Lektion 3: Aufbau eines ISMS nach ISO 27001

Praxisschulung am Beispiel der **MediTech Solutions GmbH** — Von der Theorie zur zertifizierungsfähigen Umsetzung

ISO 27001 SCHULUNG | 2026

Agenda

Diese Schulung führt Sie in **10 Modulen** durch alle Anforderungen der ISO 27001 — von der Kontextanalyse bis zur Zertifizierungsvorbereitung. Jedes Modul kombiniert Theorie mit praxisnahen Aufgaben.

01

Module 1-2

Einführung, Unternehmensvorstellung, Kontext der Organisation (Kap. 4)

02

Module 3-4

Führung & Verpflichtung (Kap. 5), Risikomanagement (Kap. 6 + ISO 27005)

03

Module 5-8

Annex A Controls: Organisatorisch, Personell, Physisch, Technologisch

04

Module 9-10

Betrieb & Verbesserung (Kap. 7–10), Zertifizierungsprozess & Zusammenfassung

Vorstellung: MediTech Solutions GmbH

Unternehmensprofil

- **Branche:** Medizintechnik / Healthcare IT
- **Standorte:** Hauptsitz München, Niederlassung Dresden
- **Mitarbeiter:** 180
- **Umsatz:** 28 Mio. EUR (Vorjahr)
- **Produkt:** Patientenmanagementsoftware „MediCare Pro"

Geschäftsmodell

MediTech entwickelt und vertreibt SaaS-basierte Patientenmanagementsoftware für Kliniken, MVZ und Arztpraxen. Das Cloud-Hosting erfolgt bei einem zertifizierten Co-Location-Dienstleister.

Kunden

Kliniken, Medizinische Versorgungszentren (MVZ), niedergelassene Arztpraxen — alle mit höchsten Anforderungen an Datenschutz und Verfügbarkeit.

IT-Landschaft & Geschäftsprozesse

Die IT-Infrastruktur von MediTech bildet die Grundlage für alle ISMS-relevanten Überlegungen — von der Asset-Erfassung bis zur Risikoanalyse.

Prozess	Kernsysteme	Sicherheitsrelevanz
Softwareentwicklung	GitLab, Jenkins CI/CD, Kubernetes	Quellcode, Zugriffsrechte
Kundenbetreuung	Jira Service Desk, Confluence	Kundendaten, Wissensbasis
Vertrieb & Marketing	Microsoft 365, CRM	Geschäftsdaten, E-Mail
Hosting & Betrieb	Co-Location RZ, AWS	Patientendaten, Verfügbarkeit
Administration	SAP Business One, HR-System	Finanz- und Personaldaten

Warum ein ISMS?

Regulatorische Anforderungen

DSGVO verpflichtet zur Absicherung von Patientendaten. DiGA-VO und MDR stellen zusätzliche IT-Sicherheitsanforderungen an Medizinprodukte.

Kundenanforderungen

Kliniken und Klinikverbünde fordern in Ausschreibungen den Nachweis eines zertifizierten ISMS als Zugangsvoraussetzung.

Risikominimierung

Strukturierter Schutz vor Cyberangriffen, Ransomware, Datenverlust und Betriebsunterbrechungen durch einen proaktiven Ansatz.

Wettbewerbsvorteil

Das ISO 27001-Zertifikat schafft nachweisbares Vertrauen bei Bestandskunden und ist ein differenzierendes Merkmal in Neukundenakquise.

ISO 27001 im Überblick

Die ISO/IEC 27001:2022 definiert die **Anforderungen** an ein Informationssicherheits-Managementsystem (ISMS). Sie ist in zwei Bereiche gegliedert:

Kapitel 4–10: ISMS-Anforderungen

- Kap. 4: Kontext der Organisation
- Kap. 5: Führung & Verpflichtung
- Kap. 6: Planung (Risikomanagement)
- Kap. 7: Unterstützung
- Kap. 8: Betrieb
- Kap. 9: Leistungsbewertung
- Kap. 10: Verbesserung

Annex A: 93 Maßnahmen in 4 Kategorien

- A.5 Organisatorisch (37 Controls)
- A.6 Personell (8 Controls)
- A.7 Physisch (14 Controls)
- A.8 Technologisch (34 Controls)

PDCA-Zyklus als Grundprinzip

Plan → Do → Check → Act — kontinuierliche Verbesserung ist keine Option, sondern Pflicht.

Zusammenspiel der Standards

ISO 27001 ist Teil einer Normen-Familie. Für eine wirksame ISMS-Implementierung sollten alle drei Kernstandards zusammen genutzt werden.

ISO 27001

Was muss sein? — Anforderungen an das ISMS. Grundlage für die Zertifizierung. Beschreibt das „Was", nicht das „Wie".

ISO 27002

Wie umsetzt? — Implementierungsleitfaden für alle 93 Controls aus Annex A. Liefert konkrete Handlungsempfehlungen.

ISO 27005

Wie bewerten? — Methodik für das Informationssicherheits-Risikomanagement. Zentral für Kapitel 6 der ISO 27001.

Deutsche Alternative: Das BSI-Grundschutz-Kompendium (BSI 200-1, 200-2, 200-3) bietet eine äquivalente, praxisorientierte Methodik und ist mit ISO 27001 mappingfähig.

Das Projektziel: Zertifizierung

MediTech Solutions hat sich ein ambitioniertes, aber realistisches Ziel gesetzt. Die folgende Roadmap strukturiert das ISMS-Projekt in fünf Phasen.

MODUL 2

Kontext der Organisation (ISO 27001 Kap. 4)

Kapitel 4.1 fordert das systematische Verstehen aller internen und externen Einflussfaktoren, die die Fähigkeit des ISMS beeinflussen, die angestrebten Ergebnisse zu erzielen.

