Ordivis

ANLAGE · INFORMATIONSSICHERHEIT

Anlage: ISMS-Dokumentation nach ISO/IEC 27001

Das dokumentierte ISMS nach ISO/IEC 27001:2022 – Lenkung und Vorlagen

Produktversion 2026.09.20 · Handbuch-Revision 1.0
Stand 20.09.2026 · Plattform .NET 10 / Windows Server

ID-28a ISMS-DOK

Anlage: ISMS-Dokumentation nach ISO/IEC 27001

Ein Informationssicherheits-Managementsystem (ISMS) lebt nicht von guten Absichten, sondern von nachweisbaren Festlegungen. Die ISO/IEC 27001:2022 verlangt an mehreren Stellen ausdrücklich *„dokumentierte Information"* – also schriftlich festgehaltene Regeln, Verfahren und Nachweise. Wer eine Zertifizierung anstrebt oder gegenüber Auftraggebern, Aufsichtsbehörden und Versicherern belastbar sein will, kommt an dieser Dokumentation nicht vorbei.

Diese Anlage ist bewusst **eigenständig** gehalten: Sie beschreibt ausschließlich das dokumentierte ISMS und stellt für jedes Pflichtdokument eine ausformulierte **Vorlage** bereit. Das Modul Informationssicherheit (siehe Kapitel *ID-28 ISMS*) verwaltet die technische Seite – Kataloge, Schutzobjekte, Risiken, Prüfungen. Diese Anlage liefert das Papier drumherum, das ein Auditor sehen möchte.

> **Wichtig.** Ordivis IT liefert die Kataloge (ISO/IEC 27001 Annex A und BSI IT-Grundschutz) und die Werkzeuge zur Modellierung, Risikobewertung und Prüfung bereits mit. Die hier abgedruckten Vorlagen sind **Textbausteine für Ihre organisatorischen Dokumente** – sie ersetzen keine Rechtsberatung und keinen Auditor. Passen Sie jede Vorlage an Ihre Organisation an, bevor Sie sie in Kraft setzen.

INHALT

1 Wie die Dokumentation aufgebaut ist

Die ISMS-Dokumentation folgt einer bewährten **Vier-Ebenen-Pyramide**. Von oben nach unten wird sie konkreter und ändert sich häufiger:

Ebene	Art	Beispiele	Ändert sich
1	**Politik** (das *Warum*)	Informationssicherheitsleitlinie	selten
2	**Richtlinien** (das *Was*)	Zugriffs-, Krypto-, Lieferanten-Richtlinie	gelegentlich
3	**Verfahren & Prozesse** (das *Wie*)	Risikoverfahren, Incident-Prozess, Change-Prozess	regelmäßig
4	**Nachweise** (der *Beweis*)	Risikoregister, Auditberichte, Schulungsnachweise	laufend

> **Tipp.** Halten Sie die oberen Ebenen kurz und stabil, die unteren detailliert und lebendig. Eine Leitlinie über zwei Seiten, die zehn Jahre trägt, ist mehr wert als ein 40-seitiges Werk, das niemand liest.

Jedes Dokument trägt einen **Lenkungskopf** (siehe Vorlage 0), damit Version, Freigabe und Gültigkeit jederzeit nachvollziehbar sind. Das ist keine Förmelei: Die Norm verlangt in Abschnitt 7.5, dass dokumentierte Information *gekennzeichnet, geprüft, freigegeben und versioniert* ist.

2 Das Dokumentenregister – was die Norm verlangt

Die folgende Tabelle listet die dokumentierte Information, die ISO/IEC 27001:2022 fordert (Spalte *Pflicht*) sowie die in der Praxis üblichen ergänzenden Dokumente. Die Spalte *Klausel* verweist auf den Normabschnitt, *Vorlage* auf den Abschnitt dieser Anlage.

