ISO/IEC 27001:2022 + Amd 1:2024 Informationssicherheits-Managementsysteme (ISMS)

Informationssicherheit, ISMS, weltweit zertifizierbar

181 Anforderungen. Diese Norm ist akkreditiert zertifizierbar. Stand 07/2026.

ISO/IEC 27001 legt die Anforderungen an ein Managementsystem für Informationssicherheit fest: risikobasiert, dokumentiert, wirksam belegt. Eine Prüfung dagegen ist ein akkreditiertes Zertifizierungsaudit in zwei Stufen (Dokumentenprüfung, dann Wirksamkeitsprüfung vor Ort), gefolgt von jährlichen Überwachungsaudits und einer Rezertifizierung nach drei Jahren.

Betrieb	Datum	Bearbeiter

4 Kontext der Organisation 8

4.1-1 Die externen und internen Themen, die die Fähigkeit der Organisation zur Erreichung der ISMS-Ergebnisse beeinflussen, sind bestimmt und werden gepflegt.

Woran man es festmacht: Belegbar über eine Kontextanalyse als eigenes Dokument oder als Abschnitt im ISMS-Handbuch: Marktumfeld, Kunden- und Vertragslage, Rechtsrahmen (DSGVO, NIS2), Technologiestack, Personalstärke, Abhängigkeit von Cloud-Anbietern. Für kleine Betriebe reicht eine einseitige Tabelle mit Datum und Reviewzyklus, sofern sie in der Managementbewertung erkennbar aktualisiert wird.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

4.1-2 Es ist bestimmt worden, ob der Klimawandel ein für die Organisation relevantes Thema ist. Die Feststellung ist begründet, unabhängig davon, ob sie positiv oder negativ ausfällt.

Woran man es festmacht: Diese Anforderung kam mit Amd 1:2024 hinzu und wird im Audit regelmäßig gezielt abgefragt. In der Kontextanalyse eine eigene Zeile führen: etwa Hitzeperioden mit Auswirkung auf Serverräume und Verfügbarkeit, Extremwetter mit Auswirkung auf Rechenzentren der Cloud-Anbieter, Stromnetzstabilität. Ein begründetes Ergebnis nicht relevant ist zulässig, ein fehlender Eintrag nicht.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

4.2-1 Die für das ISMS relevanten interessierten Parteien sind bestimmt.

Woran man es festmacht: Stakeholder-Liste mit Kunden, Beschäftigten, Auftragsverarbeitern und Unterauftragnehmern, Aufsichtsbehörden, Versicherern, Zertifizierungsstelle, Gesellschaftern. In kleinen Organisationen genügt eine Tabelle mit Partei, Erwartung und Quelle der Erwartung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

4.2-2 Die relevanten Anforderungen dieser interessierten Parteien sind bestimmt, einschließlich etwaiger Anforderungen mit Bezug zum Klimawandel.

Woran man es festmacht: Je Partei die konkrete Quelle nennen: Vertragsklausel, Auftragsverarbeitungsvertrag, Kundenfragebogen, gesetzliche Pflicht. Amd 1:2024 ergänzt hier eine Anmerkung, dass interessierte Parteien Anforderungen mit Klimabezug haben können. Es ist keine eigene Muss-Anforderung, wird im Audit aber routinemäßig angesprochen, etwa Nachhaltigkeitsfragen im Lieferantenaudit eines Großkunden. Eine Zeile in der Stakeholder-Tabelle mit Ergebnis (auch: keine solchen Anforderungen) genügt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

4.2-3 Es ist entschieden und nachvollziehbar, welche dieser Anforderungen über das ISMS behandelt werden.

Woran man es festmacht: Die Stakeholder-Tabelle um eine Spalte erweitern, die auf die adressierende Regelung verweist (Richtlinie, Control, Vertragsanlage). So wird sichtbar, dass Anforderungen nicht nur gesammelt, sondern verarbeitet wurden.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

4.3-1 **Der Anwendungsbereich des ISMS ist festgelegt und berücksichtigt die Themen aus 4.1, die Anforderungen aus 4.2 sowie Schnittstellen und Abhängigkeiten zu Tätigkeiten Dritter.**

Woran man es festmacht: Der Scope benennt Standorte, Organisationseinheiten, Produkte, Systeme und Netzgrenzen. Ausgelagerte Anteile (Hosting, Zahlungsdienstleister, Support) sind als Schnittstelle mit Verantwortungsgrenze beschrieben. Ein künstlich verengter Scope, der Kernprozesse ausklammert, wird von Zertifizierungsstellen zurückgewiesen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

4.3-2 **Der Anwendungsbereich liegt als dokumentierte Information vor und benennt die Grenzen des ISMS eindeutig.** Dokument

Woran man es festmacht: Ein freigegebenes Scope-Dokument mit Version, Datum und Freigabe durch die oberste Leitung. Der Wortlaut dieses Dokuments erscheint später auf dem Zertifikat, deshalb exakt und öffentlich zitierfähig formulieren.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

4.4-1 **Das ISMS ist einschließlich der erforderlichen Prozesse und ihrer Wechselwirkungen eingerichtet, verwirklicht, aufrechterhalten und wird fortlaufend verbessert.**

Woran man es festmacht: Eine Prozesslandkarte oder Prozessliste, die Risikomanagement, Vorfallbehandlung, Änderungsmanagement, Auditierung und Managementbewertung mit Verantwortlichen und Taktung verknüpft. Aktive Belege sind wichtiger als das Diagramm: Tickets, Protokolle, Termine im Kalender.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

5 Führung 8

5.1-1 **Die oberste Leitung übernimmt die Rechenschaftspflicht für die Wirksamkeit des ISMS und stellt sicher, dass Politik und Ziele festgelegt und mit der strategischen Ausrichtung vereinbar sind.**

Woran man es festmacht: Belege sind unterschriebene Freigaben von Politik, Scope und Erklärung zur Anwendbarkeit, Protokolle der Managementbewertung und dokumentierte Budgetentscheidungen. In Kleinstorganisationen ist die Leitung häufig identisch mit dem ISMS-Verantwortlichen, das ist zulässig, muss aber in der Rollendefinition offen benannt sein.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

5.1-2 **Die Anforderungen des ISMS sind in die Geschäftsprozesse integriert und die Bedeutung wirksamer Informationssicherheit wird kommuniziert.**

Woran man es festmacht: Nachweisbar dort, wo Sicherheit nicht als Extraordner lebt: Security-Kriterium in der Definition of Done, Sicherheitsprüfung im Angebots- oder Beschaffungsprozess, ein wiederkehrender Sicherheitspunkt im Team-Meeting-Protokoll.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

5.1-3 **Die Leitung stellt die erforderlichen Ressourcen bereit, unterstützt Personen, die zur Wirksamkeit des ISMS beitragen, und fördert die fortlaufende Verbesserung.**

Woran man es festmacht: Freigegebenes Sicherheitsbudget, Zeitkontingente für Schulungen, Beauftragung externer Auditoren oder Pentester. Ein Verbesserungs- oder Maßnahmenregister mit Einträgen aus mehreren Quartalen zeigt Kontinuität statt Einmalaktion.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

5.2-1 **Eine Informationssicherheitspolitik ist festgelegt, die zum Zweck der Organisation passt und einen Rahmen für die Informationssicherheitsziele bildet.** Dokument

Woran man es festmacht: Ein kurzes freigegebenes Politikdokument, zwei bis drei Seiten reichen. Es benennt Schutzziele, Geltungsbereich, Verantwortlichkeiten und den Grundsatz des risikobasierten Vorgehens. Generische Vorlagentexte ohne Bezug zum eigenen Geschäft fallen im Audit auf.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

5.2-2 **Die Politik enthält die Verpflichtung zur Erfüllung anwendbarer Anforderungen und zur fortlaufenden Verbesserung des ISMS.** Dokument

Woran man es festmacht: Beide Verpflichtungen müssen als expliziter Satz in der Politik stehen, das wird im Stufe-1-Audit wörtlich gegengelesen. Ergänzend auf die dahinterliegenden Prozesse verweisen (Rechtskataster, Verbesserungsregister).

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

5.2-3 **Die Politik ist innerhalb der Organisation kommuniziert und interessierten Parteien, sofern angemessen, zugänglich.** Dokument

Woran man es festmacht: Nachweis über Intranet- oder Wiki-Eintrag mit Leseanforderung, Onboarding-Checkliste mit Bestätigung, oder eine veröffentlichte Kurzfassung auf der Website. Eine Verteilerliste mit Kenntnisnahme-Quittung ist der einfachste belastbare Beleg.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

5.3-1 **Verantwortlichkeiten und Befugnisse für sicherheitsrelevante Rollen sind zugewiesen und innerhalb der Organisation bekannt gemacht.**

Woran man es festmacht: Rollenmatrix (RACI) mit ISMS-Verantwortlichem, Risikoeignern, Asset-Verantwortlichen, Vorfall-Koordinator und Datenschutzverantwortlichem. Bei Ein-Personen- oder Kleinstteams alle Rollen namentlich einer Person zuordnen und die daraus folgende Häufung von Rollen offen dokumentieren, statt sie zu verschleiern.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

5.3-2 **Die Befugnis, die Konformität des ISMS mit der Norm sicherzustellen und über die ISMS-Leistung an die oberste Leitung zu berichten, ist einer Rolle zugewiesen.**

Woran man es festmacht: Bestellschreiben oder Rollenbeschreibung für den ISMS-Verantwortlichen mit ausdrücklichem Berichtsweg zur Leitung. Der Berichtsweg muss durch Protokolle der Managementbewertung tatsächlich belegt sein.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6 Planung 21

6.1.1-1 **Ausgehend von den Themen nach 4.1 und den Anforderungen nach 4.2 sind die Risiken und Chancen bestimmt, die zu behandeln sind, um die beabsichtigten ISMS-Ergebnisse zu erreichen und unerwünschte Auswirkungen zu verhindern.**

Woran man es festmacht: Ein Register, das Kontext-Themen mit Risiken und Chancen verknüpft, getrennt oder integriert im Risikoregister geführt. Wichtig ist die Rückverfolgbarkeit: jedes Thema aus der Kontextanalyse führt sichtbar zu einer Bewertung oder einer begründeten Nichtbetrachtung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6.1.1-2 **Die Maßnahmen zum Umgang mit diesen Risiken und Chancen sind geplant, in die ISMS-Prozesse integriert und ihre Wirksamkeit wird bewertet.**

Woran man es festmacht: Maßnahmenplan mit Verantwortlichem, Termin und Wirksamkeitskriterium. Die Wirksamkeitsbewertung als eigene Spalte führen, sonst fehlt im Audit der Nachweis, dass die Maßnahme nicht nur umgesetzt, sondern auch überprüft wurde.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6.1.2-1 **Ein Prozess zur Informationssicherheits-Risikobeurteilung ist festgelegt und angewendet; er umfasst Kriterien für die Risikoakzeptanz und Kriterien für die Durchführung von Risikobeurteilungen.** Dokument

Woran man es festmacht: Eine Risikomanagement-Richtlinie mit Skalen für Eintrittswahrscheinlichkeit und Auswirkung, definierter Risikomatrix und einer klaren Akzeptanzschwelle. Die Schwelle muss ein Zahlenwert oder eine Zone sein, nicht eine Formulierung wie nach Ermessen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6.1.2-2 **Der Prozess stellt sicher, dass wiederholte Risikobeurteilungen konsistente, gültige und vergleichbare Ergebnisse liefern.**