Verstehen der Organisation (4.1)

MediTech muss sowohl interne als auch externe Rahmenbedingungen systematisch erfassen und dokumentieren — sie bilden die Grundlage für Scope und Risikobewertung.

Interne Themen

- Unternehmenskultur und Werte
- Organisationsstruktur und Hierarchien
- IT-Strategie und Digitalisierungsziele
- Ressourcenverfügbarkeit (Budget, Personal)
- Bestehende Prozesse und Systeme

Externe Themen

- Rechtliche Anforderungen (DSGVO, MDR, DiGA)
- Wettbewerbssituation und Markterwartungen
- Technologische Entwicklungen (Cloud, KI)
- Aktuelle Bedrohungslage (Cyberangriffe auf Healthcare)
- Anforderungen der Zertifizierungsstellen

Interessierte Parteien (4.2)

Eine vollständige Stakeholder-Analyse ist Voraussetzung für ein praxisnahes ISMS. Jede Partei bringt spezifische Sicherheitsanforderungen mit, die berücksichtigt werden müssen.

Stakeholder	Anforderungen	Einfluss
Kunden (Kliniken, MVZ)	Datenschutz, Verfügbarkeit, Zertifikatsnachweis	Hoch
Regulierungsbehörden	DSGVO-Compliance, Meldepflichten nach Art. 33	Hoch
Mitarbeiter	Klare Richtlinien, Schulungen, sichere Arbeitsumgebung	Mittel
Lieferanten / Dienstleister	Vertragserfüllung, Sicherheitsanforderungen	Mittel
Geschäftsführung	Risikotransparenz, Kosten-Nutzen-ROI	Hoch

ISMS-Anwendungsbereich (4.3)

Der Scope ist eine der wichtigsten Entscheidungen im ISMS-Aufbau. Er legt fest, was geprüft und zertifiziert wird — und was bewusst ausgeschlossen bleibt.

Der Anwendungsbereich muss definieren:

- Organisatorische Einheiten und Abteilungen
- Eingeschlossene Standorte
- Relevante Geschäftsprozesse
- Informationen, Assets und Systeme
- Schnittstellen zu externen Parteien und Ausschlüsse mit Begründung

Wichtig: Ausschlüsse müssen begründet werden und dürfen keine Pflichten aus ISO 27001 umgehen. Ein zu enger Scope kann die Zertifizierung gefährden.

Scope-Statement MediTech Solutions

Das folgende Scope-Statement bildet die verbindliche Grundlage für alle weiteren ISMS-Aktivitäten bei MediTech Solutions GmbH.

> „Das ISMS der MediTech Solutions GmbH umfasst die Entwicklung, den Betrieb und Support der Patientenmanagementsoftware **‚MediCare Pro'** einschließlich der zugehörigen Cloud-Infrastruktur am Standort München sowie die Entwicklungsabteilung am Standort Dresden."

Eingeschlossen

- Softwareentwicklung (München + Dresden)
- Cloud-Hosting & Betrieb (SaaS)
- Kundenportal mit Patientendaten
- First- und Second-Level-Support

Ausgeschlossen (mit Begründung)

- Marketing-Systeme — keine Patientendaten verarbeitet
- Externe Lieferanteninfrastruktur — per SLA und Vertragsklauseln geregelt
- Verwaltungsstandort Berlin — kein ISMS-relevanter Prozess

AUFGABE 1

Aufgabe 1: Stakeholder-Analyse

Aufgabe

Erstellen Sie ein vollständiges **Stakeholder-Register** für MediTech Solutions GmbH mit allen relevanten interessierten Parteien.

Anforderungen

- Mindestens 8 interessierte Parteien identifizieren
- Anforderungen an die Informationssicherheit dokumentieren
- Einfluss bewerten: hoch / mittel / niedrig

Ergebnis

Dokument: **„Stakeholder-Register"**

AUFGABE 2

Aufgabe 2: ISMS-Scope definieren

Aufgabe

Formulieren Sie ein vollständiges **Scope-Statement** für das ISMS der MediTech Solutions GmbH auf Basis der Unternehmensinformationen.

Anforderungen

- Eingeschlossene Prozesse klar benennen
- Relevante Standorte dokumentieren
- Begründete Ausschlüsse formulieren

Ergebnis

Dokument: **„ISMS-Anwendungsbereich"**

MODUL 3

Führung & Verpflichtung (ISO 27001 Kap. 5)

Informationssicherheit ist Chefsache. Kapitel 5 stellt klar: Ohne aktives Engagement der obersten Leitung kann kein wirksames ISMS entstehen. Die Geschäftsführung ist nicht delegierter Auftraggeber, sondern aktiver Träger des ISMS.

Führungsverantwortung (5.1)

Die ISO 27001 stellt klare Anforderungen an die **oberste Leitung**. Diese Pflichten können nicht an den ISB delegiert werden — sie verbleiben in der Verantwortung der Geschäftsführung.

Gesamtverantwortung übernehmen

Die GF trägt die Letztverantwortung für Wirksamkeit und Angemessenheit des ISMS.

Ressourcen bereitstellen

Budget, Personal und Infrastruktur müssen explizit für das ISMS genehmigt werden.

IS-Leitlinie genehmigen & kommunizieren

Die Leitlinie muss von der GF unterzeichnet und aktiv im Unternehmen kommuniziert werden.

Kontinuierliche Verbesserung fördern

ISMS-Ergebnisse werden in der Managementbewertung diskutiert — mindestens jährlich.

