Halderstone

Trainingsmodul

# ISMS: Geltungsbereich & SoA

ISMS-Geltungsbereich und Grenzen klar definieren und eine belastbare Erklärung zur Anwendbarkeit (SoA) pflegen

## Ist der Geltungsbereich Ihres ISMS unklar, sodass Grenzen und Entscheidungen zur Anwendbarkeit nicht belastbar sind?

# Überblick

Schwache Definitionen des Geltungsbereichs und schlecht begründete Entscheidungen zur Anwendbarkeit untergraben die Glaubwürdigkeit eines Informationssicherheitsmanagementsystems.

Dieses Trainingsmodul führt durch das Formulieren einer belastbaren Geltungsbereichsaussage, das Identifizieren von Schnittstellen und Abhängigkeiten sowie das Verknüpfen der Ergebnisse aus der Risikobehandlung mit Entscheidungen zur Anwendbarkeit von Steuerungsmassnahmen. Es zeigt, wie eine Erklärung zur Anwendbarkeit mit Begründung und Umsetzungsstand aufgebaut wird und wie Geltungsbereich und SoA über die Zeit gepflegt werden. Unterschiede zwischen dokumentierter und gelebter Umsetzung werden hervorgehoben, um Lücken zwischen Papier und Praxis zu vermeiden.

# 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)

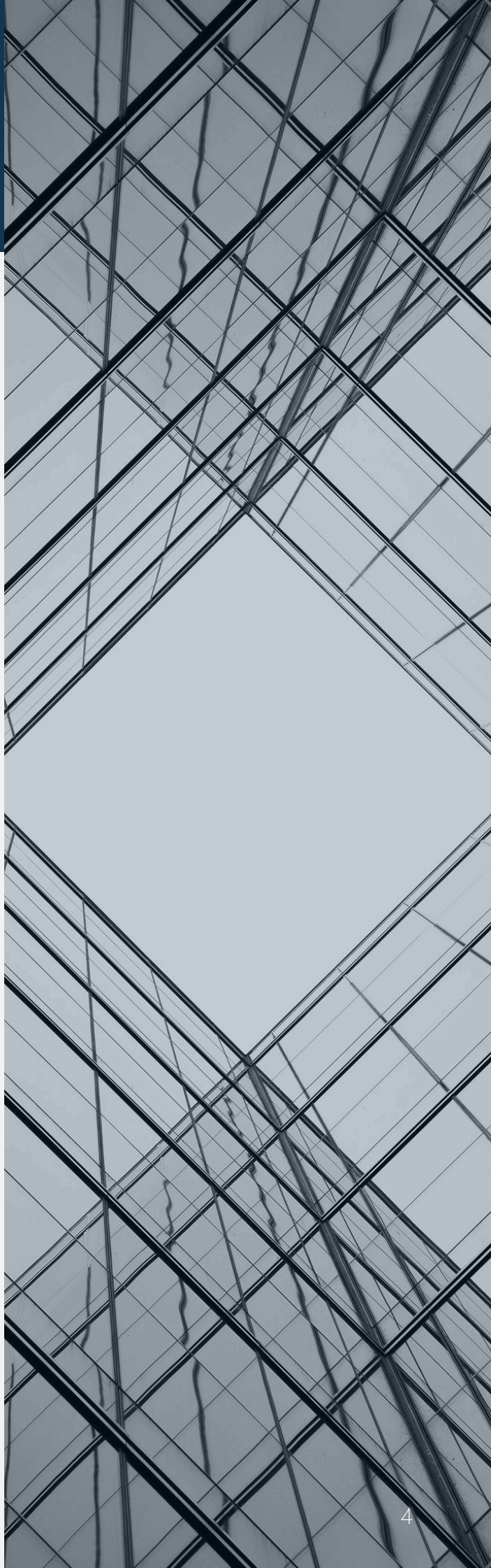
# Ist dieses Modul für Sie das Richtige?

## Es passt gut für Sie, wenn Sie...

- für das Definieren, Pflegen oder Verteidigen des Geltungsbereichs eines ISMS verantwortlich sind.
- mit unklaren, kopierten oder instabilen Erklärungen zur Anwendbarkeit zu tun haben.
- belastbare Entscheidungen zu Geltungsbereich und SoA für Audits und Sicherheitsvorfälle benötigen.
- die Grenzen des ISMS mit realen organisatorischen, technischen oder Lieferantenbeziehungen abstimmen müssen.
- wollen, dass Entscheidungen zum Geltungsbereich und zur Anwendbarkeit bei Veränderungen im Unternehmen gültig bleiben.