Nr.	Dokument	Klausel	Pflicht	Vorlage
D-01	Anwendungsbereich des ISMS (Scope)	4.3	ja	§5.1
D-02	Informationssicherheitsleitlinie	5.2	ja	§5.2
D-03	Rollen, Verantwortlichkeiten & Befugnisse	5.3	ja	§5.3
D-04	Verfahren zur Risikobeurteilung	6.1.2	ja	§5.4
D-05	Verfahren zur Risikobehandlung	6.1.3	ja	§5.5
D-06	Erklärung zur Anwendbarkeit (SoA)	6.1.3 d)	ja	§5.6
D-07	Risikobehandlungsplan	6.1.3 e)	ja	§5.7
D-08	Informationssicherheitsziele	6.2	ja	§5.8
D-09	Nachweis der Kompetenz	7.2	ja	§5.9
D-10	Risikobeurteilungsbericht (Ergebnisse)	8.2	ja	§5.10
D-11	Nachweis der Wirksamkeitsmessung	9.1	ja	§5.11
D-12	Internes Auditprogramm & -berichte	9.2	ja	§5.12
D-13	Managementbewertung (Protokoll)	9.3	ja	§5.13
D-14	Nichtkonformitäten & Korrekturmaßnahmen	10.2	ja	§5.14
D-15	Zugriffssteuerungsrichtlinie	A.5.15	empfohlen	§5.15
D-16	Richtlinie akzeptable Nutzung	A.5.10	empfohlen	§5.16
D-17	Lieferanten- & Cloud-Sicherheitsrichtlinie	A.5.19–5.23	empfohlen	§5.17
D-18	Kryptografie- & Schlüsselrichtlinie	A.8.24	empfohlen	§5.18
D-19	Incident-Management-Verfahren	A.5.24–5.28	empfohlen	§5.19
D-20	Betriebskontinuität (Bezug zum BCM)	A.5.29–5.30	empfohlen	§5.20

Achtung. Die Erklärung zur Anwendbarkeit (SoA, D-06) ist das Herzstück jeder Zertifizierung. Sie muss **alle 93 Controls des Annex A** aufführen und je Control begründen, ob es angewandt wird und warum (bzw. warum nicht). Ordivis IT erzeugt das Grundgerüst dieser Liste aus dem aktiven ISO-Katalog – die Begründungen tragen Sie ein.

3 Zuständigkeiten – wer erstellt und pflegt was

Dokument(e)	Erstellung	Freigabe	Pflege
D-01, D-02, D-08	ISB*	oberste Leitung	jährlich
D-03	ISB	oberste Leitung	bei Änderung
D-04, D-05, D-07, D-10	ISB / Risikoverantwortliche	ISB	pro Zyklus
D-06 (SoA)	ISB	oberste Leitung	pro Zyklus
D-09, D-11	ISB / Personal	ISB	laufend
D-12, D-13, D-14	interne Revision / ISB	Leitung	pro Ereignis
D-15 … D-20	Fachverantwortliche	ISB	bei Änderung

* ISB = Informationssicherheitsbeauftragte(r). In Ordivis IT existiert dafür die Systemrolle **ISB** mit allen `security.*`-Berechtigungen.

4 Lebenszyklus & Lenkung dokumentierter Information

1. **Entwurf** → Autor erstellt anhand der Vorlage, Status *Entwurf*.
2. **Prüfung** → fachliche und formale Prüfung, Kommentare eingearbeitet.
3. **Freigabe** → Freigabe durch die zuständige Stelle (siehe §3), Status *Gültig*, Version erhöht.
4. **Verteilung** → Bekanntgabe an den betroffenen Personenkreis.
5. **Überprüfung** → im festgelegten Turnus (i. d. R. jährlich) auf Aktualität geprüft.
6. **Außerkraftsetzung** → veraltete Fassungen als *Archiviert* gekennzeichnet, aber revisionssicher aufbewahrt.

Tipp. Bilden Sie ISMS-Dokumente als Configuration Items der CI-Klasse **Dokument/Richtlinie** in der CMDB ab (Governance-&-Compliance-Klassen, BSI-07). So haben Sie Version, Eigentümer und Wiedervorlage an einem Ort und können Dokumente mit Schutzobjekten verknüpfen.