Informationssicherheitspolitik (5.2)

Die IS-Leitlinie ist das **Fundament** des ISMS. Sie gibt die strategische Richtung vor und schafft die normative Grundlage für alle nachgelagerten Richtlinien und Maßnahmen.

Inhaltliche Anforderungen

- Geeignet für den Unternehmenszweck
- Informationssicherheitsziele benennen
- Verpflichtung zur Erfüllung von Anforderungen
- Verpflichtung zur kontinuierlichen Verbesserung

Formale Anforderungen

- Als dokumentierte Information verfügbar
- Intern kommuniziert (allen Mitarbeitern bekannt)
- Für externe Parteien verfügbar (soweit angemessen)
- Regelmäßig überprüft und aktualisiert

Beispiel: IS-Leitlinie MediTech Solutions

> „Die MediTech Solutions GmbH verpflichtet sich, die **Vertraulichkeit, Integrität und Verfügbarkeit** aller Informationen zu schützen — insbesondere der uns anvertrauten Patientendaten. Wir gewährleisten die Einhaltung aller gesetzlichen, regulatorischen und vertraglichen Anforderungen. Die Geschäftsführung stellt die erforderlichen Ressourcen bereit, fördert eine gelebte Kultur der Informationssicherheit und überprüft die Wirksamkeit des ISMS regelmäßig."

Diese Leitlinie bildet die normative Grundlage für alle Sicherheitsmaßnahmen bei MediTech. Sie ist von der Geschäftsführung zu unterzeichnen und allen Mitarbeitern zugänglich zu machen.

Rollen und Verantwortlichkeiten (5.3)

Klare Verantwortlichkeiten sind Voraussetzung für ein funktionierendes ISMS. Die folgende Übersicht zeigt die Kernanforderungen an die IS-Organisation bei MediTech.

Rolle	Verantwortlichkeiten
Geschäftsführung	Gesamtverantwortung, Ressourcenfreigabe, Leitliniengenehmigung
ISB (Informationssicherheitsbeauftragter)	ISMS-Aufbau und -Koordination, internes Reporting, Normenkonformität
IT-Leitung	Technische Umsetzung der Controls, Systemverantwortung
Fachbereichsleiter	Asset-Ownership, Mitwirkung bei Risikobewertung
Alle Mitarbeiter	Einhaltung von Richtlinien, Meldung von Sicherheitsvorfällen

AUFGABE 3

Aufgabe 3: IS-Leitlinie erstellen

Aufgabe

Erstellen Sie eine praxistaugliche **Informationssicherheitsleitlinie** für die MediTech Solutions GmbH, die von der Geschäftsführung unterzeichnet werden kann.

Anforderungen

- Maximale Länge: 1 Seite
- Konkrete Informationssicherheitsziele benennen
- GF-unterzeichnungsfähige Formulierung

Ergebnis & Zeit

Dokument: **„Informationssicherheitsleitlinie"**

AUFGABE 4

Aufgabe 4: RACI-Matrix entwickeln

Aufgabe

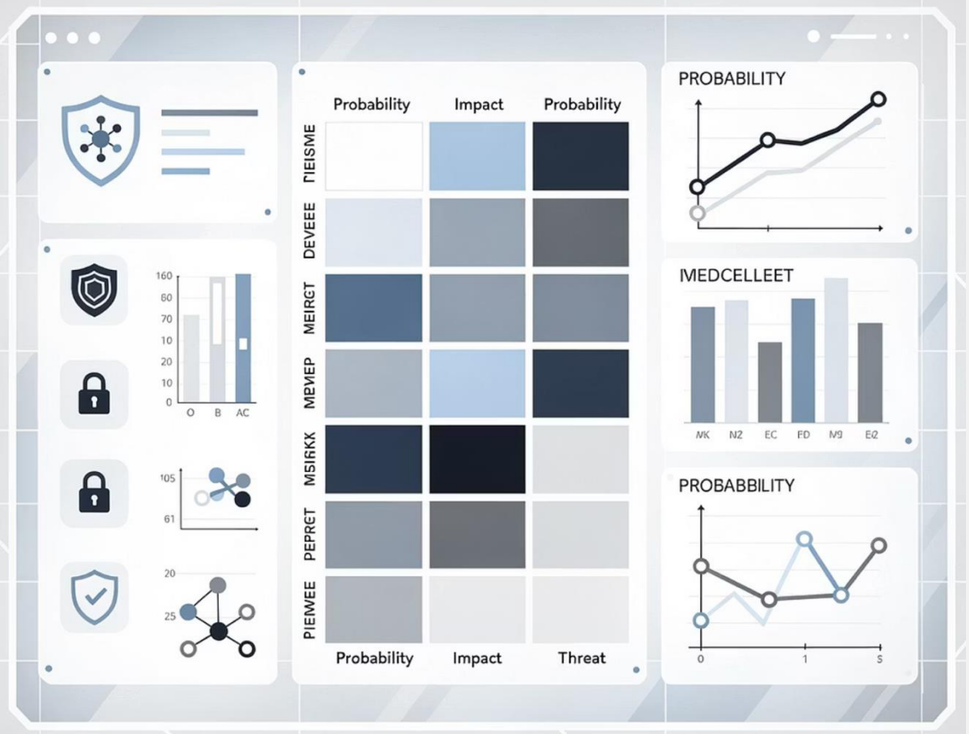
Entwickeln Sie eine vollständige **RACI-Matrix** für die IS-Organisation der MediTech Solutions GmbH, die alle wesentlichen ISMS-Aktivitäten abdeckt.