Woran man es festmacht: Belegbar über eine feste Methodik mit definierten Skalen und über den Vergleich zweier Beurteilungsstände: gleiche Risiken, gleiche Bewertungslogik, nachvollziehbare Abweichungen. Ein Versionsstand des Risikoregisters aus dem Vorjahr ist hier der stärkste Beleg.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6.1.2-3 **Informationssicherheitsrisiken sind identifiziert, um Verlust von Vertraulichkeit, Integrität und Verfügbarkeit im Anwendungsbereich zu erkennen; jedem Risiko ist ein Risikoeigner zugeordnet.**

Woran man es festmacht: Risikoregister mit Bezug auf Werte oder Prozesse, den drei Schutzzielen und einem namentlichen Risikoeigner. Der Risikoeigner muss die Befugnis besitzen, das Risiko zu akzeptieren; in kleinen Organisationen ist das in der Regel die Geschäftsführung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6.1.2-4 **Die identifizierten Risiken sind analysiert: mögliche Folgen, realistische Eintrittswahrscheinlichkeit und daraus abgeleitetes Risikoniveau sind bestimmt.**

Woran man es festmacht: Spalten für Auswirkung, Wahrscheinlichkeit und resultierendes Risikoniveau, jeweils mit kurzer Begründung. Eine Begründung in einem Satz je Risiko verhindert den häufigsten Auditbefund, nämlich Zahlen ohne Herleitung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6.1.2-5 **Die Risiken sind mit den Akzeptanzkriterien verglichen und für die Behandlung priorisiert.**

Woran man es festmacht: Aus dem Risikoregister muss hervorgehen, welche Risiken oberhalb der Akzeptanzschwelle liegen und in welcher Reihenfolge sie behandelt werden. Eine sortierte Ansicht oder eine Prioritätsspalte genügt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6.1.2-6 **Der Prozess der Risikobeurteilung liegt als dokumentierte Information vor.** Dokument

Woran man es festmacht: Die Methodik selbst ist Pflichtdokument, nicht nur ihr Ergebnis. Freigegebene Richtlinie mit Version und Freigabedatum, verlinkt aus dem ISMS-Dokumentenverzeichnis.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6.1.3-1 **Für jedes Risiko oberhalb der Akzeptanzschwelle ist eine geeignete Behandlungsoption ausgewählt (Verringern, Vermeiden, Übertragen oder Akzeptieren).**

Woran man es festmacht: Spalte Behandlungsoption im Risikoregister. Bei Akzeptanz die Begründung und die formale Zustimmung des Risikoeigners festhalten, bei Übertragung den Vertrag oder die Police nennen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.1.3-2 **Alle Maßnahmen, die zur Umsetzung der gewählten Behandlungsoptionen erforderlich sind, sind bestimmt.**

Woran man es festmacht: Maßnahmen konkret und prüfbar formulieren, mit Verantwortlichem und Termin. Verweise auf bereits laufende technische Maßnahmen (MFA-Rollout, Backup-Test) sind zulässig, wenn sie auf ein Ticket oder ein Konfigurationsartefakt zeigen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.1.3-3 **Die bestimmten Maßnahmen sind mit den Controls des Anhangs A abgeglichen worden, um zu prüfen, dass keine notwendige Maßnahme übersehen wurde.**

Woran man es festmacht: Der Abgleich ist ein eigener, nachvollziehbarer Schritt, kein Nebenprodukt. Belegbar durch eine Mapping-Spalte im Risikoregister, die auf Annex-A-Nummern verweist, sowie durch ein Protokoll des Abgleichs mit Datum.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.1.3-4 **Eine Erklärung zur Anwendbarkeit (SoA) liegt vor. Sie bewertet alle 93 Controls des Anhangs A einzeln, benennt je Control die Anwendbarkeit mit Begründung, den Umsetzungsstatus und die Begründung für jeden Ausschluss.** Dokument

Woran man es festmacht: Die SoA ist das zentrale Pflichtdokument und die Landkarte des gesamten Audits. Sie muss lückenlos sein: auch nicht anwendbare Controls erscheinen mit Begründung, nicht als Leerzeile. Empfohlene Spalten: Control-Nummer, Titel, anwendbar ja oder nein, Begründung, Umsetzungsstatus, Verweis auf Richtlinie oder Nachweis, Bezug zum Risiko. Version und Freigabe der Leitung sind zwingend, weil die SoA bei jedem Überwachungsaudit gegen die Realität geprüft wird.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.1.3-5 **Ein Risikobehandlungsplan ist erstellt, der Maßnahmen, Verantwortlichkeiten, Termine und benötigte Ressourcen zusammenführt.** Dokument

Woran man es festmacht: Kann eine eigene Registerkarte der Risikotabelle oder ein Projektboard sein. Entscheidend ist, dass Termine realistisch sind und überschrittene Termine sichtbar nachgesteuert wurden, denn genau das prüft der Auditor.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.1.3-6 **Der Risikobehandlungsplan ist von den Risikoeignern genehmigt und die verbleibenden Restrisiken sind von ihnen formal akzeptiert.** Dokument

Woran man es festmacht: Unterschrift, elektronische Freigabe oder Protokollbeschluss mit Datum. Eine Zeile im Protokoll der Managementbewertung mit Verweis auf die Version des Registers reicht aus, sofern die Version eindeutig ist.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.1.3-7 **Der Prozess der Risikobehandlung liegt als dokumentierte Information vor.** Dokument

Woran man es festmacht: In der Regel im selben Richtliniendokument wie die Risikobeurteilung geregelt. Der Ablauf von der Bewertung über die Optionswahl bis zur Restrisikoakzeptanz muss beschrieben sein.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.2-1 **Informationssicherheitsziele sind für relevante Funktionen und Ebenen festgelegt, stehen im Einklang mit der Politik und sind messbar, soweit praktikabel.**

Woran man es festmacht: Zielblatt mit drei bis sechs Zielen, jeweils mit Kennzahl, Ausgangswert, Zielwert und Frist. Beispiel: Anteil der Systeme mit MFA von 80 auf 100 Prozent bis Quartalsende. Ziele ohne Zahl gelten als nicht messbar.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.2-2 **Die Ziele berücksichtigen die anwendbaren Informationssicherheitsanforderungen sowie die Ergebnisse der Risikobeurteilung und der Risikobehandlung.**

Woran man es festmacht: Im Zielblatt eine Spalte mit Herkunft führen: aus welchem Risiko, welcher Kundenanforderung oder welcher Rechtspflicht das Ziel stammt. Das verhindert beliebig wirkende Ziele.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.2-3 **Die Ziele werden überwacht, kommuniziert und bei Bedarf aktualisiert.**

Woran man es festmacht: Quartalsweise Fortschrittsverfolgung im Zielblatt plus Kommunikation an das Team, etwa als Kurznotiz im Wiki oder als Tagesordnungspunkt im Teammeeting. Historisierte Stände zeigen die Aktualisierung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.2-4 **Die Informationssicherheitsziele liegen als dokumentierte Information vor.** Dokument

Woran man es festmacht: Ein freigegebenes Zieldokument mit Datum reicht. Es darf Teil der Managementbewertung sein, muss dort aber als eigener, wiederauffindbarer Abschnitt existieren.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.2-5 **Für jedes Ziel ist geplant, was getan wird, welche Ressourcen benötigt werden, wer verantwortlich ist, wann es abgeschlossen ist und wie die Ergebnisse bewertet werden.**

Woran man es festmacht: Diese fünf Angaben sind einzeln prüfbar und werden im Audit einzeln abgefragt. Als fünf Spalten im Zielblatt anlegen, dann ist die Konformität auf einen Blick erkennbar.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6.3-1 **Wenn die Organisation Änderungen am ISMS als notwendig erkennt, werden diese geplant durchgeführt.**

Woran man es festmacht: Belegbar über Änderungsanträge, Protokolleinträge oder Tickets, aus denen Anlass, Auswirkungsbetrachtung, Freigabe und Umsetzung hervorgehen. Typische Anlässe in kleinen Betrieben: Wechsel des Cloud-Anbieters, neue Standorte, erste Einstellung von Personal.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

7 Unterstützung 15

7.1-1 **Die für Einrichtung, Verwirklichung, Aufrechterhaltung und fortlaufende Verbesserung des ISMS erforderlichen Ressourcen sind bestimmt und bereitgestellt.**

Woran man es festmacht: Budgetzeile für Sicherheit, Werkzeuglizenzen (Passwortmanager, MDM, Log-Plattform), eingeplante Personentage für ISMS-Pflege und externe Auditleistungen. Ein Rechnungsbeleg oder eine Budgetfreigabe belegt das schneller als jede Prosa.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

7.2-1 **Die erforderliche Kompetenz der Personen, die die Informationssicherheitsleistung beeinflussen, ist bestimmt.**

Woran man es festmacht: Kompetenzmatrix oder Rollenprofile mit erforderlichen Kenntnissen je Rolle, etwa sichere Entwicklung für Entwickler, Vorfallbehandlung für den Koordinator. Bei sehr kleinen Teams eine Zeile je Person genügt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7.2-2 **Die Kompetenz ist auf Grundlage angemessener Ausbildung, Schulung oder Erfahrung sichergestellt.**

Woran man es festmacht: Zertifikate, Kursbestätigungen, Lebensläufe oder dokumentierte Praxiserfahrung. Selbstlernen ist zulässig, wenn es belegt ist, etwa durch Abschlussnachweise von Onlinekursen oder durch bestandene interne Wissenstests.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7.2-3 **Wo Kompetenzlücken bestehen, sind Maßnahmen zu deren Schließung ergriffen und deren Wirksamkeit ist bewertet worden.**

Woran man es festmacht: Schulungsplan mit Soll-Ist-Abgleich und einer Wirksamkeitsprüfung, etwa Testergebnis, Phishing-Simulationsquote oder Beobachtung im Betrieb. Die Wirksamkeitsprüfung wird häufig vergessen und ist ein klassischer Nebenbefund.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7.2-4 **Angemessene dokumentierte Information als Nachweis der Kompetenz liegt vor.** Dokument

Woran man es festmacht: Ein Kompetenz- oder Schulungsordner je Person mit Nachweisen und Datum. In kleinen Betrieben reicht ein Verzeichnis mit abgelegten PDF-Nachweisen und einer Übersichtstabelle.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7.3-1 **Die im Anwendungsbereich tätigen Personen sind sich der Informationssicherheitspolitik bewusst.**

Woran man es festmacht: Kenntnisnahme-Bestätigung beim Onboarding und bei jeder Änderung der Politik, mit Datum und Version. Ein Wiki-Lesebestätigungsfeature oder eine unterschriebene Liste genügt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7.3-2 **Die Personen kennen ihren eigenen Beitrag zur Wirksamkeit des ISMS und den Nutzen einer verbesserten Informationssicherheitsleistung.**

Woran man es festmacht: Schulungsunterlagen und Teilnahmelisten, in denen der Bezug zur eigenen Tätigkeit erkennbar ist. Im Audit werden Mitarbeitende direkt befragt, deshalb konkrete, alltagsnahe Beispiele schulen statt abstrakter Normzitate.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7.3-3 **Die Personen kennen die Konsequenzen einer Nichterfüllung der ISMS-Anforderungen.**

Woran man es festmacht: In Schulungsfolien und Arbeitsanweisungen die Folgen benennen und mit dem Verfahren aus A.6.4 verknüpfen. Auch bei Organisationen ohne Angestellte gilt dies für Auftragnehmer und Freelancer über deren Vertrag.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7.4-1 **Die interne und externe Kommunikation zum ISMS ist bestimmt: worüber, wann, mit wem und auf welche Weise kommuniziert wird.**

