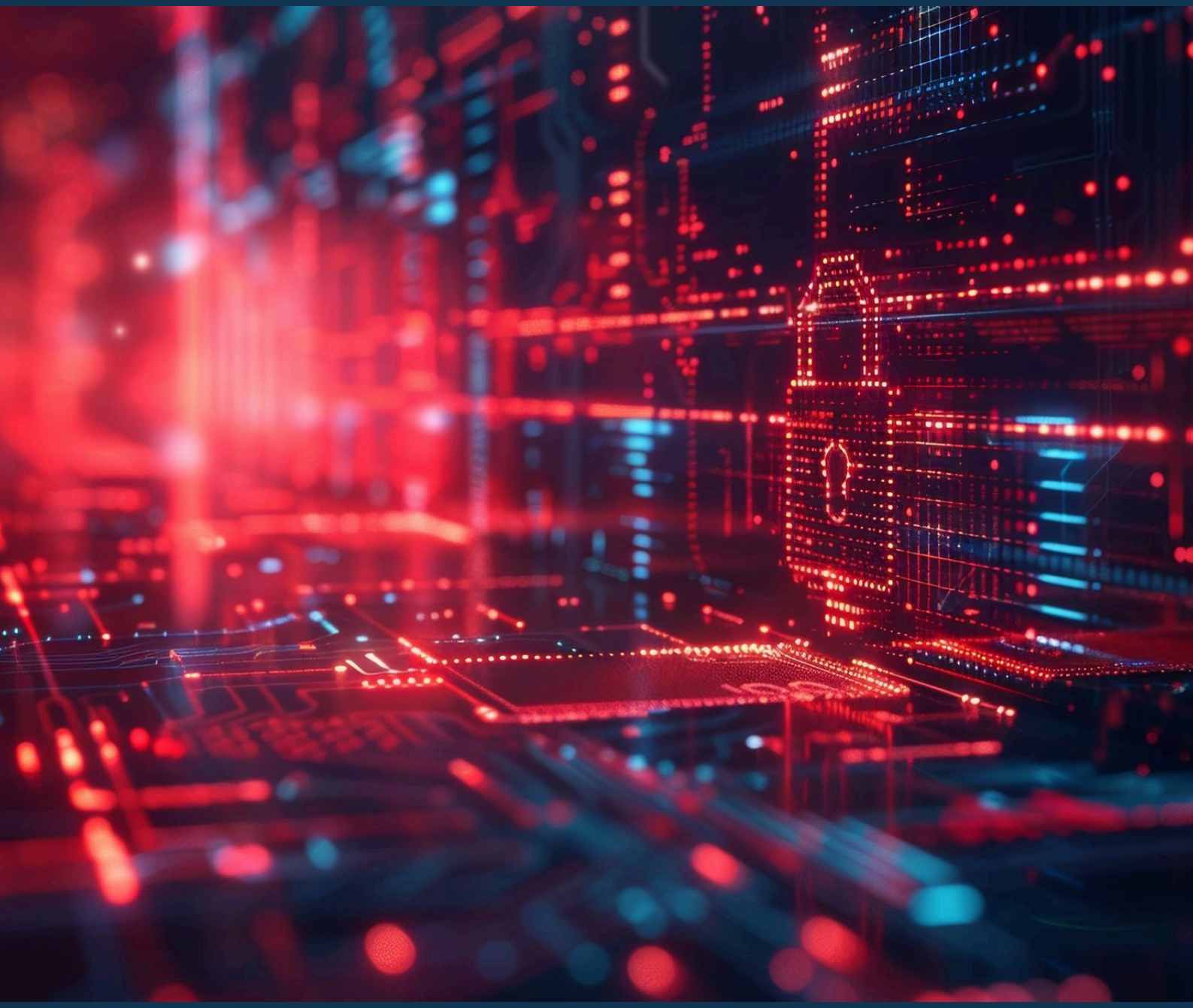
Halderstone



Trainingsmodul

Betriebliche Steuerung der Informationssicherheit

Informationssicherheitsmassnahmen in den täglichen Abläufen gemäss ISO/IEC 27001 konsistent planen, umsetzen und betreiben

Geraten Ihre ausgewählten Informations-sicherheitsmassnahmen vom Konzept in den täglichen Betrieb?