Anforderungen

- Mindestens 10 Aktivitäten (z.B. Risikobewertung, Schulung, Audit, Incident Management)
- Rollen: GF, ISB, IT-Leitung, Fachabteilungen, HR
- RACI-Logik korrekt anwenden: Responsible, Accountable, Consulted, Informed

Ergebnis & Zeit

Dokument: **„RACI-Matrix IS-Organisation"**



MODUL 4

Planung: Risikomanagement (Kap. 6 + ISO 27005)

Risikoorientierung ist das Herzstück der ISO 27001. Kapitel 6 in Verbindung mit ISO 27005 liefert den methodischen Rahmen für eine systematische, nachvollziehbare Risikobeurteilung und -behandlung.

Risikomanagement-Prozess (ISO 27005)

Kontext

Rahmenbedingungen festlegen

Identifikation

Assets und Bedrohungen erfassen

Analyse

Wahrscheinlichkeit × Auswirkung

Bewertung

Risiken priorisieren

Der Risikomanagement-Prozess ist kein einmaliges Projekt, sondern ein kontinuierlicher Zyklus. ISO 27005 liefert die Methodik, ISO 27001 Kapitel 6 die normativen Anforderungen dazu.

Risiken & Chancen (6.1.1)

ISO 27001 fordert nicht nur die Betrachtung von Risiken, sondern auch die Identifikation von Chancen — ein Aspekt, der im Tagesgeschäft oft unterbewertet wird.

Risiken für MediTech

- Cyberangriffe und Ransomware auf Patientendaten
- Systemausfälle und ungeplante Datenverluste
- Compliance-Verstöße (DSGVO, MDR, DiGA-VO)
- Reputationsschäden durch Sicherheitsvorfälle
- Lieferantenausfälle (Cloud-Provider)

Chancen durch das ISMS

- Wettbewerbsvorteil durch ISO 27001-Zertifikat
- Verbesserte Prozesseffizienz durch klare Strukturen
- Höheres Vertrauen bei Kunden und Partnern
- Bessere Versicherungskonditionen (Cyber-Police)
- Grundlage für weiteres Wachstum und Internationalisierung

Risikobeurteilung (6.1.2)

Die Risikobeurteilung erfolgt in drei aufeinander aufbauenden Schritten. Alle Schritte sind zu dokumentieren und müssen nachvollziehbar und reproduzierbar sein.

Risikoidentifikation

Was kann passieren? Welche Assets, Bedrohungen und Schwachstellen sind vorhanden?

Risikoanalyse

Wie wahrscheinlich ist der Eintritt? Wie schwer wären die Auswirkungen?

Risikobewertung

Ist das Risiko akzeptabel oder besteht Handlungsbedarf? Priorisierung anhand definierter Kriterien.

Asset-Inventar: Informationswerte bei MediTech

Das Asset-Register ist die Grundlage jeder Risikoanalyse. Ohne vollständige Kenntnis der zu schützenden Werte ist kein wirksames ISMS möglich.

Asset-Typ	Beispiele MediTech	Kritikalität
Information	Patientendaten, Quellcode, Verträge, Lizenzschlüssel	Sehr hoch
Software	MediCare Pro, Datenbanken, APIs, Betriebssysteme	Hoch
Hardware	Server, Laptops, Netzwerkgeräte, Speichermedien	Hoch
Dienste	Cloud-Hosting, E-Mail, VPN, CI/CD-Pipeline	Hoch
Personal	Entwickler, Admins, Support, Schlüsselpersonen	Mittel–Hoch

Bedrohungen & Schwachstellen

ISO 27005 Anhang C und D bieten umfangreiche Kataloge für Bedrohungen und Schwachstellen. Für MediTech sind folgende Konstellationen besonders relevant:

Typische Bedrohungen

- Ransomware und gezielte Cyberangriffe auf Healthcare
- Phishing und Social Engineering gegen Mitarbeiter
- Insider-Bedrohungen (unbeabsichtigt oder böswillig)
- Naturkatastrophen und Infrastrukturausfälle
- Hardwareausfall und Datenverlust ohne Backup

Typische Schwachstellen

- Fehlende oder verzögerte Patch-Prozesse
- Schwache oder wiederverwendete Passwörter
- Unzureichend geschulte Mitarbeiter
- Unverschlüsselte Datenspeicherung und -übertragung
- Fehlende Netzwerksegmentierung

Risikoeinschätzung: Methodik

MediTech verwendet eine quantitative Bewertungsskala. Das Risikoniveau ergibt sich als Produkt aus Eintrittswahrscheinlichkeit und Schadensausmaß.

Eintrittswahrscheinlichkeit

Bezeichnung	Wert
Selten	1
Unwahrscheinlich	2
Möglich	3
Wahrscheinlich	4
Fast sicher	5

Schadensausmaß

Bezeichnung	Wert
Unbedeutend	1
Gering	2
Mittel	3
Hoch	4
Kritisch	5

Formel: Risikowert = Eintrittswahrscheinlichkeit × Schadensausmaß (Skala 1–25)

Risikomatrix: Bewertung und Akzeptanzgrenzen

Die farbcodierte Risikomatrix visualisiert alle identifizierten Risiken und erleichtert die Priorisierung von Maßnahmen. MediTech hat folgende Akzeptanzgrenzen definiert:

🟢 Akzeptabel (1-4)

Risiko wird akzeptiert und dokumentiert. Keine unmittelbaren Maßnahmen erforderlich. Regelmäßige Überprüfung im Risikoregister.

🟡 Moderat (5-12)

Risikobehandlung wird empfohlen. Maßnahmen in der Planung berücksichtigen.

🔴 Kritisch (15-25)

Sofortmaßnahmen erforderlich. Eskalation an Geschäftsführung. Keine Akzeptanz ohne explizite GF-Entscheidung und Dokumentation.