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

- nur einen allgemeinen Überblick über ISO/IEC 27001 suchen.
- einen Kurs zu Risikoanalyse oder zur Umsetzung von Steuerungsmassnahmen erwarten.
- eine reine Einführung anhand von Vorlagen ohne Entscheidungslogik wünschen.
- bereits einen klaren, stabilen und gut begründeten ISMS-Geltungsbereich sowie eine entsprechende SoA betreiben.



# Lernergebnisse

## Zentrale Lernergebnisse

- Einen ISO/IEC 27001-konformen Geltungsbereich mit klaren Grenzen und Begründung formulieren
- Schnittstellen, Abhängigkeiten und Annahmen identifizieren, die den Geltungsbereich beeinflussen
- Ergebnisse aus der Risikobehandlung nutzen, um die Anwendbarkeit von Steuerungsmassnahmen festzulegen und zu begründen

## Zusätzliche Fähigkeiten

- Eine Erklärung zur Anwendbarkeit mit klarer Begründung und Umsetzungsstand strukturieren
- Zwischen dokumentierter Anwendbarkeit und operativer Umsetzung unterscheiden, um Lücken sichtbar zu machen
- Regeln und Auslöser für die Pflege festlegen, damit Geltungsbereich und SoA über die Zeit aktuell bleiben

# Agenda

## Was ISO/IEC 27001 von Geltungsbereich und Grenzen erwartet

Wie die Festlegung des ISMS-Geltungsbereichs als glaubwürdige Abdeckung statt als formaler Ausschluss zu verstehen ist und warum Organigramme, Standorte oder Werkzeuge allein eine Scheinsicherheit erzeugen

## Wie sich die Geltungsbereichslogik auf das ISMS anwenden lässt

Wie sich organisatorischer Kontext, Dienstleistungen und Liefermodelle in ISMS-Grenzen übersetzen lassen, einschliesslich interner Schnittstellen, geteilter Plattformen und externer Anbieter

## Wie eine operativ nutzbare Geltungsbereichsaussage aufgebaut wird

Wie eine Geltungsbereichsaussage klar beschreibt, was einbezogen ist, was ausgenommen ist und welche Schnittstellen bestehen, und wie mehrere Standorte, mehrere Dienstleistungen und Konzernstrukturen ohne Überversprechen abgebildet werden

## Wie aus Entscheidungen zur Risikobehandlung die Anwendbarkeit von Steuerungsmassnahmen abgeleitet wird

Wie Ergebnisse aus der Risikobehandlung als Input für Entscheidungen zur Anwendbarkeit von Steuerungsmassnahmen dienen und was Positionen zu «anwendbar» und «nicht anwendbar» in der Praxis belastbar macht

## Wie die Erklärung zur Anwendbarkeit aufgebaut ist und nachvollziehbar bleibt

Wie die SoA als Entscheidungsnachweis mit Begründung, Umsetzungsstand und Verweisen funktioniert und wie sie mit Politiken, Steuerungsmassnahmen und der gelebten Nachweisrealität konsistent bleibt

## Wie Geltungsbereich und SoA über die Zeit gepflegt werden

Wie organisatorische Veränderungen, Wechsel bei Lieferanten, Plattformänderungen und Sicherheitsvorfälle Aktualisierungen des Geltungsbereichs auslösen und wie Verantwortung und Überprüfungsrhythmus in die Führungsroutine eingebettet werden

## Praxisworkshop

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

# Enthaltene Unterlagen

## Lernunterlagen

- Foliensatz
- Workbook für Teilnehmende

## Vorlagen & Werkzeuge

- Vorlage für die ISMS-Geltungsbereichsaussage
- Canvas für Schnittstellen- und Grenzabgleich
- Checkliste für Geltungsbereichsentscheide
- Vorlage für die Erklärung zur Anwendbarkeit
- Register für Geltungsbereich, SoA und Änderungsanlässe

## Bestätigung

- Teilnahmebestätigung

# Vorbereitungshinweise

## Vorausgesetzter Hintergrund

Dieses Modul setzt voraus, dass die Teilnehmenden die allgemeine Logik von Kontext, Anspruchsgruppen und Grenz- bzw. Geltungsbereichsentscheiden bereits verstehen (verantwortet durch System Foundations ) und mit grundlegenden Praktiken zu dokumentierten Informationen arbeiten können.