Überblick

Massnahmen, die in der Risikobehandlung und Planung ausgewählt wurden, können an Wirksamkeit verlieren, wenn sie ohne klare Rollen, Kriterien und Änderungssteuerung umgesetzt werden.

In diesem Modul lernen die Teilnehmenden, Entscheidungen aus der Risikobehandlung in operative Routinen zu überführen, Schnittstellen und Übergaben zwischen Verantwortlichen für Massnahmen und dem Betrieb zu definieren sowie sicherheitsrelevante Änderungen in bestehende Änderungsprozesse zu integrieren. Das Modul behandelt, was «betrieben und aufrechterhalten» bei unterschiedlichen Massnahmentypen bedeutet, wie Ausnahmen und kompensierende Massnahmen gehandhabt werden, wie typische Ausfallarten erkannt werden und wie der minimale Nachweis dokumentiert wird. Es baut auf Grundlagen zu Risiko, Geltungsbereich und vorbeugenden Massnahmen auf, wiederholt diese Themen aber nicht.

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)

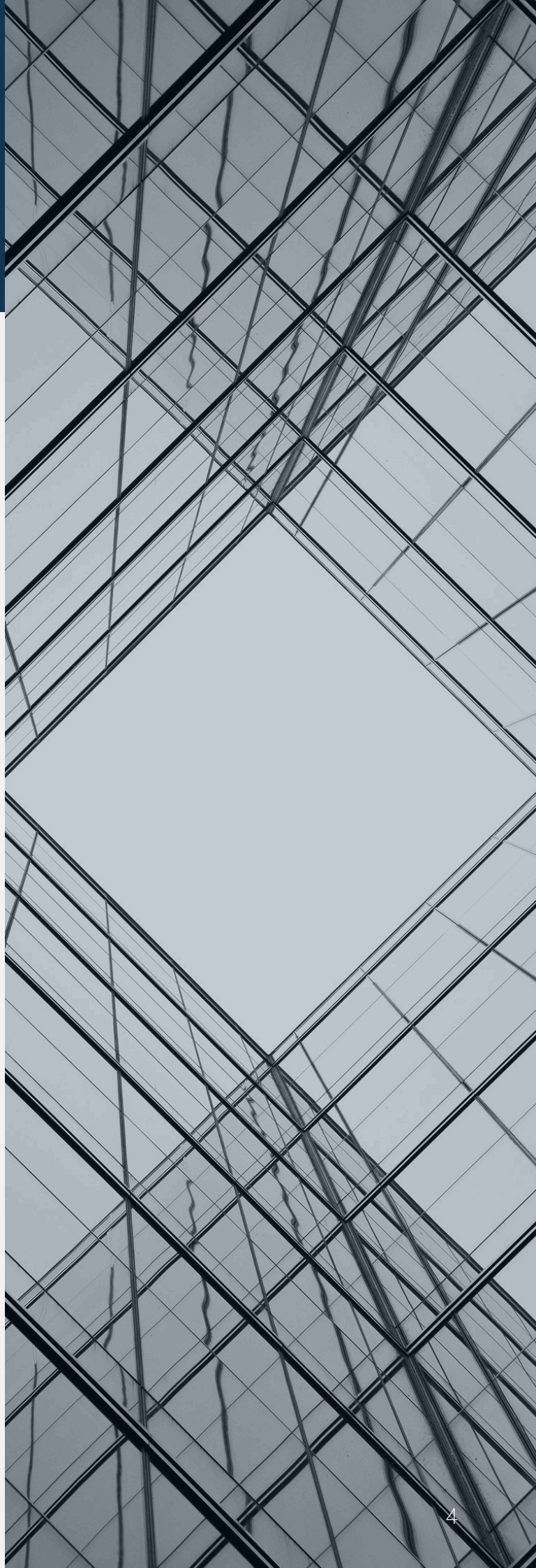
Ist dieses Modul für Sie das Richtige?

Es passt gut für Sie, wenn Sie...

- den ISMS-Tagesbetrieb und die Ausführung von Massnahmen selbst steuern oder überwachen.
- mit Massnahmen zu kämpfen haben, die auf dem Papier bestehen, in der gelebten Praxis aber abdriften.
- operative Routinen benötigen, die Sicherheitsentscheide über die Zeit nachvollziehbar halten.
- Verantwortung, Änderungen oder Übergaben über Teams oder Lieferanten hinweg steuern.
- möchten, dass ISMS-Massnahmen unter realem Lieferdruck und in Sicherheitsvorfällen Bestand haben.