Risikobehandlung (6.1.3)

Nach der Bewertung muss für jedes nicht akzeptable Risiko eine Behandlungsoption gewählt werden. ISO 27005 kennt vier grundlegende Optionen:

Statement of Applicability (SoA)

Das **Statement of Applicability** ist eines der zentralen Pflichtdokumente der ISO 27001. Es dokumentiert für alle 93 Annex-A-Controls die Entscheidung und den Umsetzungsstand.

Control	Anwendbar	Begründung	Implementierungsstand
A.5.1 IS-Leitlinien	Ja	Normative Pflicht, Grundlage des ISMS	In Erstellung
A.8.7 Malware-Schutz	Ja	Endpoint-Bedrohungen auf allen Geräten	Umgesetzt (Sophos)
A.7.4 Phys. Überwachung	Teilweise	Nur Serverraum München, nicht Dresden	Geplant

Das SoA ist ein Pflichtdokument der Zertifizierung. Es verknüpft die Ergebnisse der Risikobehandlung mit den gewählten Controls und weist nach, dass alle relevanten Risiken adressiert wurden.

AUFGABE 5

Aufgabe 5: Asset-Inventar aufbauen

Aufgabe

Erstellen Sie ein vollständiges **Asset-Register** für MediTech Solutions, das alle ISMS-relevanten Informationswerte erfasst und bewertet.

Anforderungen

- Mindestens 15 Assets in 5 Kategorien
- Asset-Owner (verantwortliche Person/Rolle) zuordnen
- Kritikalität bewerten: hoch / mittel / niedrig

Ergebnis & Zeit

Dokument: **„Asset-Register"**

AUFGABE 6

Aufgabe 6: Risikoanalyse durchführen

Aufgabe

Führen Sie eine strukturierte **Risikoanalyse** für fünf kritische Assets von MediTech durch und dokumentieren Sie die Ergebnisse im Risikoregister.

Anforderungen

- Bedrohungen und Schwachstellen je Asset identifizieren
- Eintrittswahrscheinlichkeit und Schadensausmaß bewerten (Skala 1–5)
- Risikowert berechnen und in Matrix einordnen
- Behandlungsoptionen vorschlagen

Ergebnis & Zeit

Dokument: **„Risikoregister"**

AUFGABE 7

Aufgabe 7: SoA-Entwurf erstellen

Aufgabe

Erarbeiten Sie einen Auszug aus dem **Statement of Applicability** für MediTech Solutions auf Basis der Controls A.5.1 bis A.5.10.

Anforderungen

- Anwendbarkeit jedes Controls bewerten (Ja / Nein / Teilweise)
- Begründung für jede Entscheidung dokumentieren
- Konkrete Umsetzungsmaßnahmen vorschlagen

Ergebnis

Dokument: **„Statement of Applicability (Auszug)"**

MODUL 5

Controls: Annex A im Überblick

Die ISO 27001:2022 definiert in Annex A insgesamt **93 Controls** in vier Kategorien. Das Statement of Applicability legt fest, welche Controls für MediTech anwendbar sind.

37

A.5 Organisatorisch

Richtlinien, Rollen, Asset-Management, Lieferanten, Incident

8

A.6 Personell

Einstellung, Schulung, Awareness, NDAs, Remote Work

14

A.7 Physisch

Zutritt, Umgebungssicherheit, Geräte, Entsorgung

34

A.8 Technologisch

IT-Sicherheit, Kryptografie, Entwicklung, Logging

Organisatorische Controls A.5.1–A.5.8

Diese Controls bilden das organisatorische Fundament des ISMS. Sie regeln Grundsätze, Verantwortlichkeiten und die strategische Einbettung von Informationssicherheit in das Unternehmen.

A.5.1 IS-Leitlinien

Definiert und genehmigt durch die Geschäftsführung. Bildet die normative Grundlage für alle Sicherheitsmaßnahmen.

A.5.2–A.5.4 Rollen & Leitung

IS-Rollen und Verantwortlichkeiten, Aufgabentrennung, Führungsverantwortung im täglichen Betrieb.

A.5.5–A.5.7 Kontakte & Intelligence

Behördenkontakte, Interessensgruppen, Threat Intelligence — proaktive Informationsgewinnung zur Bedrohungsabwehr.

A.5.8 IS im Projektmanagement

Informationssicherheit muss von Beginn an in alle Projekte integriert werden — kein Nachsatz, sondern Bestandteil.

Organisatorische Controls A.5.9–A.5.23

Dieser Bereich adressiert das **Asset-Management**, die **Zugangssteuerung** und das **Lieferantenmanagement** — drei Kernthemen für MediTech mit Cloud-Infrastruktur und Patientendaten.

A.5.9–A.5.14: Asset- & Informationsmanagement

Asset-Inventar, Eigentumsregelung, akzeptable Nutzung, Rückgabe von Assets, Informationsklassifizierung und -kennzeichnung sowie Handhabung von Informationen.

A.5.15–A.5.18: Zugangs- & Identitätsmanagement

Zugangskontrollrichtlinie, Identitätsverwaltung, Authentisierungsinformationen, Zugriffsrechte — besonders kritisch für privilegierte Konten im Cloud-Umfeld.

A.5.19–A.5.23: Lieferanten & Cloud-Dienste

Informationssicherheit in Lieferantenbeziehungen, Sicherheitsanforderungen in Verträgen, Überwachung und Management von Cloud-Diensten (besonders relevant für MediTech's Co-Location und AWS).