5 Die Vorlagen

Die folgenden Vorlagen sind vollständig ausformuliert. Ersetzen Sie die in **«Spitzklammern»** gesetzten Platzhalter durch Ihre Angaben. Textteile in *kursiv* sind Ausfüllhinweise und werden vor Inkraftsetzung entfernt.

5.0 Vorlage 0 – Lenkungskopf (für jedes Dokument)

Jedes ISMS-Dokument beginnt mit diesem Kopf:

Feld	Inhalt
Dokumenttitel	«z. B. Informationssicherheitsleitlinie»
Dokumentnummer	«D-02»
Version	«1.0»
Klassifizierung	«intern / vertraulich»
Eigentümer	«Rolle/Person»
Erstellt von / am	«Name», «TT.MM.JJJJ»
Geprüft von / am	«Name», «TT.MM.JJJJ»
Freigegeben von / am	«Leitung», «TT.MM.JJJJ»
Gültig ab	«TT.MM.JJJJ»
Nächste Überprüfung	«TT.MM.JJJJ»

Änderungshistorie

Version	Datum	Autor	Änderung
1.0	«TT.MM.JJJJ»	«Name»	Erstfassung

5.1 D-01 – Anwendungsbereich des ISMS (Scope)

Zweck: Legt fest, welche Teile der Organisation, welche Standorte, Prozesse und Werte das ISMS abdeckt (Klausel 4.3). Der Scope ist die Grenze, innerhalb derer alle weiteren Festlegungen gelten.

1. Organisation. Das ISMS gilt für «Organisation/Gesellschaft», nachfolgend „die Organisation".

2. Eingeschlossene Bereiche. Vom ISMS erfasst sind: - Standorte: «z. B. Hauptsitz Musterstadt, Rechenzentrum X» - Organisationseinheiten: «z. B. IT-Betrieb, Entwicklung, Kundenservice» - Geschäftsprozesse: «z. B. Betrieb der SaaS-Plattform, Kundendatenverarbeitung» - Informationswerte: «z. B. Kundendaten, Quellcode, Betriebsdokumentation»

3. Ausgeschlossene Bereiche und Begründung. Nicht erfasst sind «Bereich» *(Begründung: «…»)*.

4. Schnittstellen & Abhängigkeiten. Externe Abhängigkeiten mit Sicherheitsrelevanz: «z. B. Cloud-Provider, Managed-Service-Dienstleister, Zahlungsdienstleister».

5. Interessierte Parteien und deren Anforderungen (Klausel 4.2): «Kunden (Vertraulichkeit), Aufsicht (DSGVO/NIS-2), Versicherer (Mindeststandards)».

> **Wichtig.** Der Scope muss zum Zertifikat passen: Nur was hier steht, wird geprüft und zertifiziert. Ein zu weiter Scope überfordert, ein zu enger entwertet das Zertifikat.

5.2 D-02 – Informationssicherheitsleitlinie

Zweck: Das oberste Bekenntnis der Leitung zur Informationssicherheit (Klausel 5.2). Kurz, verbindlich, von der Geschäftsführung unterschrieben.

Präambel. Informationen sind ein wesentlicher Wert der «Organisation». Ihr Schutz hinsichtlich **Vertraulichkeit, Integrität und Verfügbarkeit** ist Grundlage unseres Geschäfts und unserer Vertrauenswürdigkeit. Die Leitung bekennt sich zu einem systematischen Informationssicherheits-Management nach ISO/IEC 27001.

Grundsätze. 1. Informationssicherheit ist Leitungsaufgabe und Teil aller Geschäftsprozesse. 2. Wir beurteilen Risiken systematisch und behandeln sie nach festgelegten Kriterien. 3. Gesetzliche, vertragliche und regulatorische Anforderungen werden eingehalten. 4. Jede/r Beschäftigte trägt Verantwortung und wird geschult. 5. Sicherheitsvorfälle werden gemeldet, bearbeitet und ausgewertet. 6. Wir verbessern das ISMS fortlaufend (PDCA).

Ziele. Konkrete, messbare Ziele sind im Dokument D-08 festgelegt.

Verbindlichkeit. Diese Leitlinie ist für alle Beschäftigten und für Dritte im Geltungsbereich verbindlich. Verstöße werden gemäß «Regelung» geahndet.