Woran man es festmacht: Eine Kommunikationsmatrix mit Zeilen wie Sicherheitsvorfall an Kunden, Meldung an Aufsichtsbehörde binnen 72 Stunden, Statusbericht an Leitung monatlich. Sie ist die Grundlage der Krisenkommunikation und wird nach jedem Vorfall gegengeprüft.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7.5.1-1 **Das ISMS umfasst die von der Norm geforderte dokumentierte Information sowie diejenige, die die Organisation für die Wirksamkeit des ISMS als notwendig bestimmt hat.** Dokument

Woran man es festmacht: Ein Dokumentenverzeichnis, das jedes ISMS-Dokument mit Zweck, Eigentümer, Version und Speicherort führt. Es macht sichtbar, dass die Pflichtdokumente vollständig sind, und ist der schnellste Einstieg für den Auditor.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

7.5.2-1 **Beim Erstellen und Aktualisieren von Dokumenten sind angemessene Kennzeichnung, Format und Medium sichergestellt und es erfolgt eine Überprüfung und Genehmigung auf Angemessenheit.**

Woran man es festmacht: Einheitlicher Dokumentenkopf mit Titel, Version, Datum, Autor und Freigebendem. In Git-basierten Umgebungen erfüllen Pull-Request-Reviews mit Approval die Prüfung und Genehmigung, wenn die Historie unveränderlich ist.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

7.5.3-1 **Dokumentierte Information ist dort verfügbar und geeignet, wo und wann sie benötigt wird.**

Woran man es festmacht: Ein zentraler, für alle Berechtigten erreichbarer Ablageort mit Suchfunktion. Prüfbar durch Stichprobe: eine beliebige Arbeitsanweisung muss in unter einer Minute auffindbar sein.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

7.5.3-2 **Dokumentierte Information ist angemessen geschützt, insbesondere vor Verlust der Vertraulichkeit, unsachgemäßer Verwendung und Verlust der Integrität.**

Woran man es festmacht: Zugriffsrechte auf ISMS-Dokumente nach Rolle, Versionierung mit Historie, Schreibschutz für freigegebene Stände und Backup des Dokumentenablageorts. Der Backup-Nachweis wird hier oft vergessen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

7.5.3-3 **Verteilung, Zugriff, Wiederauffindung, Speicherung, Änderungssteuerung sowie Aufbewahrung und Verfügung über dokumentierte Information sind geregelt.**

Woran man es festmacht: Eine kurze Dokumentenlenkungsregel mit Aufbewahrungsfristen und Löschregeln. Sie muss mit den Rechtspflichten (Handelsrecht, Steuerrecht, DSGVO) abgeglichen sein und ist die Grundlage für A.5.33 und A.8.10.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

7.5.3-4 **Dokumentierte Information externen Ursprungs, die für die Planung und den Betrieb des ISMS notwendig ist, ist gekennzeichnet und gelenkt.**

Woran man es festmacht: Liste externer Dokumente mit Version und Bezugsquelle: Normtexte, Gesetzestexte, Herstellerhärtungsleitfäden, Cloud-Sicherheitsdokumentation, Auftragsverarbeitungsverträge. Ohne Versionsstand ist die Lenkung nicht nachweisbar.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8 Betrieb 8

8.1-1 **Die zur Erfüllung der Informationssicherheitsanforderungen und zur Umsetzung der Maßnahmen aus Kapitel 6 notwendigen Prozesse sind geplant, verwirklicht und gesteuert; Kriterien für die Prozesse sind festgelegt.**

Woran man es festmacht: Betriebshandbuch oder Runbooks mit klaren Kriterien, etwa maximale Zeit bis zum Einspielen kritischer Patches, Freigabekriterien für Deployments, Schwellenwerte für Alarme. Kriterien ohne Zahlen sind im Audit wertlos.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8.1-2 **Dokumentierte Information liegt in dem Umfang vor, der Vertrauen schafft, dass die Prozesse wie geplant durchgeführt wurden.** Dokument

Woran man es festmacht: Betriebsaufzeichnungen als Beleg: Ticket-Historie, CI-Pipeline-Läufe, Patch-Berichte, Backup-Protokolle, Zugriffsreviews. Diese Aufzeichnungen sind der eigentliche Wirksamkeitsnachweis im Stufe-2-Audit.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8.1-3 **Geplante Änderungen werden gesteuert und die Folgen unbeabsichtigter Änderungen werden betrachtet; erforderlichenfalls werden nachteilige Auswirkungen abgemildert.**

Woran man es festmacht: Änderungsprozess mit Freigabe und Rollback-Pfad, verknüpft mit A.8.32. Bei unbeabsichtigten Änderungen (Fehlkonfiguration, versehentliche Rechteausweitung) den Vorfall dokumentieren und die Korrektur nachweisen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8.1-4 **Extern bereitgestellte Prozesse, Produkte und Dienstleistungen, die für das ISMS relevant sind, sind bestimmt und werden gesteuert.**

Woran man es festmacht: Dienstleisterliste mit Kritikalität, Vertragsbezug und Nachweisstand (ISO-27001-Zertifikat des Anbieters, SOC-2-Bericht, Auftragsverarbeitungsvertrag). Für kleine Betriebe ist das der wichtigste Hebel, weil ein Großteil der IT ohnehin extern läuft.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8.2-1 **Risikobeurteilungen werden in geplanten Abständen sowie bei wesentlichen Änderungen oder Vorfällen durchgeführt und berücksichtigen die festgelegten Kriterien.**

Woran man es festmacht: Ein Rhythmus (üblich jährlich) plus definierte Auslöser für außerplanmäßige Beurteilungen. Belegbar über datierte Versionsstände des Risikoregisters und Einträge im Kalender oder Ticketsystem.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8.2-2 **Die Ergebnisse der Risikobeurteilungen sind als dokumentierte Information aufbewahrt.** Dokument

Woran man es festmacht: Historisierte Fassungen des Risikoregisters mit Datum, nicht nur der aktuelle Stand. Wer die Datei nur überschreibt, kann die Entwicklung nicht belegen; Versionierung im Dateisystem oder in Git löst das.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8.3-1 **Der Risikobehandlungsplan wird umgesetzt.**

Woran man es festmacht: Abgleich Plan gegen Realität: erledigte Maßnahmen mit Umsetzungsdatum und konkretem Artefakt (Konfiguration, Richtlinie, Vertrag). Offene Maßnahmen brauchen eine dokumentierte Begründung und ein neues Zieldatum.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8.3-2 **Die Ergebnisse der Risikobehandlung sind als dokumentierte Information aufbewahrt.** Dokument

Woran man es festmacht: Statusberichte oder abgeschlossene Maßnahmenpositionen mit Nachweisverweis. Das Register selbst genügt, wenn Erledigungsdatum und Nachweislink je Zeile geführt werden.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9 Bewertung der Leistung 21

9.1-1 Es ist bestimmt, was überwacht und gemessen wird, einschließlich der Informationssicherheitsprozesse und der Maßnahmen.

Woran man es festmacht: Kennzahlenblatt mit einer überschaubaren Zahl belastbarer Metriken: Patch-Rückstand, Anteil MFA, Zeit bis Vorfallbehebung, Ergebnis des letzten Restore-Tests, offene Findings. Wenige, wirklich erhobene Kennzahlen schlagen eine lange Wunschliste.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.1-2 Die Methoden zur Überwachung, Messung, Analyse und Bewertung sind festgelegt und liefern gültige Ergebnisse.

Woran man es festmacht: Je Kennzahl die Datenquelle und die Berechnungsweise dokumentieren, etwa Auswertung aus dem Schwachstellenscanner oder aus dem Identity-Provider-Report. Nachvollziehbarkeit der Quelle ist der Kern der Gültigkeit.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.1-3 Es ist festgelegt, wann und durch wen überwacht und gemessen wird sowie wann die Ergebnisse analysiert und bewertet werden.

Woran man es festmacht: Im Kennzahlenblatt Spalten für Turnus und Verantwortlichen führen. Ein wiederkehrender Kalendertermin für die Auswertung belegt die Regelmäßigkeit besser als jede Beschreibung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.1-4 Die Ergebnisse der Überwachung und Messung sind als dokumentierte Information aufbewahrt. Dokument

Woran man es festmacht: Archivierte Auswertungen, exportierte Dashboards oder ein fortgeschriebenes Kennzahlenblatt mit Zeitreihe. Eine reine Live-Ansicht ohne Historie erfüllt die Anforderung nicht.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.1-5 Die Informationssicherheitsleistung und die Wirksamkeit des ISMS sind auf Basis der Messergebnisse bewertet.

Woran man es festmacht: Eine schriftliche Bewertung, nicht nur Zahlen: Trend, Ursachen, Handlungsbedarf. Dieser Bewertungstext ist zugleich eine Eingabe für die Managementbewertung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.2.1-1 Interne Audits werden in geplanten Abständen durchgeführt und liefern Informationen darüber, ob das ISMS die eigenen Anforderungen und die Normanforderungen erfüllt und wirksam umgesetzt ist.

Woran man es festmacht: Vor dem Zertifizierungsaudit muss mindestens ein vollständiger interner Auditzyklus über den gesamten Scope abgeschlossen sein. Fehlt er, ist die Zertifizierung nicht erreichbar, das ist einer der häufigsten Stolpersteine bei Erstzertifizierungen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.2.2-1 Ein Auditprogramm ist geplant, eingerichtet und aufrechterhalten; es legt Häufigkeit, Methoden, Verantwortlichkeiten, Planungsanforderungen und Berichterstattung fest und berücksichtigt die Bedeutung der betroffenen Prozesse sowie Ergebnisse vorheriger Audits.

Woran man es festmacht: Ein Mehrjahres-Auditprogramm, das alle Kapitel und alle anwendbaren Controls über den Zertifikatszyklus abdeckt, mit stärkerer Taktung für kritische Bereiche. Eine einfache Tabelle über drei Jahre reicht vollkommen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.2.2-2 **Für jedes Audit sind Auditkriterien und Auditumfang festgelegt.**

Woran man es festmacht: Auditplan je Termin mit Kriterien (Norm, eigene Richtlinien, Verträge) und klarem Umfang. Ein Auditplan von einer Seite je Audit genügt und ist zugleich die Grundlage des Berichts.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.2.2-3 **Die Auditoren sind so ausgewählt und die Audits so durchgeführt, dass Objektivität und Unparteilichkeit sichergestellt sind. Niemand auditiert die eigene Arbeit.**

Woran man es festmacht: Die Unabhängigkeit ist hier die harte Hürde: Wer die Richtlinien geschrieben und die Systeme konfiguriert hat, darf sie nicht selbst auditieren. In sehr kleinen Organisationen bedeutet das praktisch immer einen externen internen Auditor, etwa einen beauftragten Berater oder einen Kollegen aus einem Partnerunternehmen; ein Auditvertrag plus Unabhängigkeitserklärung des Auditors ist der Nachweis. Nur bei ausreichend großen Teams ist eine interne Rochade zwischen Personen ohne Zuständigkeit für den geprüften Bereich möglich, und das ist dann in der Rollenmatrix zu belegen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.2.2-4 **Die Auditergebnisse werden dem relevanten Management berichtet.**

Woran man es festmacht: Auditbericht mit Feststellungen, Abweichungen, Empfehlungen und Verteiler, plus Nachweis der Übergabe an die Leitung, etwa Protokollpunkt oder E-Mail-Übergabe mit Datum.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.2.2-5 **Dokumentierte Information über das Auditprogramm und die Auditergebnisse ist aufbewahrt.** Dokument

Woran man es festmacht: Auditprogramm, Auditpläne, Auditberichte und die daraus abgeleiteten Maßnahmen an einem Ort ablegen. Die Verknüpfung von Feststellung zu Korrekturmaßnahme (Kapitel 10.2) muss durchgängig erkennbar sein.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.3.1-1 **Die oberste Leitung bewertet das ISMS in geplanten Abständen, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.**