Organisatorische Controls A.5.24–A.5.37

Der letzte Block der organisatorischen Controls umfasst **Incident Management**, **Business Continuity** und **Compliance** — operativ unverzichtbare Bereiche für einen SaaS-Anbieter mit regulierten Kundendaten.

A.5.24–A.5.28: Incident Management & Meldewesen

Vorbereitung, Identifikation, Eindämmung, Wiederherstellung und Nachbereitung von Sicherheitsvorfällen. Meldung an Behörden nach Art. 33 DSGVO.

A.5.29–A.5.30: BCM & IKT-Bereitschaft

Business-Continuity-Management und IKT-Bereitschaft für kritische Dienste. Für MediTech besonders relevant bei Cloud-Infrastruktur und Klinik-SLAs.

A.5.31–A.5.37: Compliance, Datenschutz & Audits

Rechtliche und regulatorische Anforderungen, Datenschutz (DSGVO), Audits, unabhängige Prüfung der Informationssicherheit und technische Compliance.

AUFGABE 8

Aufgabe 8: Richtlinienrahmen definieren

Aufgabe

Erstellen Sie ein vollständiges **Richtlinienverzeichnis** für MediTech Solutions, das alle erforderlichen IS-Richtlinien identifiziert und strukturiert.

Anforderungen

- Mindestens 10 erforderliche Richtlinien auflisten
- Zuordnung zu den relevanten Annex-A-Controls
- Gültigkeitsbereich und Verantwortlichen je Richtlinie definieren

Ergebnis

Dokument: **„Richtlinienverzeichnis"**

AUFGABE 9

Aufgabe 9: Klassifizierungsschema entwickeln

Aufgabe

Entwickeln Sie ein praxistaugliches **Informationsklassifizierungsschema** für MediTech Solutions, das den Umgang mit sensiblen Patientendaten klar regelt.

Anforderungen

- 3–4 Klassifizierungsstufen definieren (z.B. Öffentlich, Intern, Vertraulich, Geheim)
- Handhabungsregeln pro Stufe beschreiben (Speicherung, Übertragung, Löschung)
- Konkrete Beispiele für MediTech-Informationen je Stufe angeben

Ergebnis

Dokument: **„Klassifizierungsrichtlinie"**

MODUL 6

Controls: Personelle Maßnahmen (A.6)

Menschen sind sowohl das größte Risiko als auch die stärkste Verteidigungslinie. Die 8 Controls in Kategorie A.6 regeln den gesamten Mitarbeiterlebenszyklus — von der Einstellung bis zur Kündigung.

Personelle Controls A.6.1–A.6.4

Die ersten vier Controls adressieren den Eintritt ins Unternehmen und legen die Grundlagen für eine sicherheitsbewusste Unternehmenskultur bei MediTech.

1

A.6.1 Sicherheitsüberprüfung

Überprüfung neuer Mitarbeiter und Auftragnehmer vor Einstellung — insbesondere für Rollen mit Zugang zu Patientendaten oder Produktivumgebungen.

2

A.6.2 Arbeitsvertragsbedingungen

Informationssicherheitspflichten müssen explizit in Arbeitsverträgen verankert sein. Verstöße müssen konsequent adressiert werden.

3

A.6.3 IS-Bewusstsein & Schulung

Regelmäßige Awareness-Maßnahmen für alle Mitarbeiter. Rollenspezifische Schulungen für IT, Entwickler und Management.

4

A.6.4 Disziplinarverfahren

Klarer Prozess für den Umgang mit Sicherheitsverstößen — verhältnismäßig, dokumentiert und konsequent angewendet.

Personelle Controls A.6.5–A.6.8

Diese Controls decken kritische Szenarien ab, die in der Praxis häufig vernachlässigt werden: das Ausscheiden von Mitarbeitern, vertragliche Absicherung und das mobile Arbeiten.

A.6.5 Beendigung von Arbeitsverhältnissen

Strukturierter Offboarding-Prozess: Zugriffsrechte entziehen, Equipment zurückfordern, Übergabe dokumentieren. Besonders kritisch bei privilegierten Konten.

A.6.6 Vertraulichkeitsvereinbarungen

NDAs und Verschwiegenheitspflichten müssen vor Informationszugang unterzeichnet sein — auch für Auftragnehmer und Lieferanten mit Systemzugang.

A.6.7 Remote-Arbeit

Sichere Heimarbeitsplätze, VPN-Pflicht, Regelungen zu privaten Geräten (BYOD) und öffentlichen WLAN-Netzwerken für alle MediTech-Mitarbeiter.

A.6.8 Meldung von Sicherheitsereignissen

Einfacher, niederschwelliger Meldeprozess für Mitarbeiter. Keine Bestrafung für gutgläubige Meldungen — Sicherheitskultur stärken.

Awareness-Programm bei MediTech

Ein wirksames Awareness-Programm ist kein einmaliges Event, sondern ein kontinuierlicher Prozess. MediTech plant folgendes Jahresprogramm:

Quartal	Maßnahme	Zielgruppe	Format
Q1	Onboarding-Schulung neue Mitarbeiter	Alle Neuzugänge	Präsenz-Workshop
Q2	Phishing-Simulation + Nachschulung	Alle Mitarbeiter	Simulierter Angriff
Q3	Datenschutz-Refresher (DSGVO)	Alle Mitarbeiter	E-Learning
Q4	Social-Engineering-Awareness	Management, IT	Tabletop-Übung

Fortlaufend: Monatlicher Security Newsletter, verpflichtende E-Learning-Module mit Wissenstest und automatischer Dokumentation der Schulungsquote.

AUFGABE 10

Aufgabe 10: Awareness-Plan erstellen

Aufgabe

Erstellen Sie einen vollständigen **Jahres-Awareness-Plan** für MediTech Solutions, der alle Mitarbeitergruppen zielgruppengerecht anspricht.