Freigabe. «Ort, Datum» – «Name, Funktion (Geschäftsführung)» – Unterschrift: ___

5.3 D-03 – Rollen, Verantwortlichkeiten & Befugnisse

Zweck: Weist die sicherheitsrelevanten Rollen zu (Klausel 5.3).

Rolle	Verantwortung	Besetzt mit
Oberste Leitung	Gesamtverantwortung, Ressourcen, Freigaben	«Name»
Informationssicherheitsbeauftragte(r) (ISB)	Betrieb & Steuerung des ISMS	«Name»
Risikoeigentümer	Bewertung/Behandlung „ihrer" Risiken	«Bereich»
IT-Betrieb	Umsetzung technischer Maßnahmen	«Team»
Datenschutzbeauftragte(r)	Schnittstelle DSGVO	«Name»
Alle Beschäftigten	Einhaltung, Meldung von Vorfällen	–

> **Tipp.** In Ordivis IT bildet die Rolle **ISB** die/den Informationssicherheitsbeauftragte(n) technisch ab. Weisen Sie sie in der Benutzerverwaltung genau den Personen zu, die hier benannt sind.

5.4 D-04 – Verfahren zur Risikobeurteilung

Zweck: Legt fest, wie Risiken identifiziert, analysiert und bewertet werden (Klausel 6.1.2) – reproduzierbar und vergleichbar.

1. Methode. Risiken werden je Schutzobjekt aus **Gefährdung** × **Schwachstelle** abgeleitet und nach **Eintrittshäufigkeit** und **Schadenshöhe** bewertet.

2. Bewertungsskala. Je Dimension 1–5; das Risiko ergibt sich als Produkt (1–25):

Risikowert	Kategorie	Bedeutung
1–4	akzeptabel	keine weitere Maßnahme nötig
5–12	tragbar	Maßnahmen prüfen
13–25	kritisch	Behandlung verbindlich, Freigabe durch Leitung

3. Gefährdungsbasis. Grundlage sind die **47 elementaren Gefährdungen des BSI** sowie der **Enterprise-Gefährdungskatalog** (moderne Risiken: Supply-Chain, Cloud, KI, Regulatorik). Beide sind in Ordivis IT hinterlegt.

4. Ablauf. Schutzbedarf feststellen → Gefährdungen zuordnen → bewerten → dokumentieren → Ergebnis in Bericht D-10.

5. Turnus. Mindestens jährlich sowie bei wesentlichen Änderungen.

> **Wichtig.** Ordivis IT setzt genau dieses Verfahren um: 5×5-Bewertung, Kategorien, Heat-Map und automatische Benachrichtigung bei kritischem Restrisiko. Dieses Dokument beschreibt die *Regel*, das Modul liefert die *Durchführung*.

5.5 D-05 – Verfahren zur Risikobehandlung

Zweck: Wie mit bewerteten Risiken umgegangen wird (Klausel 6.1.3).

Strategien. Für jedes nicht akzeptable Risiko wird eine Strategie gewählt: - **Reduzieren** – Maßnahmen (Controls) umsetzen. - **Vermeiden** – die risikobehaftete Tätigkeit einstellen. - **Übertragen** – z. B. Versicherung, Auslagerung mit vertraglicher Absicherung. - **Akzeptieren** – bewusste, dokumentierte und **freigegebene** Hinnahme des Restrisikos.

Restrisiko. Nach Behandlung wird das Restrisiko erneut bewertet. Kritische Restrisiken bedürfen der **ausdrücklichen Freigabe durch die oberste Leitung**.

Auswahl der Maßnahmen. Maßnahmen werden aus dem Annex A (bzw. BSI-Bausteinen) abgeleitet; die Auswahl wird in der SoA (D-06) begründet und im Risikobehandlungsplan (D-07) terminiert.

5.6 D-06 – Erklärung zur Anwendbarkeit (Statement of Applicability, SoA)

Zweck: Führt alle 93 Annex-A-Controls auf und begründet je Control Anwendung/Ausschluss (Klausel 6.1.3 d). Das zentrale Prüfdokument.

