Halderstone

Trainingsmodul

Informationssicherheitsmassnahmen auc

Anwendbarkeit, Umsetzungsnachweise und typische Schwachstellen über die Annex-A-Massnahmenthemen von ISO/IEC 27001 hinweg beurteilen

Geht Ihr Audit über die reine Listenprüfung von Massnahmen hinaus und schafft nachvollziehbare Klarheit darüber, wie Informationssicherheit tatsächlich funktioniert?

Überblick

Viele Organisationen können ihre Annex-A-Massnahmen beschreiben, tun sich aber schwer damit aufzuzeigen, weshalb jede Massnahme gilt, wie sie umgesetzt ist und ob sie über Standorte, Teams und Lieferanten hinweg konsistent wirkt. Das führt zu einem Auditmuster von «Politikanachweisen» ohne operativen Beleg und zu wiederholten Feststellungen, die Symptome tiefer liegender Systemschwächen sind.

Dieses normspezifische Auditmodul fokussiert auf die Anwendbarkeit und Begründung von Annex-A-Massnahmen über die Erklärung zur Anwendbarkeit, auf Nachweiserwartungen je Massnahmenthema und auf typische systemische ISMS-Fehler. Es setzt voraus, dass die Grundlagen der Informationssicherheit anderweitig bereits behandelt wurden, und wiederholt keine generische Auditpraxis; es wendet Auditbeurteilung auf den Massnahmenkatalog von ISO/IEC 27001 an – für interne Audits und Audits durch Dritte, etwa Zertifizierungsstellen oder unabhängige Nachweisanbieter.

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

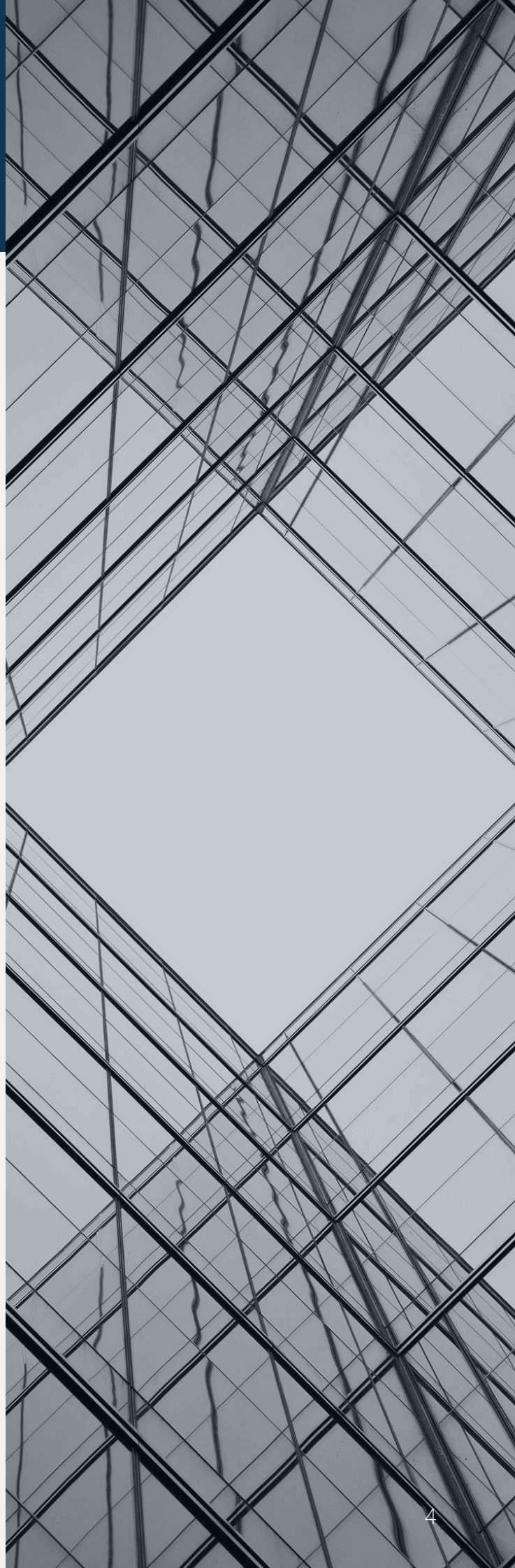
Ist dieses Modul für Sie das Richtige?

Es passt gut für Sie, wenn Sie...