Woran man es festmacht: Mindestens jährlich, terminlich vor dem externen Audit. Auch in Kleinstorganisationen muss es ein datiertes, unterschriebenes Protokoll geben, selbst wenn Leitung und ISMS-Verantwortlicher dieselbe Person sind.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.3.2-1 **Die Managementbewertung berücksichtigt den Status der Maßnahmen aus vorherigen Managementbewertungen.**

Woran man es festmacht: Das Protokoll beginnt mit einer Nachverfolgungstabelle der Vorjahresbeschlüsse mit aktuellem Status. Fehlt dieser Rückbezug, gilt die Bewertung als unvollständig.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.3.2-2 **Die Managementbewertung berücksichtigt Änderungen bei den externen und internen Themen, die für das ISMS relevant sind, einschließlich relevanter Aspekte des Klimawandels.**

Woran man es festmacht: Eigener Tagesordnungspunkt mit Verweis auf die aktualisierte Kontextanalyse. Der Klimabezug ist an dieser Stelle nicht eigens im Normtext genannt (Amd 1:2024 ändert nur 4.1 und 4.2), kommt aber über die Änderungen der Themen nach 4.1 hier herein und wird von Auditoren so erwartet. Auch das Ergebnis nicht relevant, unverändert gehört protokolliert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9.3.2-3 **Die Managementbewertung berücksichtigt Änderungen bei den Anforderungen interessierter Parteien, die für das ISMS relevant sind.**

Woran man es festmacht: Neue Kundenanforderungen aus Verträgen und Sicherheitsfragebögen, neue Rechtspflichten, Anforderungen der Zertifizierungsstelle. Als Liste mit Quellenangabe ins Protokoll.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9.3.2-4 **Die Managementbewertung berücksichtigt Rückmeldungen zur Informationssicherheitsleistung, einschließlich Nichtkonformitäten und Korrekturmaßnahmen, Überwachungs- und Messergebnissen, Auditergebnissen und der Erfüllung der Informationssicherheitsziele.**

Woran man es festmacht: Diese vier Blöcke einzeln als Tagesordnungspunkte führen, sonst fehlt im Protokoll später einer davon. Kennzahlenblatt, Auditbericht und Zielblatt als Anlagen beifügen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9.3.2-5 **Die Managementbewertung berücksichtigt Rückmeldungen von interessierten Parteien.**

Woran man es festmacht: Kundenbeschwerden mit Sicherheitsbezug, Ergebnisse von Kundenaudits, Meldungen aus dem Hinweisgeberkanal, Rückmeldungen von Dienstleistern. Auch die Feststellung, dass keine eingegangen sind, wird protokolliert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9.3.2-6 **Die Managementbewertung berücksichtigt die Ergebnisse der Risikobeurteilung und den Status des Risikobehandlungsplans.**

Woran man es festmacht: Aktuelles Risikoregister und Umsetzungsstand des Behandlungsplans als Anlage, mit expliziter Bestätigung der Restrisikoakzeptanz durch die Risikoeigner.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9.3.2-7 **Die Managementbewertung berücksichtigt Möglichkeiten zur fortlaufenden Verbesserung.**

Woran man es festmacht: Ein Tagesordnungspunkt mit konkreten Verbesserungsideen und Entscheidung je Idee. Die angenommenen Ideen wandern als Einträge mit Termin ins Verbesserungsregister.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9.3.3-1 **Die Ergebnisse der Managementbewertung enthalten Entscheidungen zu Chancen für fortlaufende Verbesserung und zu jeglichem Änderungsbedarf am ISMS.**

Woran man es festmacht: Das Protokoll endet mit einem Beschlussteil: Entscheidung, Verantwortlicher, Termin. Ein Protokoll ohne Beschlüsse ist im Audit ein Befund, weil dann die Leitungswirkung fehlt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9.3.3-2 **Dokumentierte Information als Nachweis der Ergebnisse der Managementbewertung ist aufbewahrt.** Dokument

Woran man es festmacht: Unterschriebenes Protokoll mit Datum, Teilnehmenden, Eingaben, Bewertung und Beschlüssen. Es gehört zu den ersten Dokumenten, die eine Zertifizierungsstelle in Stufe 1 anfordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10 Verbesserung 7

10.1-1 **Die Eignung, Angemessenheit und Wirksamkeit des ISMS werden fortlaufend verbessert.**

Woran man es festmacht: Ein Verbesserungsregister mit Einträgen aus mehreren Quellen (Audits, Vorfälle, Ideen, Kennzahlenabweichungen) und sichtbarem Fortschritt über die Zeit. Kontinuität über mehrere Monate ist der Beleg, nicht die Menge der Einträge.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10.2-1 **Beim Auftreten einer Nichtkonformität wird darauf reagiert: sie wird gesteuert und korrigiert und die Folgen werden behandelt.**

Woran man es festmacht: Abweichungsmeldung mit Sofortmaßnahme und Datum. Quellen sind interne Audits, externe Audits, Vorfälle und eigene Feststellungen im Betrieb; alle laufen in dasselbe Register.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10.2-2 **Es wird bewertet, ob Maßnahmen zur Beseitigung der Ursachen erforderlich sind, damit die Nichtkonformität nicht erneut oder an anderer Stelle auftritt; dazu gehört die Prüfung, ob ähnliche Nichtkonformitäten bestehen oder auftreten könnten.**

Woran man es festmacht: Ursachenanalyse dokumentieren, etwa mit 5-Why oder Ishikawa, plus eine ausdrückliche Aussage zur Übertragbarkeit auf andere Systeme oder Prozesse. Der Übertragbarkeitsschritt wird am häufigsten übersehen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10.2-3 **Erforderliche Korrekturmaßnahmen sind umgesetzt und ihre Wirksamkeit ist überprüft.**

Woran man es festmacht: Je Maßnahme Umsetzungsdatum, Nachweisartefakt und eine spätere Wirksamkeitsprüfung mit eigenem Datum. Zwei Datumsangaben je Zeile sind der einfachste Weg, die Wirksamkeitsprüfung nicht zu verlieren.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10.2-4 **Falls erforderlich, werden aufgrund der Nichtkonformität Änderungen am ISMS vorgenommen.**

Woran man es festmacht: Wenn eine Nichtkonformität auf eine Lücke in Richtlinie, Risikoregister oder SoA zurückgeht, muss die Änderung dort sichtbar werden. Der Verweis von der Abweichung auf die geänderte Dokumentenversion schließt die Kette.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10.2-5 **Die Korrekturmaßnahmen sind den Auswirkungen der aufgetretenen Nichtkonformitäten angemessen.**

Woran man es festmacht: Eine Einstufung nach Schwere im Register, aus der die Verhältnismäßigkeit der Maßnahme hervorgeht. Weder Bagatellen mit Projektaufwand noch schwere Abweichungen mit einer bloßen Erinnerungsmail.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10.2-6 **Dokumentierte Information über die Art der Nichtkonformitäten, die daraufhin getroffenen Maßnahmen und die Ergebnisse der Korrekturmaßnahmen ist aufbewahrt.** Dokument

Woran man es festmacht: Ein Abweichungs- und Korrekturmaßnahmenregister mit den Spalten Art, Ursache, Maßnahme, Verantwortlicher, Termin, Ergebnis der Wirksamkeitsprüfung. Es ist ein Pflichtnachweis und wird in jedem Überwachungsaudit gezogen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5 Anhang A: Organisatorische Controls 37

A.5.1 Richtlinien für Informationssicherheit: Eine übergeordnete Sicherheitsrichtlinie und themenspezifische Richtlinien sind festgelegt, von der Leitung genehmigt, kommuniziert und werden in geplanten Abständen sowie bei wesentlichen Änderungen überprüft.

Dokument

Woran man es festmacht: Richtliniensatz mit Version, Freigabedatum und nächstem Reviewtermin, plus Nachweis der Kenntnisnahme. Für kleine Betriebe genügen eine Rahmenrichtlinie und wenige Themenrichtlinien (Zugang, Kryptographie, Remote-Arbeit, Vorfälle).

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.2 Informationssicherheitsrollen und -verantwortlichkeiten: Die Rollen und Verantwortlichkeiten für Informationssicherheit sind entsprechend den Bedürfnissen der Organisation definiert und zugewiesen.

Woran man es festmacht: Rollenmatrix mit Namen, Vertretung und Aufgaben. In Kleinstorganisationen die Häufung mehrerer Rollen bei einer Person offen ausweisen und mit den kompensierenden Kontrollen aus A.5.3 verknüpfen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.3 Aufgabentrennung: Aufgaben und Zuständigkeiten, die sich gegenseitig kontrollieren sollten, liegen nicht in einer Hand. Ziel ist, dass niemand allein eine Änderung veranlassen, freigeben und verdecken kann.

Woran man es festmacht: In kleinen Organisationen ist eine vollständige Trennung strukturell nicht möglich; ein pauschales erfüllt fällt im Auditgespräch sofort auf. Belastbar ist eine ehrliche Analyse: Welche Aufgabenkombinationen sind kritisch (Entwickeln und Freigeben, Rechte vergeben und Rechte nutzen, Zahlung anweisen und freigeben), welche davon liegen bei einer Person, und welche kompensierenden Kontrollen greifen. Bewährt sind unveränderliche Audit-Logs mit Zugriff für einen Dritten, MFA für privilegierte Konten, automatisierte CI-Gates und Branch-Protection statt Vier-Augen-Prinzip, eine periodische Durchsicht der Logs durch eine externe Person sowie eine getrennte Freigabe für Zahlungen. Analyse und kompensierende Kontrollen als eigenes, datiertes Dokument führen und in der SoA verlinken.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.4 Managementverantwortlichkeiten: Die Leitung verlangt von allen Personen die Anwendung der Informationssicherheit gemäß den festgelegten Richtlinien und Verfahren.

Woran man es festmacht: Verpflichtung in Arbeits- und Auftragnehmerverträgen, Kenntnisnahme der Richtlinien beim Onboarding, regelmäßige Erinnerung durch die Leitung. Belege sind unterschriebene Verpflichtungserklärungen und Meetingprotokolle.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.5 Kontakt mit Behörden: Angemessene Kontakte zu relevanten Behörden werden gepflegt und sind im Bedarfsfall abrufbar.

Woran man es festmacht: Kontaktliste mit zuständiger Datenschutzaufsicht, Polizei oder Zentralstelle Cybercrime, BSI-Meldestelle und, bei Betroffenheit, NIS2-Meldewegen. Fristen (etwa 72 Stunden nach DSGVO) direkt in der Liste vermerken.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.6 Kontakt mit speziellen Interessengruppen: Kontakte zu Fachgruppen, Sicherheitsforen und Fachverbänden werden gepflegt.