Aufbau je Zeile:

Control	Titel	Anwendbar	Umsetzungs-status	Begründung / Ausschlussgrund	Nachweis
A.5.1	Informationssicherheits-richtlinien	ja	umgesetzt	Leitlinie D-02 in Kraft	D-02
A.5.7	Threat Intelligence	ja	in Umsetzung	Prozess im Aufbau	«…»
A.8.23	Web-Filter	nein	–	keine Web-Nutzung im Scope	–

Control	Titel	Anwendbar	Umsetzungs-status	Begründung / Ausschlussgrund	Nachweis
…	*(alle 93 Controls)*				

Achtung. Kein Annex-A-Control darf fehlen. Ausschlüsse sind zulässig, müssen aber **sachlich begründet** sein („nicht anwendbar, weil …"). „Vergessen" ist kein Ausschlussgrund.

Tipp. Ordivis IT erzeugt das SoA-Grundgerüst aus dem aktiven ISO-Katalog und dem Modellierungsstand. Exportieren Sie die Liste, ergänzen Sie Begründung und Nachweis, und legen Sie sie als freigegebenes Dokument ab.

5.7 D-07 – Risikobehandlungsplan

Zweck: Der terminierte Maßnahmenplan (Klausel 6.1.3 e).

Nr.	Risiko	Maßnahme (Control)	Verantwortlich	Frist	Status	Restrisiko
1	«R-…»	«A.8.x – …»	«Name»	«TT.MM.JJJJ»	offen	«Kat.»

Wichtig. Ordivis IT führt diesen Plan als *Grundschutz-Check*-Maßnahmen bzw. Risikobehandlung im Modul – Status *offen → in Arbeit → umgesetzt → verifiziert*. Der ausgedruckte Maßnahmenplan-Bericht aus Ordivis IT ist der Nachweis zu diesem Dokument.

5.8 D-08 – Informationssicherheitsziele

Zweck: Messbare Ziele je Planungszeitraum (Klausel 6.2).

Ziel	Kennzahl	Ausgangswert	Zielwert	Frist	Verantwortlich
Phishing-Resistenz erhöhen	Klickrate Testphishing	«18 %»	«< 5 %»	«Q4»	ISB
Patch-Rückstand senken	offene kritische CVEs	«30»	«0»	«laufend»	IT-Betrieb
Awareness	geschulte MA	«60 %»	«100 %»	«Q3»	Personal

Ziele sind **spezifisch, messbar, terminiert** und werden in der Managementbewertung (D-13) überprüft.

5.9 D-09 – Nachweis der Kompetenz & Awareness

Zweck: Beleg, dass Beteiligte kompetent und sensibilisiert sind (Klausel 7.2/7.3).

Person/Rolle	Erforderliche Kompetenz	Nachweis	Datum	Nächste Auffrischung
ISB	ISO-27001-Grundlagen	«Zertifikat»	«…»	«…»
Alle MA	Security-Awareness	Schulungsteilnahme	«…»	jährlich

5.10 D-10 – Risikobeurteilungsbericht

Zweck: Dokumentiertes Ergebnis der Risikobeurteilung (Klausel 8.2).

Enthält: Stichtag, betrachteter Scope, angewandtes Verfahren (Verweis D-04), **Risikoregister** (alle Risiken mit Brutto-/Restwert und Kategorie), Heat-Map und Gesamteinschätzung der Risikolage.

> **Tipp.** Das **Risikoregister-PDF** aus Ordivis IT (farbcodiert nach Kategorie, mit Heat-Map) erfüllt diesen Zweck unmittelbar. Ergänzen Sie ein kurzes Vorwort und die Freigabe.

5.11 D-11 – Nachweis der Wirksamkeitsmessung (Monitoring)

Zweck: Beleg, dass die Wirksamkeit gemessen wird (Klausel 9.1).