- prüfen wollen, ob Annex-A-Massnahmen in der Praxis wirken und nicht nur auf dem Papier.
- die Anwendbarkeit und Begründung von Massnahmen über die Erklärung zur Anwendbarkeit testen möchten.
- Massnahmenaussagen entlang von Politik, Prozess, Konfiguration und Aufzeichnungen End-to-End nachverfolgen.
- die nachweisbasierte Beurteilung über verschiedene Massnahmenthemen hinweg stärken wollen.
- Auditfeststellungen suchen, die systemische Schwächen statt blosse Lücken in Massnahmenlisten aufzeigen.

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

- primär Sicherheitsmassnahmen entwerfen, umsetzen oder verbessern möchten.
- Grundlagen zu Massnahmentheorie oder technischer Umsetzung erwarten.
- Audits bevorzugen, die sich auf Dokumentation oder Politikkonsistenz beschränken.
- formell korrekte, aber schwache Massnahmenaussagen nicht hinterfragen wollen.



Lernergebnisse

Zentrale Lernergebnisse

- Anwendbarkeitsentscheidungen für Annex-A-Massnahmen mit konsistenten Kriterien zur Qualität der Begründung und zum Geltungsbereich hinterfragen
- Aussagen zu Massnahmen, Umsetzung und Betrieb unterscheiden und erkennen, welcher Nachweis fehlt
- Erwartete Nachweisarten je Annex-A-Massnahmenthema identifizieren

Zusätzliche Fähigkeiten

- Praktische, nachvollziehbare Nachweiswege von der Absicht einer Massnahme bis zum operativen Beleg über Funktionen und Lieferanten hinweg aufbauen
- Wiederkehrende systemische ISMS-Schwachstellen hinter wiederholten Problemen mit Massnahmen erkennen
- Auditbeurteilung für Annex A in internen Audits und in Nachweiskontexten durch Dritte anwenden, ohne in eine reine Listenprüfung zurückzufallen

Agenda

Annex A im Auditkontext

Wie Annex-A-Massnahmen genutzt werden, um Nachweisbarkeit und Wirkung zu beurteilen, und nicht nur als Liste vorhandener Dokumente

Anwendbarkeit und Begründung von Massnahmen

Wie sich die Glaubwürdigkeit von Einschlüssen, Ausschlüssen und Anpassungen in der Erklärung zur Anwendbarkeit sowie schwache Begründungen als Nachweislücken zeigen

Nachweiserwartungen je Massnahmenthema (ISO/IEC 27001)

Wie organisatorische Massnahmen, personenbezogene Massnahmen und technologische Massnahmen zu betrachten sind, mit Fokus auf aussagekräftige auditrelevante Signale

Physische Massnahmen in realen Umgebungen

Wie Standortrealität, Gemeinschaftsflächen, Besucherhandhabung und Bewegungen von Assets zu beurteilen sind, einschliesslich Schnittstellen und Bruchstellen zwischen physischen und technischen Massnahmen

Eine Massnahme End-to-End nachverfolgen

Wie eine einzelne Massnahmenaussage über Politik, Prozess, Konfiguration und Aufzeichnungen hinweg verfolgt wird, inklusive Schnittstellen zu IT, HR, Facilities, Lieferanten und geteilten Plattformen

Massnahmenpakete auf dem Papier und Muster der Drift

Wie deklarierte Massnahmen ohne operative Verantwortung, fragmentierte Umsetzung über Standorte oder Werkzeuge und ein Drift in der Risikobehandlung erkannt werden, wenn sich Erklärung zur Anwendbarkeit und Realität über die Zeit auseinanderentwickeln

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
- Sammlung typischer Schwachstellen
- KI-Prompt-Sammlung

Bestätigung

- Teilnahmebestätigung

Vorbereitungshinweise

Vorausgesetzter Hintergrund

Dieses Modul setzt Folgendes voraus:

- Verständnis auf Auditorenstufe für Nachweis, angemessene berufliche Sorgfalt und Disziplin bei Feststellungen (Auditpraxis wird hier nicht erneut vermittelt)
- Arbeitskenntnisse der Struktur von ISO/IEC 27001, einschliesslich der Rolle der Erklärung zur Anwendbarkeit und der Annex-A-Massnahmen
- Grundlagen der Informationssicherheit, zum Beispiel Zugriffskontrolle, Protokollierung, Änderungsmanagement und Sicherheitsvorfallbehandlung, als Ausgangsbasis