Hilfreicher Hintergrund umfasst:

- Vertrautheit mit den Dienstleistungen, Prozessen, dem Liefermodell und den wichtigsten Lieferanten des Unternehmens
- Grundlegende Informationssicherheitskenntnisse (Assets/Dienstleistungen, gängige Kategorien von Steuerungsmassnahmen, Konzepte geteilter Verantwortung)
- Grundlogik von Risiko und Risikobehandlung als Fähigkeit im Managementsystem (die Methode wird hier nicht vermittelt)

## Vorbereitungsmodule

### Grundlagen (je nach Vorwissen)

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

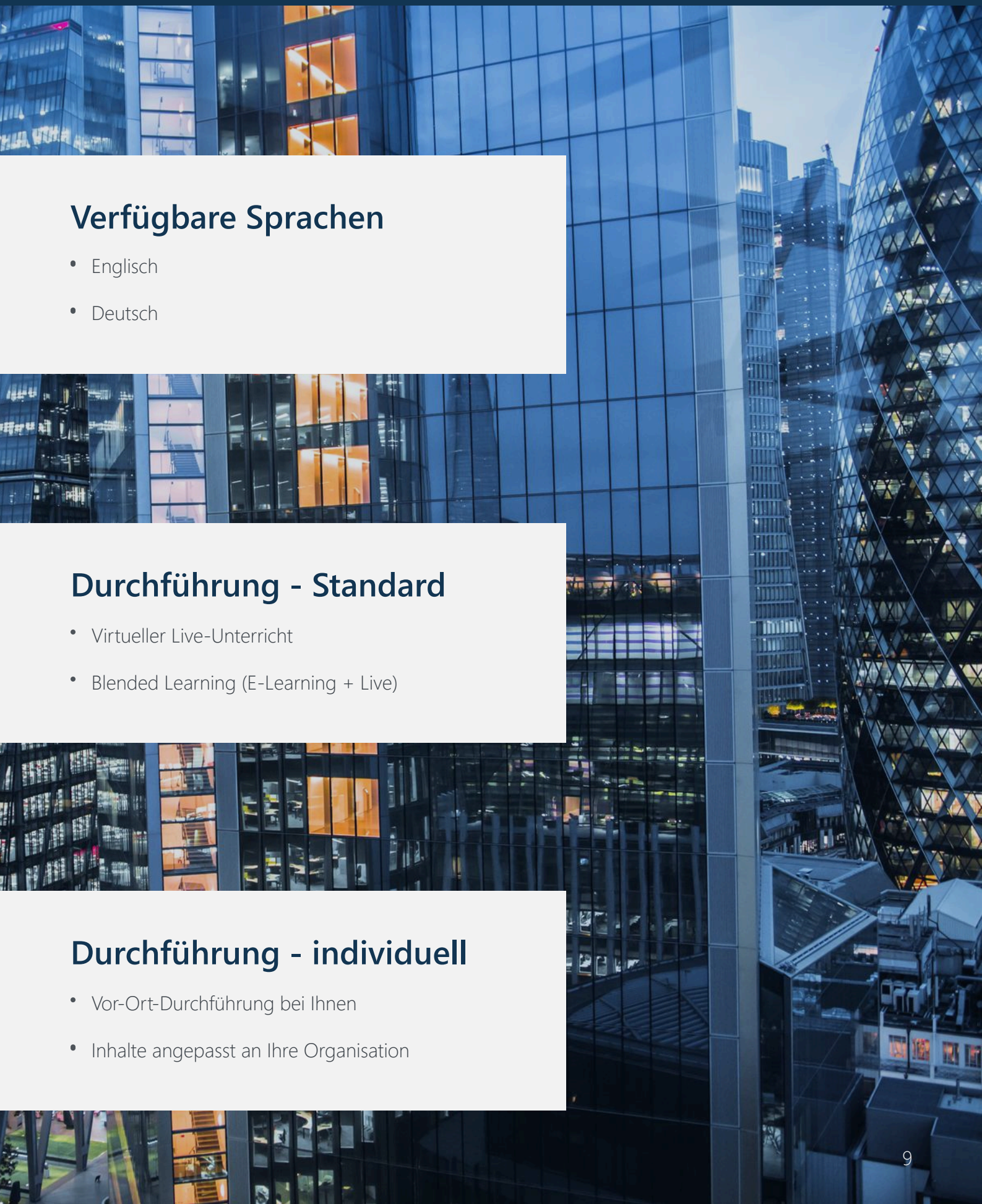
- Kontext & Geltungsbereich

### Unterstützend (optional)

Hilfreich, aber nicht erforderlich, um wirksam teilnehmen zu können

- 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