Woran man es festmacht: Mitgliedschaften, abonnierte Warnmeldungen (CERT-Bund, Herstellerfeeds), Teilnahme an Fachgruppen. Ein einfacher Nachweis: Liste der Abonnements plus ein Beispiel, wie eine Meldung zu einer Handlung geführt hat.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.7 **Threat Intelligence: Informationen über Bedrohungen für die Informationssicherheit werden gesammelt und ausgewertet, um daraus geeignete Maßnahmen abzuleiten.**

Woran man es festmacht: Neu in der Fassung 2022. Praktikabel für kleine Betriebe: Abonnement von CERT-Bund-Warnmeldungen und Hersteller-Advisories, monatliche Kurzauswertung mit Relevanzentscheidung und daraus abgeleiteten Tickets. Der Nachweis ist die Auswertung, nicht das Abonnement.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.8 **Informationssicherheit im Projektmanagement: Informationssicherheit ist in das Projektmanagement integriert, unabhängig von der Projektart.**

Woran man es festmacht: Sicherheitspunkte in der Projektcheckliste: Schutzbedarf, Risikobetrachtung, Datenschutzprüfung, Sicherheitsabnahme vor Go-live. In agilen Teams als feste Punkte in Definition of Ready und Definition of Done verankern.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.9 **Inventar der Informationen und anderer damit verbundener Werte: Ein Verzeichnis der Informationen und zugehörigen Werte mit benannten Eigentümern ist erstellt und wird gepflegt.**

Woran man es festmacht: Asset-Inventar mit Hardware, Software, Cloud-Diensten, Datenbeständen, Domains und Zugängen, jeweils mit Eigentümer und Schutzbedarf. Bei kleinen Betrieben aus MDM-Export, Lizenzliste und Cloud-Konsole automatisch zusammenführbar; ein aktuelles Datum ist Pflicht.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.10 **Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten: Regeln für den zulässigen Gebrauch und den Umgang mit Informationen und Werten sind festgelegt, dokumentiert und umgesetzt.** Dokument

Woran man es festmacht: Nutzungsrichtlinie für Geräte, Netze, Cloud-Konten und KI-Werkzeuge, mit Bestätigung der Kenntnisnahme. Der Umgang mit privaten Geräten und mit externen KI-Diensten sollte ausdrücklich geregelt sein, weil dort die meisten Abflüsse entstehen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.11 **Rückgabe von Werten: Endet oder ändert sich eine Zusammenarbeit, ist geregelt und quittiert, dass sämtliche überlassenen Geräte, Schlüssel, Zugänge und Unterlagen zurückkommen.**

Woran man es festmacht: Offboarding-Checkliste mit Rückgabequittung für Laptop, Token, Schlüssel, Zertifikate und Datenträger, plus Sperrung der Konten am selben Tag. Gilt genauso für Freelancer und Praktikanten.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.12 **Klassifizierung von Informationen: Informationen sind nach Schutzbedarf hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und rechtlicher Anforderungen klassifiziert.**

Woran man es festmacht: Ein einfaches Schema mit drei bis vier Stufen (öffentlich, intern, vertraulich, streng vertraulich) und je Stufe konkreten Handhabungsregeln. Die Zuordnung im Asset-Inventar oder in der Verarbeitungsübersicht führen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.13 **Kennzeichnung von Informationen: Die Schutzstufe ist am Dokument, an der Datei oder an der Nachricht selbst erkennbar, damit Empfänger ohne Rückfrage wissen, wie sie damit umgehen müssen.**

Woran man es festmacht: Kennzeichnung in Dokumentkopf, Dateinamen, E-Mail-Betreff oder über Labels im Cloud-Office (Sensitivity Labels). Nachweis über Stichproben tatsächlich gekennzeichneter Dokumente, nicht nur über die Regel.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.14 **Informationsübertragung: Regeln, Verfahren und Vereinbarungen für die Übertragung von Informationen innerhalb der Organisation und mit externen Parteien sind vorhanden.**

Woran man es festmacht: Regelung, welcher Kanal für welche Klassifizierungsstufe zulässig ist: verschlüsselte E-Mail oder Datenraum für vertrauliche Inhalte, kein Versand über private Messenger. Vertrauliche Übertragungen mit Vertraulichkeitsvereinbarungen unterlegen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.15 **Zugangssteuerung: Regeln zur Steuerung des physischen und logischen Zugangs zu Informationen und Werten sind auf Basis der Geschäfts- und Sicherheitsanforderungen festgelegt und umgesetzt.**

Woran man es festmacht: Zugangsrichtlinie nach Kenntnis-nur-wenn-nötig und Minimalrechte, mit Rollen-Rechte-Zuordnung. Nachweis über die tatsächliche Rechtekonfiguration im Identity-Provider, nicht über die Richtlinie allein.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.16 **Identitätsmanagement: Der gesamte Lebenszyklus von Identitäten wird gesteuert.**

Woran man es festmacht: Prozess von Anlage über Änderung bis Deaktivierung, möglichst zentral über einen Identity-Provider mit Single Sign-on. Keine geteilten Sammelkonten; wo technisch unvermeidbar, das Konto benennen, begründen und die Nutzung protokollieren.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.17 **Authentifizierungsinformation: Die Zuteilung und Verwaltung von Authentifizierungsinformationen wird durch einen Managementprozess gesteuert, der Personen zum sachgerechten Umgang anhält.**

Woran man es festmacht: Passwortmanager als Pflichtwerkzeug, Richtlinie zu Passwortqualität und MFA, sicherer Erstzugang und Zurücksetzverfahren mit Identitätsprüfung. Nachweis über Konfigurationsscreenshots und den Bericht des Passwortmanagers.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.18 **Zugangsrechte: Zugangsrechte werden gemäß der Zugangssteuerungsrichtlinie zugewiesen, überprüft, geändert und entzogen.**

Woran man es festmacht: Periodischer Zugriffsreview, mindestens jährlich, mit dokumentiertem Ergebnis je Konto und Beleg für entzogene Rechte. Der Entzug am Austrittstag ist ein Punkt, den Auditoren gezielt an einem konkreten Fall nachvollziehen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.19 **Informationssicherheit in Lieferantenbeziehungen: Prozesse und Verfahren zur Steuerung der Sicherheitsrisiken aus der Nutzung von Produkten und Dienstleistungen Dritter sind festgelegt und umgesetzt.**

Woran man es festmacht: Lieferantenliste mit Kritikalitätsstufe und Prüftiefe. Bei kritischen Anbietern Nachweise einholen (ISO-27001-Zertifikat, SOC-2-Bericht) statt eigener Audits, das ist für kleine Betriebe der einzig realistische Weg.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.20 **Behandlung von Informationssicherheit in Lieferantenvereinbarungen: Relevante Sicherheitsanforderungen sind mit jedem Lieferanten vereinbart und in den Verträgen festgehalten.**

Woran man es festmacht: Vertragsanlage Informationssicherheit mit Meldepflichten bei Vorfällen, Unterauftragnehmerregelung, Löschpflichten und Auditrecht. Bei Standarddiensten reichen die Anbieterbedingungen plus Auftragsverarbeitungsvertrag, wenn deren Inhalt geprüft und dokumentiert wurde.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.21 **Umgang mit Informationssicherheit in der IKT-Lieferkette: Prozesse zur Steuerung der Sicherheitsrisiken in der Lieferkette für Informations- und Kommunikationstechnik sind festgelegt und umgesetzt.**

Woran man es festmacht: Betrifft Software-Abhängigkeiten und Unterauftragnehmer der Anbieter. Praktisch: Software-Stückliste (SBOM) oder Abhängigkeitsliste, automatisierte Prüfung auf verwundbare Pakete in der CI, Bezug von Software nur aus signierten oder offiziellen Quellen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.22 **Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen: Änderungen an Dienstleistungen der Lieferanten werden regelmäßig überwacht, überprüft und gesteuert.**

Woran man es festmacht: Jährliche Lieferantenbewertung mit Blick auf Vorfälle, Verfügbarkeitsberichte und Zertifikatsgültigkeit, plus ein Kanal für Änderungsankündigungen des Anbieters. Ergebnis als kurze Notiz je Lieferant.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.23 **Informationssicherheit bei Nutzung von Cloud-Diensten: Prozesse für Erwerb, Nutzung, Verwaltung und Beendigung von Cloud-Diensten sind entsprechend den Sicherheitsanforderungen festgelegt.**

Woran man es festmacht: Neu in der Fassung 2022 und für kleine, cloudbasierte Betriebe das zentrale Control. Nachweis über eine Cloud-Richtlinie mit Freigabeprozess für neue Dienste, dokumentiertem Modell der geteilten Verantwortung je Dienst, Härtungseinstellungen und einer Exit-Strategie inklusive Datenrückgabe und Löschbestätigung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.24 **Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen: Prozesse, Rollen und Verantwortlichkeiten für die Vorfallbehandlung sind geplant und festgelegt.** Dokument

Woran man es festmacht: Incident-Response-Plan mit Meldeweg, Rollen, Eskalationsstufen, Erreichbarkeiten außerhalb der Geschäftszeiten und Kommunikationsvorlagen. Realistisch für kleine Teams: eine Seite, dafür geübt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.25 **Beurteilung und Entscheidung über Informationssicherheitsereignisse: Sicherheitsereignisse werden beurteilt und es wird entschieden, ob sie als Informationssicherheitsvorfall einzustufen sind.**

Woran man es festmacht: Triage-Kriterien mit Schweregradmatrix und ein Ereignisregister, in dem auch verworfene Ereignisse mit Begründung erscheinen. Die Trennung von Ereignis und Vorfall muss im Register erkennbar sein.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.26 **Reaktion auf Informationssicherheitsvorfälle: Vorfälle werden gemäß den dokumentierten Verfahren behandelt.**

Woran man es festmacht: Vorfallakten mit Zeitleiste, ergriffenen Maßnahmen, beteiligten Personen und Abschlussentscheidung. Gab es noch keinen echten Vorfall, ist eine dokumentierte Übung (Tabletop) der beste verfügbare Nachweis.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.27 **Erkenntnisse aus Informationssicherheitsvorfällen: Erkenntnisse aus Vorfällen werden genutzt, um die Sicherheitsmaßnahmen zu stärken.**

Woran man es festmacht: Nachbetrachtung ohne Schuldzuweisung mit Ursachenanalyse und abgeleiteten Maßnahmen, verknüpft mit dem Verbesserungsregister und, wo nötig, mit dem Risikoregister.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.28 **Sammlung von Beweismaterial: Es ist geregelt, wie Spuren zu einem Sicherheitsereignis erkannt, gesichert und so aufbewahrt werden, dass sie später noch verwertbar sind.**

Woran man es festmacht: Kurzverfahren zur Beweissicherung: Systeme nicht vorschnell neu aufsetzen, Abbilder und Logs sichern, Übergabekette dokumentieren. Für kleine Betriebe genügt die Festlegung, ab welchem Schweregrad ein externer Forensikdienstleister hinzugezogen wird, samt Kontaktdaten.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.29 **Informationssicherheit während einer Störung: Die Organisation plant, wie die Informationssicherheit während einer Störung auf einem angemessenen Niveau aufrechterhalten wird.**

Woran man es festmacht: Notfallregelungen dürfen Sicherheit nicht aushebeln. Dokumentieren, dass auch im Notbetrieb MFA, Protokollierung und Zugangsbeschränkungen gelten, und Notfallzugänge (Break-Glass-Konten) versiegelt, dokumentiert und nachträglich überprüft werden.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.30 **IKT-Bereitschaft für Business Continuity: Die Bereitschaft der Informations- und Kommunikationstechnik ist auf Basis von Geschäftsfortführungszielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und getestet.**

Woran man es festmacht: Neu in der Fassung 2022. Nachweis über festgelegte Wiederanlaufziele (RTO) und Datenverlusttoleranz (RPO) je kritischem System, ein Wiederanlaufverfahren und mindestens einen dokumentierten Test pro Jahr. Ein erfolgreicher Restore-Test mit Datum und Dauer ist der stärkste Einzelbeleg.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.31 **Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen: Die relevanten Anforderungen und das Vorgehen zu ihrer Erfüllung sind identifiziert, dokumentiert und aktuell gehalten.** Dokument