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

- nach dem Design, der Auswahl oder der Auslegung von Anhang A suchen.
- technische Härtung, Konfiguration oder Werkzeugunterstützung erwarten.
- Risikobeurteilung, Gestaltung der SoA oder Massnahmenziele von Grund auf erklärt haben möchten.
- bereits stabile, klar verantwortete und konsistent umgesetzte ISMS-Massnahmen betreiben.



Lernergebnisse

Zentrale Lernergebnisse

- Risikobehandlungsentscheide in operative Steuerungsroutinen mit klaren Aufgaben und Zeitpunkten überführen
- Schnittstellen und Übergaben zwischen Verantwortlichen für Massnahmen, IT-Betrieb und Dienstleistungsmanagement definieren
- Sicherheitsrelevante Änderungen in allgemeine Änderungsmanagement-Prozesse integrieren

Zusätzliche Fähigkeiten

- Festlegen, was «betrieben und aufrechterhalten» bei unterschiedlichen Massnahmentypen bedeutet und welcher Nachweis nötig ist
- Ausnahmen und kompensierende Massnahmen handhaben, ohne die Wirkabsicht der Massnahme zu untergraben
- Typische Ausfallarten von Massnahmen erkennen und minimale Nachweise für Governance und Nachweisführung erstellen

Agenda

Was operative Steuerung in der ISO/IEC 27001-Praxis bedeutet

Wie operative Steuerung die ISMS-Absicht in wiederholbare Umsetzung überführt und wo sie typischerweise durch Drift, informelle Ausnahmen, unklare Verantwortung oder stille Änderungen aus dem Takt gerät

Planung und Steuerung des ISMS-Betriebs

Wie ausgewählte Massnahmen und Anforderungen in konkrete operative Routinen mit definierten Verantwortlichen, Auslösern und Frequenzen überführt werden, ohne den ISMS-Geltungsbereich neu zu ziehen

Kontrollierte Änderungen im Informationssicherheitsbetrieb

Wie sicherheitsrelevante Änderungen erkannt, beurteilt, freigegeben und in bestehende Änderungsprozesse integriert werden, ohne parallele Sicherheitsabläufe zu schaffen

Anhang A-Massnahmen betreiben, ohne die Massnahmen neu zu vermitteln

Wie Anhang A-Massnahmen durch Routinen, Steuerungsmassnahmen und minimalen nachvollziehbaren Nachweis praktisch betrieben und aufrechterhalten werden, statt sie neu zu dokumentieren

Ausgelagerte und durch Lieferanten betriebene Massnahmen

Wie durch Lieferanten betriebene Massnahmen über klare Schnittstellen, Verantwortlichkeiten und operative Überprüfungspunkte auditierbar und steuerbar werden

Operative Abweichungen, Sicherheitsvorfälle und Nachverfolgung von Korrekturmassnahmen

Wie operative Abweichungen und Sicherheitsvorfälle unterschieden, eskaliert, eingedämmt und in Korrekturmassnahmen überführt werden, ohne Verantwortlichkeiten zu verwischen

Praxisworkshop

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

Enthaltene Unterlagen

Lernunterlagen

- Foliensatz
- Workbook für Teilnehmende

Vorlagen & Werkzeuge

- ISMS-Matrix für operative Steuerung
- Vorlage für die Spezifikation operativer Routinen
- Checkliste für sicherheitsrelevante Änderungsfolgen
- Protokoll für Ausnahmen und kompensierende Massnahmen
- Arbeitsblatt für Lieferantenschnittstellen bei Massnahmen
- Leitfaden für den minimalen operativen Nachweis

Bestätigung

- Teilnahmebestätigung

Vorbereitungshinweise

Vorausgesetzter Hintergrund

Dieses Modul setzt allgemeine Vertrautheit mit der Umsetzung von Managementsystemen und grundlegenden Informations-sicherheitskonzepten voraus. Es setzt zudem Grundlagen der operativen Steuerung voraus und fokussiert auf die ISO/IEC 27001-spezifische Anwendung.