Anforderungen

- Mindestens 4 Maßnahmen pro Jahr
- Zielgruppenspezifisch: IT-Abteilung, Management, alle Mitarbeiter
- Erfolgsmessung definieren (z.B. Schulungsquote, Phishing-Klickrate)

Ergebnis & Zeit

Dokument: **„Awareness- & Schulungsplan"**

MODUL 7

Controls: Physische Maßnahmen (A.7)

Physische Sicherheit schützt die Infrastruktur vor unbefugtem Zugang, Umweltbedrohungen und materiellen Schäden. Für MediTech mit zwei unterschiedlichen Standorten besonders relevant.

Physische Controls A.7.1–A.7.7

Die ersten sieben Controls definieren den Schutz von Gebäuden, Räumen und Arbeitsbereichen. MediTech muss sowohl den Hauptsitz München als auch die Dresdner Niederlassung abdecken.

- **A.7.1 Physische Sicherheitsperimeter**

  Definierte Sicherheitsbereiche mit klaren Grenzen — Bürogebäude, Serverräume, Entwicklungsbereiche. Unterschiedliche Schutzniveaus je Zone.

- **A.7.2 Physischer Zutritt**

  Zutrittskontrolle durch Chip-Karten, PIN oder biometrische Merkmale. Besucherregistrierung und -begleitung in sicherheitsrelevanten Bereichen.

- **A.7.3–A.7.5 Büros, Überwachung & Umwelt**

  Absicherung von Büros und Serverräumen, physische Kameraüberwachung in kritischen Bereichen, Schutz vor Feuer, Wasser und Stromausfall.

- **A.7.6–A.7.7 Sicherheitsbereiche & Clean Desk**

  Regelungen für das Arbeiten in sensiblen Bereichen. Clean-Desk- und Clear-Screen-Policy für alle Mitarbeiter verbindlich einführen.

Physische Controls A.7.8–A.7.14

Diese Controls adressieren den sicheren Umgang mit Geräten und Infrastruktur — von der sicheren Aufstellung bis zur kontrollierten Entsorgung ausgedienter Hardware.

- **A.7.8–A.7.9 Geräteaufstellung & außer Haus**

  Physische Sicherung von Servern und Netzwerkgeräten. Klare Regelungen für das Mitführen von Geräten außerhalb der Unternehmensräume (Laptops, Smartphones).

- **A.7.10–A.7.11 Speichermedien & Versorgung**

  Regelungen für mobile Datenträger (USB, externe Festplatten), Verschlüsselungspflicht. Absicherung der Stromversorgung und Klimatisierung im Serverraum.

- **A.7.12–A.7.14 Verkabelung, Wartung & Entsorgung**

  Schutz von Datenkabeln vor Abhören und Manipulation. Regelmäßige Gerätewartung. Zertifizierte und datenschutzkonforme Entsorgung oder Wiederverwendung ausgedienter Hardware.

Physische Sicherheit bei MediTech: Standortvergleich

Beide Standorte haben unterschiedliche Sicherheitsprofile und erfordern standortspezifische Maßnahmen im ISMS-Scope.

München – Hauptsitz

- Eigenes Bürogebäude mit Empfang und Rezeption
- Serverraum im Keller mit Klimatisierung
- Zutrittskontrolle per Chip-Karte (3 Zonen)
- Videoüberwachung Eingang und Serverraum
- USV und Notstromversorgung vorhanden

Dresden – Entwicklung

- Gemietete Bürofläche im Shared-Building
- Kein eigener Serverraum — nur Entwickler-Workstations
- Shared-Building-Zugang — eingeschränkte Kontrolle
- Handlungsbedarf: Clean Desk Policy, Fensterschloss, Besuchermanagement

Dresden erfordert besondere Aufmerksamkeit — der eingeschränkte Einfluss auf das Gebäudemanagement muss im ISMS-Scope und Risikoregister berücksichtigt werden.

AUFGABE 11

Aufgabe 11: Zutrittskonzept erarbeiten

Aufgabe

Erstellen Sie ein vollständiges **Zutrittskonzept** für den Standort München der MediTech Solutions GmbH mit klarer Zoneneinteilung und Berechtigungsstruktur.

Anforderungen

- Zoneneinteilung definieren: öffentlich / intern / eingeschränkt / Hochsicherheit
- Zutrittsberechtigungen nach Rollen zuordnen
- Besucherregelungen und Begleitpflicht festlegen

Ergebnis

Dokument: **„Zutrittsrichtlinie"**

MODUL 8

Controls: Technologische Maßnahmen (A.8)

Mit 34 Controls ist A.8 die umfangreichste Kategorie des Annex A. Sie deckt das gesamte Spektrum der IT-Sicherheit ab — von Endgeräten über Netzwerke bis hin zur sicheren Softwareentwicklung.

Technologische Controls A.8.1–A.8.12

Endgeräte & Zugriffsrechte

- A.8.1 Benutzerendgeräte (MDM, Verschlüsselung)
- A.8.2 Privilegierte Zugriffsrechte (PAM)
- A.8.3 Informationszugang (Need-to-know)
- A.8.4 Quellcode-Zugang (Git-Berechtigungen)
- A.8.5 Sichere Authentisierung (MFA)
- A.8.6 Kapazitätsmanagement

Schutz & Härtung

- A.8.7 Malware-Schutz (EDR/Antivirus)
- A.8.8 Schwachstellenmanagement (Patch-Prozess)
- A.8.9 Konfigurationsmanagement (Hardening)
- A.8.10 Datenlöschung (sichere Löschverfahren)
- A.8.11 Datenmaskierung (Pseudonymisierung)
- A.8.12 Data Leakage Prevention (DLP)

Technologische Controls A.8.13–A.8.24

Dieser Block adressiert den laufenden Betrieb: **Datensicherung, Monitoring und Netzwerksicherheit** sind für MediTech als SaaS-Anbieter mit Patientendaten besonders kritisch.