Was wird gemessen	Methode	Turnus	Ergebnis	Verantwortlich
Umsetzungsgrad Controls	Grundschutz-Check-Fortschritt	quartalsweise	«xx %»	ISB
Risikolage	Anzahl kritischer Risiken	monatlich	«n»	ISB
Vorfälle	Incident-Statistik	monatlich	«n»	IT-Betrieb

> **Tipp.** Das **ISMS-Dashboard** in Ordivis IT liefert Schutzbedarfsverteilung, Check-Fortschritt und Risikolage auf einen Blick – die laufende Datengrundlage für diesen Nachweis.

5.12 D-12 – Internes Auditprogramm & Auditbericht

Zweck: Planung und Ergebnis interner Audits (Klausel 9.2).

Auditprogramm (Jahresplan)

Audit	Bereich/Controls	Termin	Auditor	Status
A-1	A.5 organisatorisch	«Q1»	«Name (unabhängig)»	geplant

Auditbericht (je Audit): Ziel & Umfang, Kriterien, Feststellungen (Konformitäten/Abweichungen), Empfehlungen, Fazit. Abweichungen fließen in D-14 ein.

> **Wichtig.** Der Auditor muss vom geprüften Bereich **unabhängig** sein. In kleinen Organisationen ist ein externer Dienstleister oft die praktikabelste Lösung.

5.13 D-13 – Managementbewertung (Management Review)

Zweck: Regelmäßige Bewertung des ISMS durch die Leitung (Klausel 9.3). Mindestens jährlich.

Pflicht-Eingaben (Agenda): 1. Status offener Maßnahmen aus der letzten Bewertung 2. Änderungen interner/externer Themen 3. Rückmeldungen zur Sicherheitsleistung (Kennzahlen D-11) 4. Ergebnisse von

Audits (D-12) 5. Erfüllungsgrad der Ziele (D-08) 6. Vorfälle & Nichtkonformitäten (D-14) 7. Rückmeldungen interessierter Parteien 8. Verbesserungsmöglichkeiten

Pflicht-Ergebnisse (Beschlüsse): Verbesserungsentscheidungen, Ressourcenbedarf, angepasste Ziele.

Protokoll: Teilnehmer, Datum, behandelte Punkte, **Beschlüsse mit Verantwortlichen und Fristen**.

5.14 D-14 – Nichtkonformitäten & Korrekturmaßnahmen

Zweck: Umgang mit Abweichungen (Klausel 10.2).

Nr.	Abweichung	Quelle	Sofortmaßnahme	Ursachenanalyse	Korrekturmaßnahme	Frist	Wirksamkeit geprüft
N-1	«…»	Audit A-1	«…»	«…»	«…»	«…»	«ja/nein»

Wichtig. Nicht nur den Symptom beheben, sondern die **Ursache** – sonst kehrt die Abweichung zurück. Die Wirksamkeit der Korrektur ist zu prüfen und zu dokumentieren.

5.15 D-15 – Zugriffssteuerungsrichtlinie

Bezug: A.5.15/A.5.18/A.8.2 f. Regelt, wer worauf zugreifen darf.

Kernfestlegungen: **Need-to-know** und **least privilege**; rollenbasierte Rechtevergabe; Genehmigung und Entzug von Zugängen; regelmäßige **Rezertifizierung** der Rechte; besondere Kontrolle **privilegierter** Konten; MFA für «Systeme». Verantwortlich: «Rolle». Überprüfung: jährlich.

5.16 D-16 – Richtlinie zur akzeptablen Nutzung

Bezug: A.5.10. Was Nutzer mit Informationen und Mitteln dürfen – und was nicht.

Regelt u. a.: dienstliche vs. private Nutzung, Umgang mit E-Mail/Internet, Clean-Desk/Clear-Screen, Umgang mit mobilen Geräten und Wechseldatenträgern, Verbot ungenehmigter Cloud-/KI-Tools (Schatten-IT), Meldepflicht bei Vorfällen. Von jeder/m Beschäftigten zu **bestätigen**.

5.17 D-17 – Lieferanten- & Cloud-Sicherheitsrichtlinie

Bezug: A.5.19–A.5.23. Sicherheit in der Lieferkette und bei Cloud-Diensten.