Hilfreiche Vorkenntnisse sind:

- Verständnis von Rollen, Verantwortlichkeiten und dokumentierten Informationen in Managementsystemen in der gelebten Praxis
- Grundlegende Vertrautheit mit gängigen Informations-sicherheitsmassnahmen

Vorbereitungsmodule

Grundlagen (je nach Vorwissen)

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

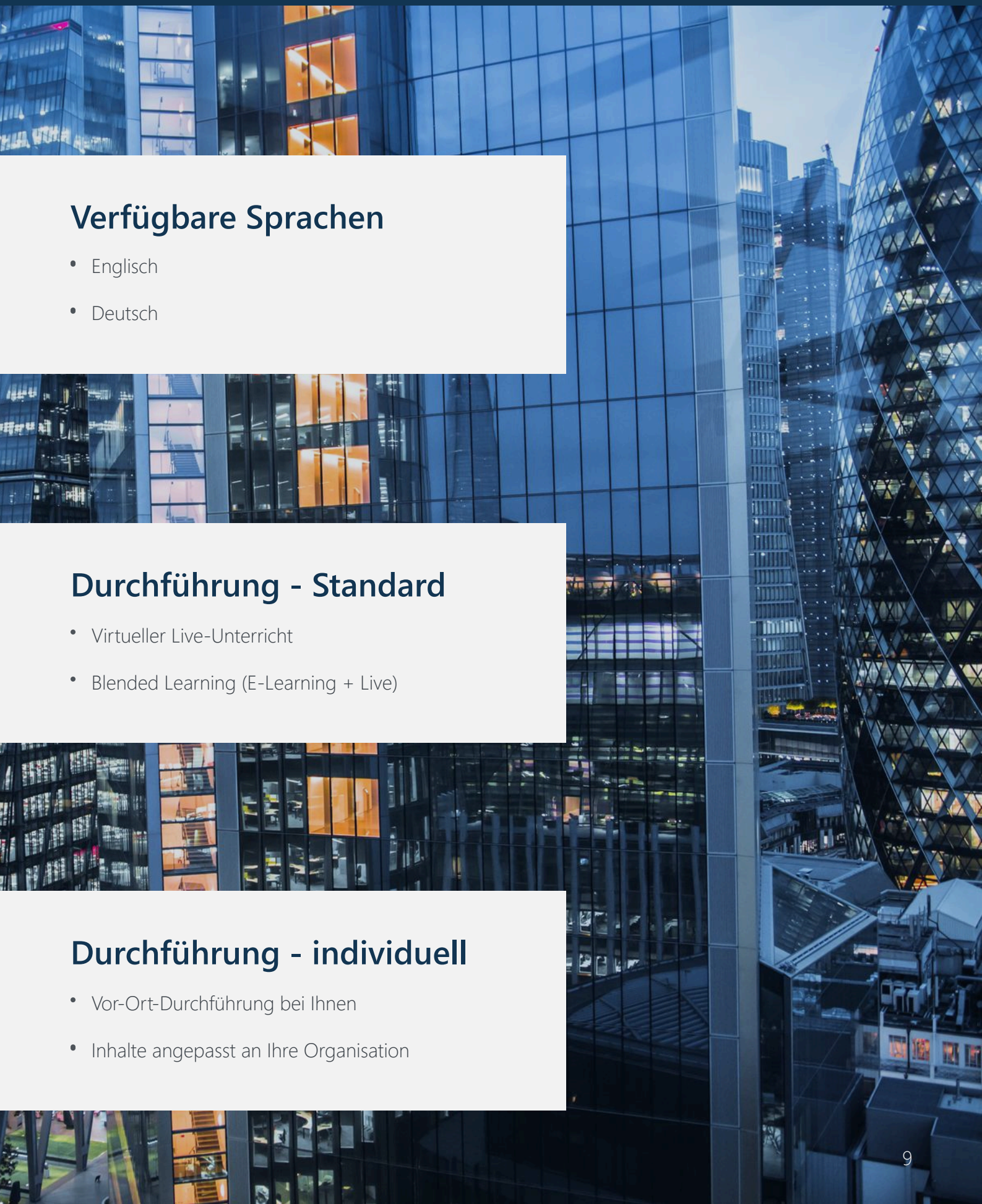
- Betriebliche Steuerung
- Informationssicherheits-Risikomanagement

Unterstützend (optional)

Hilfreich, aber nicht erforderlich, um wirksam teilnehmen zu können

- Informationssicherheitsmassnahmen verstehen

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