Vorbereitungsmodule

Grundlagen (je nach Vorwissen)

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

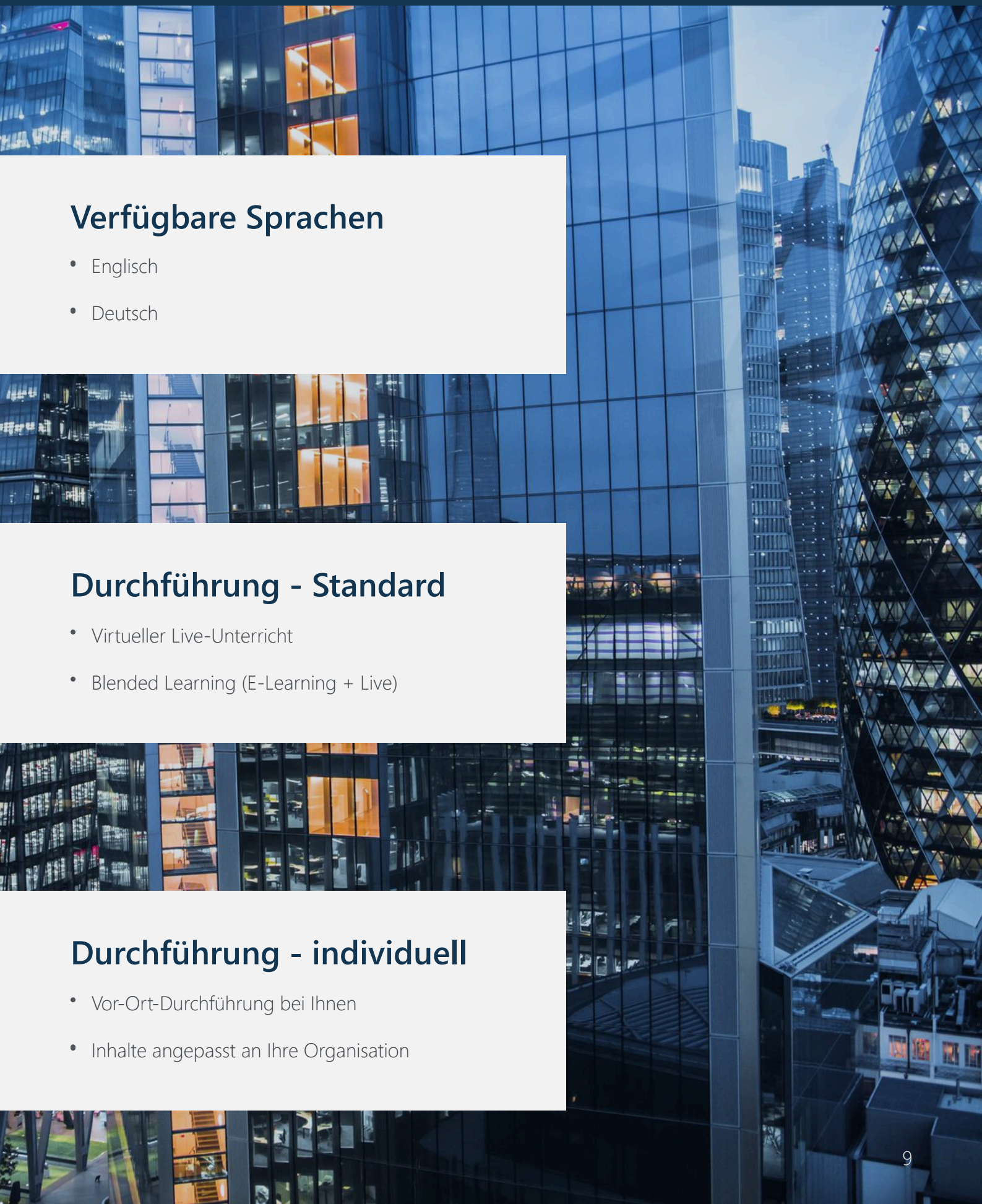
- Audit-Grundsätze
- Informationssicherheitsmassnahmen verstehen

Unterstützend (optional)

Hilfreich, aber nicht erforderlich, um wirksam teilnehmen zu können

- Betriebliche Steuerung auditieren

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