Festlegungen: Sicherheitsanforderungen in Verträgen/AVV; Bewertung von Dienstleistern vor Beauftragung; Umgang mit **Nth-Party**-Abhängigkeiten; Regelung der geteilten Verantwortung (Shared Responsibility) bei Cloud; Exit-/Rückführungsstrategie gegen Vendor-Lock-in; regelmäßige Überprüfung der Dienstleister.

5.18 D-18 – Kryptografie- & Schlüsselrichtlinie

Bezug: A.8.24. Einsatz von Verschlüsselung und Verwaltung von Schlüsseln.

Festlegungen: zugelassene Verfahren/Schlüssellängen; Verschlüsselung ruhender und übertragener Daten; **Schlüssellebenszyklus** (Erzeugung, Verteilung, Aufbewahrung, Rotation, Vernichtung); Zuständigkeiten; Vorbereitung auf **Post-Quantum**-Migration langlebig vertraulicher Daten.

5.19 D-19 – Incident-Management-Verfahren

Bezug: A.5.24–A.5.28. Wie Sicherheitsvorfälle behandelt werden.

Ablauf: **Erkennen** → **Melden** → **Klassifizieren** → **Eindämmen** → **Beheben** → **Wiederherstellen** → **Auswerten** (Lessons Learned). Meldewege und Erreichbarkeiten, Eskalationsstufen, Beweissicherung, gesetzliche Meldepflichten (z. B. DSGVO 72 h, NIS-2). Verzahnung mit dem Service-Desk/Ticketing.

5.20 D-20 – Betriebskontinuität (Bezug zum BCM)

Bezug: A.5.29–A.5.30. Aufrechterhaltung der Informationssicherheit in Störungen.

Verweist auf das **BCM-Modul** (BSI 200-4 / ISO 22301): BIA, Notfallpläne, RTO/RPO, Wiederanlaufreihenfolge. Diese Richtlinie stellt sicher, dass Sicherheit auch im Notbetrieb gewahrt bleibt (z. B. Zugriffskontrolle bei Ausweichlösungen).

6 Startpaket – die Reihenfolge der Einführung

Wer ein ISMS neu aufbaut, geht in dieser Reihenfolge vor:

1. **Scope** (D-01) und **Leitlinie** (D-02) festlegen und freigeben.
2. **Rollen** (D-03) besetzen – ISB benennen.
3. **Risikoverfahren** (D-04/D-05) beschließen.
4. Schutzobjekte in Ordivis IT modellieren, **Risiken bewerten** → Bericht D-10.
5. **SoA** (D-06) erstellen, **Behandlungsplan** (D-07) terminieren.
6. **Ziele** (D-08) setzen, **Awareness** (D-09) starten.
7. Betrieb: **Monitoring** (D-11), **Audit** (D-12), **Review** (D-13), **Korrekturen** (D-14).
8. Ergänzende Richtlinien (D-15 ff.) nach Bedarf und Risikolage.

> **Tipp.** Fangen Sie klein an: ein enger, sauberer Scope mit vollständiger Dokumentation ist mehr wert als ein breiter Scope mit Lücken. Erweitern lässt sich später jederzeit.

7 Verweise

- Kapitel **ID-28 ISMS** – Bedienung des Moduls Informationssicherheit.
- Kapitel **ID-29 BCM** – Betriebskontinuität und Notfallplanung.
- Kapitel **ID-44 Rollen & Rechte** – Systemrolle ISB und Berechtigungen.
- ISO/IEC 27001:2022 und ISO/IEC 27002:2022 (Umsetzungsleitfaden Controls) – bei der jeweiligen Normungsstelle zu beziehen.

Verwandte Themen

- **ID-28 – Modul Informationssicherheit (ISMS)** – das Modul, mit dem diese Dokumente gepflegt werden
- **ID-29 – Modul Business Continuity Management** – Fortführungspläne als Nachweis zu A.5.29 f.
- **ID-32 – Modul Datenschutz (Art. 30 DSGVO)** – gemeinsame Nachweise mit dem Datenschutz
- **ID-44 – Rollen- & Rechte-Matrix** – Rechte für Lenkung und Freigabe