Woran man es festmacht: Rechtskataster mit DSGVO, Telekommunikationsrecht, Handels- und Steuerrecht, gegebenenfalls NIS2 oder branchenspezifischen Vorgaben, jeweils mit der umsetzenden Regelung und dem Prüfdatum. Jährlicher Review reicht, muss aber datiert sein.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.32 **Geistige Eigentumsrechte: Angemessene Verfahren zum Schutz geistiger Eigentumsrechte sind umgesetzt.**

Woran man es festmacht: Lizenzverzeichnis für eingesetzte Software, Prüfung von Open-Source-Lizenzen im Produkt (Lizenzscanner in der CI) und eine Regel zum Umgang mit Fremdcode und mit generiertem Code. Nachweis: Lizenzbericht aus dem Build.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.33 **Schutz von Aufzeichnungen: Geschäfts- und Nachweisunterlagen sind so abgelegt, dass sie nicht verloren gehen, nicht unbemerkt verändert werden und nicht in falsche Hände geraten, und zwar über die gesamte Aufbewahrungsfrist.**

Woran man es festmacht: Aufbewahrungsplan mit gesetzlichen Fristen, revisionssichere Ablage, Zugriffsbeschränkung und Backup. Für steuerlich relevante Belege die gesetzlichen Fristen ausdrücklich nennen, das prüfen Auditoren gern konkret.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.34 **Privatsphäre und Schutz personenbezogener Daten: Die Anforderungen an Privatsphäre und den Schutz personenbezogener Daten sind entsprechend geltendem Recht identifiziert und erfüllt.**

Woran man es festmacht: Verzeichnis von Verarbeitungstätigkeiten, Auftragsverarbeitungsverträge, Löschkonzept, Betroffenenrechteprozess, gegebenenfalls Datenschutz-Folgenabschätzung. Die Verzahnung mit dem ISMS über eine gemeinsame Assetliste spart doppelte Pflege.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.35 **Unabhängige Überprüfung der Informationssicherheit: Das Vorgehen der Organisation zur Steuerung der Informationssicherheit wird in geplanten Abständen und bei wesentlichen Änderungen unabhängig überprüft.**

Woran man es festmacht: Belegbar durch das interne Audit mit unabhängigem Auditor, durch externe Penetrationstests oder durch das Zertifizierungsaudit selbst. Unabhängig heißt: nicht durch die Person, die den geprüften Bereich verantwortet.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.36 **Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit: Die Einhaltung der eigenen Sicherheitsrichtlinien und der geltenden Vorgaben wird regelmäßig überprüft.**

Woran man es festmacht: Compliance-Checks mit Datum und Ergebnis, etwa Konfigurationsprüfung gegen die eigene Härtungsvorgabe, Stichproben zur Kennzeichnung von Dokumenten, automatisierte Policy-Checks in der Cloud. Abweichungen laufen in das Korrekturmaßnahmenregister.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.5.37 **Dokumentierte Betriebsabläufe: Betriebsabläufe für informationsverarbeitende Einrichtungen sind dokumentiert und den Personen zugänglich gemacht, die sie benötigen.** Dokument

Woran man es festmacht: Runbooks für Backup und Restore, Deployment, Benutzerverwaltung, Patching und Vorfallbehandlung. Kurz und aktuell schlägt umfangreich und veraltet; ein Änderungsdatum je Runbook ist Pflicht.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.6 Anhang A: Personenbezogene Controls 8

A.6.1 **Sicherheitsüberprüfung: Wer für die Organisation tätig werden soll, wird vorab in einem rechtlich zulässigen und zum Schutzbedarf passenden Umfang überprüft; bei sensiblen Rollen wird die Prüfung im Verlauf des Arbeitsverhältnisses wiederholt.**

Woran man es festmacht: Ohne Angestellte ist dieses Control als derzeit nicht anwendbar begründbar, das Verfahren für den Einstellungsfall sollte trotzdem definiert und in der Erklärung zur Anwendbarkeit als geplant hinterlegt sein. Praktikabler Umfang in Deutschland: Prüfung von Identität, Lebenslauf und Referenzen, Zeugnisse; ein Führungszeugnis nur, wenn der Schutzbedarf es rechtfertigt und es rechtlich zulässig ist. Für Freelancer und Auftragnehmer denselben Standard über den Vertrag verlangen, sonst entsteht genau hier die Lücke.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.6.2 **Beschäftigungs- und Arbeitsvertragsbedingungen: Die vertraglichen Vereinbarungen benennen die Verantwortlichkeiten der Beschäftigten und der Organisation für die Informationssicherheit.**

Woran man es festmacht: Sicherheitsklausel im Arbeits- oder Dienstleistungsvertrag mit Verweis auf die geltenden Richtlinien. Bei Freelancern die gleiche Klausel im Werk- oder Dienstvertrag, plus Vertraulichkeitsvereinbarung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.6.3 **Informationssicherheitsbewusstsein, -ausbildung und -schulung: Beschäftigte und relevante externe Personen erhalten angemessene Sensibilisierung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien der Organisation.**

Woran man es festmacht: Jährliche Schulung mit Teilnahmenachweis und Datum, ergänzt um Phishing-Simulationen mit ausgewerteter Klickrate. Auch Solo-Selbstständige brauchen einen Nachweis der eigenen Fortbildung, etwa Kursbestätigungen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.6.4 **Disziplinarverfahren: Ein formales, kommuniziertes Verfahren zum Vorgehen gegen Personen, die Sicherheitsrichtlinien verletzt haben, ist vorhanden.**

Woran man es festmacht: Ohne Angestellte als derzeit nicht anwendbar begründbar, das Verfahren muss für den Einstellungsfall aber definiert sein; nur die Anwendung, nicht die Regelung, entfällt. Erforderlich ist eine gestufte, kommunizierte Reaktionsskala (Gespräch, Ermahnung, Abmahnung, Kündigung) unter Beachtung von Arbeitsrecht und Mitbestimmung. Für Auftragnehmer die Sanktionsstufe vertraglich abbilden, etwa Vertragsstrafe oder Kündigungsrecht.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.6.5 **Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung: Sicherheitsrelevante Verantwortlichkeiten und Pflichten, die nach Beendigung oder Wechsel fortbestehen, sind definiert, durchgesetzt und den Betroffenen mitgeteilt.**

Woran man es festmacht: Offboarding-Checkliste mit Rechteentzug, Rückgabe, Übergabe der Assets und ausdrücklichem Hinweis auf fortbestehende Vertraulichkeitspflichten. Ein unterschriebenes Austrittsgespräch-Protokoll ist der einfachste Beleg.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.6.6 **Vertraulichkeits- oder Geheimhaltungsvereinbarungen: Es ist bestimmt, wer eine Vertraulichkeitsvereinbarung unterzeichnen muss. Der Inhalt passt zum Schutzbedarf der Informationen, die Vereinbarungen sind unterschrieben, abgelegt und werden regelmäßig auf Aktualität durchgesehen.**

Woran man es festmacht: Unterschriebene Vertraulichkeitsvereinbarungen für Beschäftigte, Freelancer, Dienstleister und Praktikanten, mit Nachwirkungsfrist. Eine Übersichtstabelle mit Vertragspartner, Datum und Gültigkeit macht den Bestand prüfbar.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.6.7 **Remote-Arbeit: Sicherheitsmaßnahmen sind umgesetzt, wenn Personen außerhalb der Räumlichkeiten der Organisation arbeiten und dabei auf Informationen der Organisation zugreifen.**

Woran man es festmacht: Homeoffice- und Remote-Richtlinie mit Vorgaben zu Festplattenverschlüsselung, Bildschirmsperre, sicherem WLAN, Nutzung von VPN oder Zero-Trust-Zugang, Sichtschutz und Verbot der Nutzung privater Geräte ohne Freigabe. Nachweis über MDM-Compliance-Report der Endgeräte.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.6.8 **Meldung von Informationssicherheitsereignissen: Es besteht ein Mechanismus, über den Personen beobachtete oder vermutete Sicherheitsereignisse zeitnah melden können.**

Woran man es festmacht: Ein klar kommunizierter Meldeweg (Postfach, Chatkanal, Telefonnummer) mit Zusicherung der Sanktionsfreiheit bei gutgläubiger Meldung. Nachweis: Meldeaufkommen im Ereignisregister; ein dauerhaft leeres Register ist im Audit ein Warnsignal.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.7 Anhang A: Physische Controls 14

A.7.1 **Physische Sicherheitsperimeter: Sicherheitsperimeter sind festgelegt und werden genutzt, um Bereiche mit Informationen und informationsverarbeitenden Einrichtungen zu schützen.**

Woran man es festmacht: Beschreibung der Perimeter mit Skizze oder Fotos: Gebäude, Büro, Serverschrank. Im Homeoffice ist der Perimeter der abschließbare Arbeitsraum oder ersatzweise ein abschließbarer Schrank; das ist zu beschreiben, nicht wegzulassen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.7.2 **Physischer Zutritt: Sichere Bereiche sind durch angemessene Zutrittskontrollen und Zugangspunkte geschützt.**

Woran man es festmacht: Schlüssel- oder Kartenverzeichnis mit Ausgabe und Rückgabe, Besucherregelung mit Begleitung und Protokoll. Bei Nutzung eines Coworking-Space oder eines Rechenzentrums die Zutrittsregelung des Betreibers als Nachweis heranziehen und vertraglich absichern.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.7.3 **Sichern von Büros, Räumen und Einrichtungen: Für Büros, Räume und Einrichtungen ist physische Sicherheit gestaltet und umgesetzt.**

Woran man es festmacht: Abschließbare Türen, Fenstersicherung im Erdgeschoss, keine Sichtbarkeit vertraulicher Bildschirme von außen, kein Firmenschild an sensiblen Bereichen. Kurze Beschreibung plus Foto genügt als Beleg.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.7.4 **Physische Überwachung: Räumlichkeiten werden fortlaufend auf unbefugten physischen Zutritt überwacht.**

Woran man es festmacht: Neu in der Fassung 2022. Möglich sind Alarmanlage, Bewegungsmelder, Videoüberwachung oder Zutrittsprotokolle. Videoüberwachung ist datenschutzrechtlich zu prüfen; im Homeoffice ist die begründete Alternative eine Kombination aus Alarmanlage, verschlossenem Raum und der Feststellung, dass keine sensiblen Server vorgehalten werden.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.7.5 **Schutz vor physischen und umweltbedingten Bedrohungen: Es besteht Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und vorsätzlichen oder unbeabsichtigten Schäden.**

Woran man es festmacht: Betrachtung von Feuer, Wasser, Hitze, Stromausfall und Einbruch, mit den vorhandenen Maßnahmen (Rauchmelder, Feuerlöscher, keine Geräte unter Wasserleitungen, Auslagerung des Backups an einen anderen Ort). Hier greift der Bezug zur Klimawandel-Bestimmung aus 4.1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.7.6 **Arbeiten in Sicherheitsbereichen: Für das Arbeiten in Sicherheitsbereichen sind Maßnahmen gestaltet und umgesetzt.**

Woran man es festmacht: Regeln für Serverraum oder Bereiche mit hoher Vertraulichkeit: kein unbeaufsichtigter Fremdzugang, Aufzeichnungsverbot für Kamera und Mobilgerät, Protokollierung der Arbeiten. Bestehen keine Sicherheitsbereiche, ist das mit Verweis auf Cloud-Betrieb begründbar.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.7.7 **Aufgeräumter Arbeitsplatz und Bildschirmsperre: Regeln für einen aufgeräumten Arbeitsplatz mit Blick auf Papiere und Wechselmedien sowie für gesperrte Bildschirme sind festgelegt und werden eingehalten.**