A.8.13–A.8.16: Backup, Redundanz & Logging

Regelmäßige Datensicherung (3-2-1-Regel), Redundanz für kritische Systeme, zentrales Log-Management und kontinuierliches Monitoring auf Anomalien.

A.8.17–A.8.20: Systemadministration & Software

Zeitsynchronisation (NTP), Kontrolle privilegierter Systemwerkzeuge, restriktive Software-Installationsrichtlinien — nur freigegebene Software darf installiert werden.

A.8.21–A.8.24: Netzwerk & Web-Sicherheit

Netzwerksicherheitsmanagement, Web-Filterung (DNS-basiert), Netzwerksegmentierung zwischen Produktiv-, Entwicklungs- und Administrationsumgebung.

Technologische Controls A.8.25–A.8.34

Für MediTech als Softwareentwickler sind die Controls zum **Secure Development Lifecycle** besonders relevant — Code-Qualität und Sicherheitsanforderungen müssen von Anfang an integriert sein.

A.8.25–A.8.28: Secure Development Lifecycle

Sicherheitsprinzipien im gesamten Entwicklungsprozess: Sicherheitsanforderungen, sichere Systemarchitektur, Coding-Standards und gesicherte Entwicklungsumgebungen in GitLab und Kubernetes.

A.8.29–A.8.31: Tests & Outsourcing

Sicherheitstests (SAST, DAST, Penetrationstests), Sicherheitsanforderungen an ausgelagerte Entwicklung, Trennung von Test- und Produktivumgebungen.

A.8.32–A.8.34: Change, Testdaten & Audit-Logging

Formales Change-Management für Produktivumgebungen, Anonymisierung von Produktionsdaten in Testumgebungen, unveränderliche Audit-Logs für forensische Zwecke.

Technische Umsetzung bei MediTech: Control-Mapping

Die folgende Tabelle zeigt, wie ausgewählte Controls aus A.8 bereits heute bei MediTech umgesetzt sind oder konkret geplant werden:

Control	MediTech-Umsetzung	Tool/System	Status
A.8.7 Malware-Schutz	Endpoint Detection & Response auf allen Geräten	Sophos Intercept X	Umgesetzt
A.8.8 Schwachstellen	Automatisierter Patch-Prozess, monatlicher Scan	Qualys, Ansible	In Einführung
A.8.13 Backup	Täglich inkrementell, vollständig, offline Kopie	Veeam, AWS S3	Umgesetzt
A.8.15 Logging	Zentrales Log-Management mit SIEM-Anbindung	ELK-Stack, Wazuh	Geplant
A.8.23 Web-Filter	DNS-basierte Filterung und URL-Kategorisierung	Cisco Umbrella	Umgesetzt

AUFGABE 12

Aufgabe 12: Backup-Konzept erstellen

Aufgabe

Erstellen Sie ein vollständiges **Backup- & Recovery-Konzept** für alle kritischen Systeme der MediTech Solutions GmbH unter Berücksichtigung der SaaS-Kunden-SLAs.

Anforderungen

- Backup-Strategie auf Basis der **3-2-1-Regel** beschreiben
- RPO (Recovery Point Objective) und RTO (Recovery Time Objective) für verschiedene Systemklassen definieren
- Prozess für regelmäßige Wiederherstellungstests festlegen

Ergebnis & Zeit

Dokument: **„Backup- & Recovery-Konzept"**

AUFGABE 13

Aufgabe 13: Logging-Richtlinie definieren

Aufgabe

Definieren Sie die Anforderungen an das **zentrale Logging und Monitoring** für die IT-Infrastruktur der MediTech Solutions GmbH.

Anforderungen

- Zu protokollierende Ereignisse und Systeme benennen
- Aufbewahrungsfristen definieren (unter Berücksichtigung DSGVO, Art. 5)
- Zugriffsberechtigungen auf Log-Daten und Integritätsschutz regeln

Ergebnis & Zeit

Dokument: **„Logging- & Monitoring-Richtlinie"**

MODUL 9

Betrieb, Überwachung & Verbesserung (Kap. 7-10)

Ein aufgebautes ISMS muss gelebt, gemessen und kontinuierlich verbessert werden. Kapitel 7 bis 10 definieren, wie der laufende Betrieb des ISMS sicherzustellen ist.

Unterstützung (Kapitel 7)

Kapitel 7 stellt sicher, dass das ISMS die nötigen Ressourcen und die organisatorische Infrastruktur erhält, um wirksam zu funktionieren.

7.1 Ressourcen

Personal, Budget und Infrastruktur müssen explizit für das ISMS bereitgestellt und dokumentiert sein.

7.2 Kompetenz

Qualifikationsanforderungen definieren, Schulungsbedarf erheben, Nachweise aufbewahren (z.B. ISO 27001 Lead Implementer-Zertifizierungen).

7.3-7.4 Bewusstsein & Kommunikation

Alle Mitarbeiter müssen die IS-Leitlinie kennen. Interne und externe Kommunikationswege für ISMS-relevante Informationen definieren.

7.5 Dokumentierte Information

Lenkung, Versionierung und Freigabe aller ISMS-Dokumente. Kein Dokument ohne Verantwortlichen, Versionsnummer und Freigabedatum.