Woran man es festmacht: Gilt vollständig auch im Homeoffice und ist deshalb nicht als nicht anwendbar zu erklären. Nachweisbar durch eine kurze Regel (Unterlagen wegschließen, Bildschirmsperre nach fünf Minuten, keine Notizzettel mit Zugangsdaten) plus die technisch erzwungene Sperre per Geräterichtlinie, deren Konfiguration exportierbar ist.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.7.8 **Platzierung und Schutz von Geräten und Betriebsmitteln: Geräte sind sicher platziert und geschützt.**

Woran man es festmacht: Aufstellung außerhalb von Durchgangs- und Publikumsbereichen, kein Einblick von außen, Schutz vor Hitze und Feuchtigkeit, Kabelsicherung oder Schloss bei mobilen Geräten. Kurzbeschreibung im Rahmen der Homeoffice- oder Bürorichtlinie.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.7.9 **Sicherheit von Werten außerhalb der Räumlichkeiten: Werte, die sich außerhalb der Räumlichkeiten befinden, sind geschützt.**

Woran man es festmacht: Das betrifft in kleinen Organisationen vor allem den Laptop, das Smartphone und externe Datenträger, und darf nicht wegdiskutiert werden. Nachweis: Festplattenverschlüsselung erzwungen, Fernlöschung über MDM aktiviert, Regel gegen Zurücklassen im Fahrzeug und gegen Nutzung in öffentlichen Netzen ohne VPN, dazu ein Verlustmeldeweg. Der MDM-Compliance-Report mit Verschlüsselungsstatus je Gerät ist der belastbarste Einzelbeleg.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.7.10 **Speichermedien: Speichermedien werden über ihren gesamten Lebenszyklus hinweg entsprechend dem Klassifizierungsschema und den Handhabungsanforderungen gesteuert, von der Beschaffung über Nutzung und Transport bis zur Entsorgung.**

Woran man es festmacht: Gilt auch bei rein mobiler Arbeit, weil USB-Sticks, externe Festplatten und Backup-Medien vorhanden sind. Nachweis: Medienverzeichnis, verschlüsselte Datenträger, Verbot nicht freigegebener Wechselmedien technisch erzwungen, sichere Aufbewahrung an einem abschließbaren Ort, Übergabe an A.7.14 bei Ausmusterung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.7.11 **Versorgungseinrichtungen: Informationsverarbeitende Einrichtungen sind gegen Ausfall der Versorgung, insbesondere der Stromversorgung, geschützt.**

Woran man es festmacht: Bei eigenem Serverbetrieb unterbrechungsfreie Stromversorgung mit dokumentiertem Test. Bei reinem Cloud-Betrieb ist der Nachweis der Verweis auf die Anbieterzusagen sowie eine Regelung zur Arbeitsfähigkeit bei lokalem Strom- oder Internetausfall (Mobilfunk-Tethering, Ausweichstandort).

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.7.12 **Sicherheit der Verkabelung: Kabel für Strom, Daten und Kommunikation sind vor Abhören, Störungen und Beschädigung geschützt.**

Woran man es festmacht: Bei eigener Verkabelung Schutz gegen Beschädigung und unbefugten Zugang zu Patchfeldern. Bei kleinen Büros und im Homeoffice ist die Begründung schlank, aber sie ist zu geben: Router und Netzwerkdosen sind nicht öffentlich zugänglich, offene Ports sind deaktiviert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.7.13 **Instandhaltung von Geräten und Betriebsmitteln: Geräte werden korrekt instand gehalten, um Verfügbarkeit, Integrität und Vertraulichkeit von Informationen sicherzustellen.**

Woran man es festmacht: Wartungsplan oder Herstellersupport-Status je Gerät, Regel zum Umgang mit Reparaturen durch Dritte (Datenträger vorher entfernen oder Daten löschen, Vertraulichkeitsvereinbarung mit dem Dienstleister). Ende-des-Supports-Termine im Asset-Inventar führen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.7.14 **Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln: Bevor ein Gerät mit Speicher weitergegeben, verkauft oder verschrottet wird, ist geprüft und festgehalten, dass keine schützenswerten Daten und keine lizenzpflichtige Software mehr darauf rekonstruierbar sind.**

Woran man es festmacht: Gilt auch im Homeoffice und für ausgemusterte private Altgeräte, die dienstlich genutzt wurden. Nachweis: Löschprotokoll je Gerät mit Seriennummer, Datum und Verfahren (kryptografisches Löschen bei verschlüsselten SSDs, Überschreiben, physische Zerstörung), oder ein Vernichtungszertifikat des Dienstleisters. Bei verschlüsselten Geräten reicht das dokumentierte Vernichten des Schlüssels, wenn das Verfahren beschrieben ist.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8 Anhang A: Technologische Controls 34

A.8.1 Endpunktgeräte des Benutzers: Auf Endgeräten gespeicherte, verarbeitete oder darüber zugängliche Informationen sind geschützt.

Woran man es festmacht: Härtungsvorgabe je Betriebssystem, zentrale Verwaltung über MDM, Festplattenverschlüsselung, automatische Updates, Bildschirmsperre. Der Compliance-Report des MDM mit Status je Gerät belegt alle Punkte auf einmal.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.2 Privilegierte Zugangsrechte: Die Zuteilung und Nutzung privilegierter Zugangsrechte ist eingeschränkt und wird gesteuert.

Woran man es festmacht: Liste aller Administratorkonten mit Begründung, getrennte Admin-Konten ohne Alltagsnutzung, MFA erzwungen, zeitlich begrenzte Rechteerhöhung wo möglich, periodische Überprüfung. Das ist in kleinen Organisationen die wichtigste kompensierende Kontrolle zu A.5.3.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.3 Informationszugangsbeschränkung: Der Zugang zu Informationen und anderen zugehörigen Werten ist gemäß der festgelegten Zugangssteuerungsrichtlinie beschränkt.

Woran man es festmacht: Berechtigungskonzept mit Rollen und Gruppen statt Einzelrechten, Nachweis über einen Export der Gruppenzugehörigkeiten. Öffentliche Freigabelinks in Cloud-Speichern regelmäßig prüfen und ablaufen lassen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.4 Zugang zum Quellcode: Lese- und Schreibzugriff auf Quellcode, Entwicklungswerkzeuge und Softwarebibliotheken ist angemessen gesteuert.

Woran man es festmacht: Repository-Rechte nach Rolle, geschützte Hauptbranches, erzwungene Reviews oder erzwungene Statuschecks, kein direkter Push auf main. Nachweis über die Branch-Protection-Konfiguration und die Mitgliederliste der Organisation.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.5 Sichere Authentifizierung: Sichere Authentifizierungstechniken und -verfahren sind auf Basis der Zugangsbeschränkungen und der themenspezifischen Richtlinie umgesetzt.

Woran man es festmacht: MFA für alle externen Zugänge und alle Administratorkonten, phishing-resistente Verfahren (Passkeys, FIDO2) wo möglich, Sperrung nach Fehlversuchen. Nachweis über den MFA-Abdeckungsbericht des Identity-Providers.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.6 Kapazitätssteuerung: Speicher, Rechenleistung, Bandbreite und Lizenzen werden beobachtet, und der Bedarf wird so rechtzeitig nachgeführt, dass Engpässe die Verfügbarkeit nicht gefährden.

Woran man es festmacht: Monitoring von Speicher, Rechenlast, Lizenzkontingenten und Cloud-Budgets mit Schwellenwert-Alarmen. Bei kleinen Betrieben genügt ein Alarm auf Speicherfüllstand und Kostenlimit plus ein jährlicher Kapazitätsblick.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.7 Schutz gegen Schadsoftware: Technische Abwehrmaßnahmen gegen Schadsoftware sind aktiv und aktuell, und die Personen, die die Geräte nutzen, sind so geschult, dass sie die Abwehr nicht unterlaufen.

Woran man es festmacht: Aktiver Endpunktschutz mit zentraler Statusübersicht, Mailfilter mit Anhang- und Linkprüfung, Regel gegen die Ausführung nicht freigegebener Software. Der Statusbericht der Schutzlösung mit Datum ist der direkte Nachweis.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.8 **Handhabung von technischen Schwachstellen: Die Organisation erfährt aktiv von Schwachstellen in der eingesetzten Technik, entscheidet je Fund, wie stark sie davon betroffen ist, und schließt die Lücke innerhalb festgelegter Fristen oder begründet einen anderen Umgang.**

Woran man es festmacht: Schwachstellenmanagement mit Quelle (Scanner, Abhängigkeitsprüfung in der CI, Herstellermeldungen), Bewertung nach Schweregrad und definierten Fristen je Stufe, etwa kritisch binnen 7 Tagen. Nachweis: Scanberichte über mehrere Zeitpunkte, aus denen der Rückgang offener Findings hervorgeht.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.9 **Konfigurationsmanagement: Konfigurationen von Hardware, Software, Diensten und Netzwerken, einschließlich Sicherheitskonfigurationen, sind festgelegt, dokumentiert, umgesetzt, überwacht und werden überprüft.**

Woran man es festmacht: Neu in der Fassung 2022. Nachweis über dokumentierte Basiskonfigurationen (Härtungsvorgaben) und deren Durchsetzung, idealerweise als Infrastruktur-als-Code im Versionskontrollsystem oder über MDM-Profile. Abweichungserkennung (Drift Detection) und ein periodischer Konfigurationsvergleich runden es ab.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.10 **Löschung von Informationen: In Informationssystemen, auf Geräten und auf Speichermedien gespeicherte Informationen werden gelöscht, sobald sie nicht mehr benötigt werden.**

Woran man es festmacht: Neu in der Fassung 2022 und eng mit der DSGVO verzahnt. Nachweis über ein Löschkonzept mit Fristen je Datenkategorie, technisch umgesetzte Aufbewahrungsregeln (Retention Policies) in Cloud-Diensten und Datenbanken sowie Löschprotokolle. Auch Backups und Log-Archive brauchen eine Frist.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.11 **Datenmaskierung: Datenmaskierung wird gemäß der themenspezifischen Richtlinie zur Zugangssteuerung und den geschäftlichen sowie rechtlichen Anforderungen eingesetzt.**

Woran man es festmacht: Neu in der Fassung 2022. Praktisch: keine Produktionsdaten in Test- und Entwicklungsumgebungen, sondern anonymisierte oder synthetische Daten; Pseudonymisierung in Auswertungen; Maskierung von Kontonummern und Zugangsdaten in Logs und Support-Oberflächen. Nachweis über das Skript oder Verfahren zur Testdatengenerierung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.12 **Verhinderung von Datenlecks: Maßnahmen zur Verhinderung von Datenabfluss sind auf Systeme, Netzwerke und Geräte angewendet, die sensible Informationen verarbeiten, speichern oder übertragen.**

Woran man es festmacht: Neu in der Fassung 2022. In kleinen Organisationen realistisch: Kontrolle der Freigabelinks im Cloud-Speicher, Blockieren nicht freigegebener Wechselmedien, Regeln gegen Weiterleitung an private Postfächer, Prüfung der Eingabe vertraulicher Daten in externe KI-Dienste, Erkennung von Zugangsdaten im Quellcode (Secret Scanning). Nachweis über die Konfiguration und über Auswertungen der Treffer.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.13 **Sicherung von Informationen: Für Daten, Software und Systeme bestehen Sicherungen nach einer festgelegten Regel (Umfang, Takt, Aufbewahrung, Ablageort), und die Wiederherstellung daraus wird in regelmäßigen Abständen tatsächlich erprobt.**

Woran man es festmacht: Backup-Richtlinie mit Häufigkeit, Aufbewahrung und Offsite-Kopie nach dem 3-2-1-Prinzip, Verschlüsselung der Sicherungen, Schutz gegen Überschreiben durch Ransomware (unveränderliche Sicherungen). Entscheidend ist der dokumentierte Wiederherstellungstest mit Datum und Ergebnis, denn ein ungetestetes Backup gilt im Audit als nicht vorhanden.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.14 **Redundanz von informationsverarbeitenden Einrichtungen: Informationsverarbeitende Einrichtungen sind mit ausreichender Redundanz ausgestattet, um die Verfügbarkeitsanforderungen zu erfüllen.**

Woran man es festmacht: Redundanz muss zu den Verfügbarkeitszielen passen, nicht zum Maximum. Nachweis über Architekturbeschreibung mit redundanten Instanzen oder Zonen, Ausweichgeräte, sowie eine begründete Entscheidung, wo bewusst keine Redundanz besteht.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.15 **Protokollierung: Sicherheitsrelevante Vorgänge hinterlassen eine Spur. Die Protokolle werden erzeugt, aufbewahrt, gegen Veränderung geschützt und tatsächlich ausgewertet, nicht nur gesammelt.**

Woran man es festmacht: Protokolliert werden mindestens Anmeldungen und Fehlversuche, Rechteänderungen, administrative Aktionen und Zugriffe auf vertrauliche Daten. Die Logs sind gegen Veränderung geschützt und mit einer definierten Aufbewahrungsfrist versehen; unveränderliche Logs sind in kleinen Organisationen zugleich die Kompensation für die fehlende Aufgabentrennung nach A.5.3.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.16 **Überwachungsaktivitäten: Netzwerke, Systeme und Anwendungen werden auf anomales Verhalten überwacht und es werden angemessene Maßnahmen zur Bewertung möglicher Sicherheitsvorfälle ergriffen.**

Woran man es festmacht: Neu in der Fassung 2022. Praktikabel ohne eigenes Sicherheitsteam: Alarme des Identity-Providers auf unmögliche Anmeldeorte und Fehlversuchsserien, Alarme der Cloud-Plattform auf ungewöhnliche Ausgaben oder Rechteänderungen, Weiterleitung an ein überwachtes Postfach mit definierter Reaktionszeit. Nachweis über Alarmregeln plus Beispiele bearbeiteter Alarme.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.17 **Uhrensynchronisation: Alle Systeme, die Protokolle schreiben, beziehen ihre Zeit aus einer festgelegten, vertrauenswürdigen Quelle, sodass Ereignisse systemübergreifend in die richtige Reihenfolge gebracht werden können.**

Woran man es festmacht: NTP-Konfiguration auf Servern und Endgeräten, einheitliche Zeitzone in den Logs (idealerweise UTC). Ohne synchrone Zeit ist eine Vorfallrekonstruktion nach A.5.28 nicht belastbar; ein Konfigurationsauszug reicht als Nachweis.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.18 **Gebrauch von Hilfsprogrammen mit privilegierten Rechten: Der Einsatz von Hilfsprogrammen, die Systemschutzmaßnahmen umgehen können, ist eingeschränkt und wird streng gesteuert.**

Woran man es festmacht: Liste zugelassener Administrationswerkzeuge, Beschränkung der lokalen Administratorrechte, Anwendungssteuerung (Allowlisting) wo möglich, Protokollierung der Nutzung. Nachweis: Richtlinie plus Konfiguration der Rechteverwaltung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.19 **Installation von Software auf Systemen im Betrieb: Verfahren und Maßnahmen zur sicheren Verwaltung der Softwareinstallation auf produktiven Systemen sind umgesetzt.**

Woran man es festmacht: Nur freigegebene Software aus vertrauenswürdigen Quellen, Installation über zentrale Verteilung oder Paketmanager, Rückbaupfad und Aufbewahrung der Vorversion. Nachweis über Freigabeliste und Deployment-Protokolle.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.20 **Netzwerksicherheit: Netze und aktive Netzkomponenten haben einen benannten Verantwortlichen, eine gehärtete Konfiguration und ein nachvollziehbares Regelwerk dafür, welcher Verkehr überhaupt zugelassen ist.**

Woran man es festmacht: Firewall-Regelwerk nach dem Prinzip alles verboten, was nicht erlaubt ist, dokumentierte offene Ports mit Begründung, sichere WLAN-Konfiguration, Ändern der Standardzugangsdaten von Netzwerkgeräten. Nachweis über Regelwerk-Export und einen externen Portscan.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.21 **Sicherheit von Netzwerkdiensten: Sicherheitsmechanismen, Dienstgüte und Verwaltungsanforderungen von Netzwerkdiensten sind identifiziert, umgesetzt und überwacht.**

Woran man es festmacht: Je genutztem Netzwerkdienst (VPN, DNS, Mail, CDN) die Sicherheitszusagen und die eigene Konfiguration dokumentieren, inklusive Verschlüsselung in Transit und Dienstgütezusagen des Anbieters. Nachweis: Konfigurationsübersicht plus Vertrag oder Servicebeschreibung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.22 **Trennung von Netzwerken: Das Netz ist in Zonen aufgeteilt, sodass Dienste, Nutzergruppen und Systeme mit unterschiedlichem Schutzbedarf nicht ungefiltert aufeinander zugreifen können.**

Woran man es festmacht: Getrennte Netzsegmente oder VLAN für Gäste, Verwaltung und Produktion, in der Cloud getrennte Konten oder virtuelle Netze mit Sicherheitsgruppen. Im Homeoffice ist die praktikable Umsetzung ein separates Netz oder VLAN für dienstliche Geräte, getrennt von privaten Geräten und Smart-Home-Technik.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.23 **Web-Filterung: Der Zugriff auf externe Websites wird gesteuert, um die Exponiertheit gegenüber schädlichen Inhalten zu verringern.**

Woran man es festmacht: Neu in der Fassung 2022. Umsetzbar mit geringem Aufwand über einen filternden DNS-Dienst oder die im Endpunktschutz enthaltene Web-Filterung, mit Sperrkategorien und Protokollierung geblockter Aufrufe. Nachweis über die Filterkonfiguration und einen Auswertungsbericht.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.24 **Verwendung von Kryptographie: Es ist verbindlich geregelt, wo verschlüsselt wird, mit welchen Verfahren, und wie die Schlüssel über ihren gesamten Lebenszyklus erzeugt, aufbewahrt, gewechselt und vernichtet werden.** Dokument

Woran man es festmacht: Kryptographie-Richtlinie mit zugelassenen Verfahren und Mindestlängen, Verschlüsselung in Transit (TLS) und im Ruhezustand, sowie ein Schlüsselverwaltungsverfahren mit Erzeugung, Aufbewahrung, Wechsel und Vernichtung. Nachweis über die Richtlinie plus die Konfiguration von Schlüsseldienst oder Tresor.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.25 **Sicherer Entwicklungslebenszyklus: Regeln für die sichere Entwicklung von Software und Systemen sind festgelegt und werden angewendet.**

Woran man es festmacht: Beschreibung des Entwicklungsprozesses mit Sicherheitspunkten je Phase: Anforderung, Entwurf, Umsetzung, Test, Freigabe, Betrieb. Für kleine Teams reicht eine Seite, die auf die konkreten CI-Gates und die Reviewpflicht verweist.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.26 **Anforderungen an die Anwendungssicherheit: Sicherheitsanforderungen an Anwendungen sind bei Entwicklung und Beschaffung identifiziert, spezifiziert und genehmigt.**

Woran man es festmacht: Sicherheitsanforderungen als eigene Punkte in der Anforderungsliste oder als wiederverwendbare Checkliste, orientiert etwa an gängigen Prüfstandards für Anwendungssicherheit. Nachweis über Tickets oder Anforderungsdokumente mit Sicherheitsbezug.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.27 **Sichere Systemarchitektur und Prinzipien für die Systemtechnik: Grundsätze für sichere Systemgestaltung sind festgelegt, dokumentiert und werden auf Entwicklungstätigkeiten angewendet.**

Woran man es festmacht: Dokumentierte Prinzipien wie Minimalrechte, mehrschichtige Verteidigung, sichere Standardeinstellungen, Datensparsamkeit und Zero-Trust-Ansatz, plus deren sichtbare Anwendung in Architekturskizzen oder Entscheidungsprotokollen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

A.8.28 **Sichere Codierung: Grundsätze für sicheres Programmieren werden bei der Softwareentwicklung angewendet.**

Woran man es festmacht: Neu in der Fassung 2022. Nachweis über verbindliche Coding-Regeln, statische Codeanalyse und Secret Scanning als verpflichtende CI-Gates, Nutzung geprüfter Bibliotheken sowie dokumentierte Code-Reviews. Bei fehlender Aufgabentrennung ersetzen erzwungene automatisierte Gates das Vier-Augen-Prinzip; das ist so zu begründen und mit der Pipeline-Konfiguration zu belegen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.29 **Sicherheitstests in Entwicklung und Abnahme: Prozesse für Sicherheitstests sind im Entwicklungslebenszyklus festgelegt und umgesetzt.**

Woran man es festmacht: Automatisierte Sicherheitstests in der Pipeline (Abhängigkeitsprüfung, statische und dynamische Analyse) plus periodischer Penetrationstest bei erhöhtem Schutzbedarf. Nachweis über Testberichte mit Datum und die Nachverfolgung der Befunde.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.30 **Ausgegliederte Entwicklung: Ausgelagerte Entwicklungstätigkeiten werden gesteuert, überwacht und überprüft.**

Woran man es festmacht: Bei Fremdentwicklung Sicherheitsanforderungen vertraglich festlegen, Codeeigentum und Prüfrecht sichern, Code-Reviews und Sicherheitstests vor Abnahme durchführen. Ohne ausgelagerte Entwicklung ist die Nichtanwendbarkeit in der SoA schlüssig zu begründen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.31 **Trennung von Entwicklungs-, Test- und Produktionsumgebungen: Entwicklungs-, Test- und Produktionsumgebungen sind getrennt und werden geschützt.**

Woran man es festmacht: Getrennte Konten, Projekte oder Namensräume, getrennte Zugangsdaten und getrennte Datenbestände. In Kombination mit A.8.11 sicherstellen, dass keine Produktionsdaten in nichtproduktive Umgebungen gelangen. Nachweis über die Umgebungsübersicht und die Rechtezuordnung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.32 **Änderungssteuerung: Änderungen an informationsverarbeitenden Einrichtungen und Informationssystemen unterliegen Verfahren zur Änderungssteuerung.**

Woran man es festmacht: Änderungsprozess mit Antrag, Auswirkungsbetrachtung, Test, Freigabe, Umsetzung und Rollback-Pfad. In Entwicklungsteams erfüllt eine Pull-Request-Pipeline mit erzwungenen Prüfungen und protokollierten Deployments diesen Punkt, wenn die Historie unveränderlich ist.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.33 **Testinformationen: Testinformationen sind angemessen ausgewählt, geschützt und verwaltet.**

Woran man es festmacht: Grundsatz: keine echten Personendaten in Testsystemen. Wo dies unvermeidbar ist, Freigabe, Maskierung, Zugriffsbeschränkung und Löschung nach dem Test dokumentieren. Nachweis über das Testdatenkonzept und die Löschprotokolle.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

A.8.34 **Schutz von Informationssystemen während Auditprüfungen: Auditprüfungen, die den Zugriff auf produktive Systeme umfassen, sind geplant und mit dem Management abgestimmt, um Störungen des Betriebs zu vermeiden.**

Woran man es festmacht: Auditvereinbarung mit Zeitfenster, Umfang, nur lesendem Zugriff wo möglich, Protokollierung der Auditzugriffe und Freigabe durch die Leitung. Gilt auch für Penetrationstests: eine schriftliche Testfreigabe mit Zeitfenster und Notfallkontakt ist der Nachweis.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung