Ordivis

MODUL · INFORMATIONSSICHERHEIT

Modul Informationssicherheit (ISMS)

ISMS nach BSI IT-Grundschutz und ISO/IEC 27001 in einem Modul

Produktversion 2026.08.19 · Handbuch-Revision 1.0
Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-28 ISMS

Modul Informationssicherheit (ISMS)

Informationssicherheit ist mehr als ein Virenscanner. Es geht um die Frage, wie eine Organisation ihre Daten und Systeme planvoll schützt: Welche Informationen sind besonders schützenswert? Welche Gefahren drohen ihnen? Welche Maßnahmen sind getroffen, und wer ist dafür verantwortlich? Ohne System bleibt das Stückwerk – hier eine Regel, dort eine Vorkehrung, aber kein belastbares Gesamtbild und kein Nachweis gegenüber Prüfern.

Ein *ISMS* (Informationssicherheits-Managementsystem) ist der organisierte Rahmen für genau diese Fragen. Statt das Rad neu zu erfinden, stützt man sich dabei auf anerkannte Regelwerke. Zwei sind hier hinterlegt: der BSI IT-Grundschutz aus Deutschland und der internationale Standard ISO/IEC 27001. Beide liefern Kataloge von Anforderungen (sogenannte Controls oder Bausteine), die man Schritt für Schritt umsetzt und dokumentiert. Das Modul führt diese Kataloge, verknüpft sie mit den Schutzobjekten aus der CMDB und hält Umsetzungsstand, Risiken und Nachweise an einem Ort fest.

INHALT

1 Zweck & Nutzen

- Strukturierte Umsetzung von Sicherheitsanforderungen.
- Nachweise für Audits und Zertifizierung.
- Verzahnung mit CMDB (Schutzobjekte) und Risiken.

2 Frameworks & Kataloge

Der **Sicherheitskatalog** zeigt die Einträge des gewählten Frameworks links als Liste und rechts das Detail zum markierten Eintrag. Welches Framework Sie sehen, steuert das Feld *Katalog* in der Kopfzeile – siehe Abbildung 1.

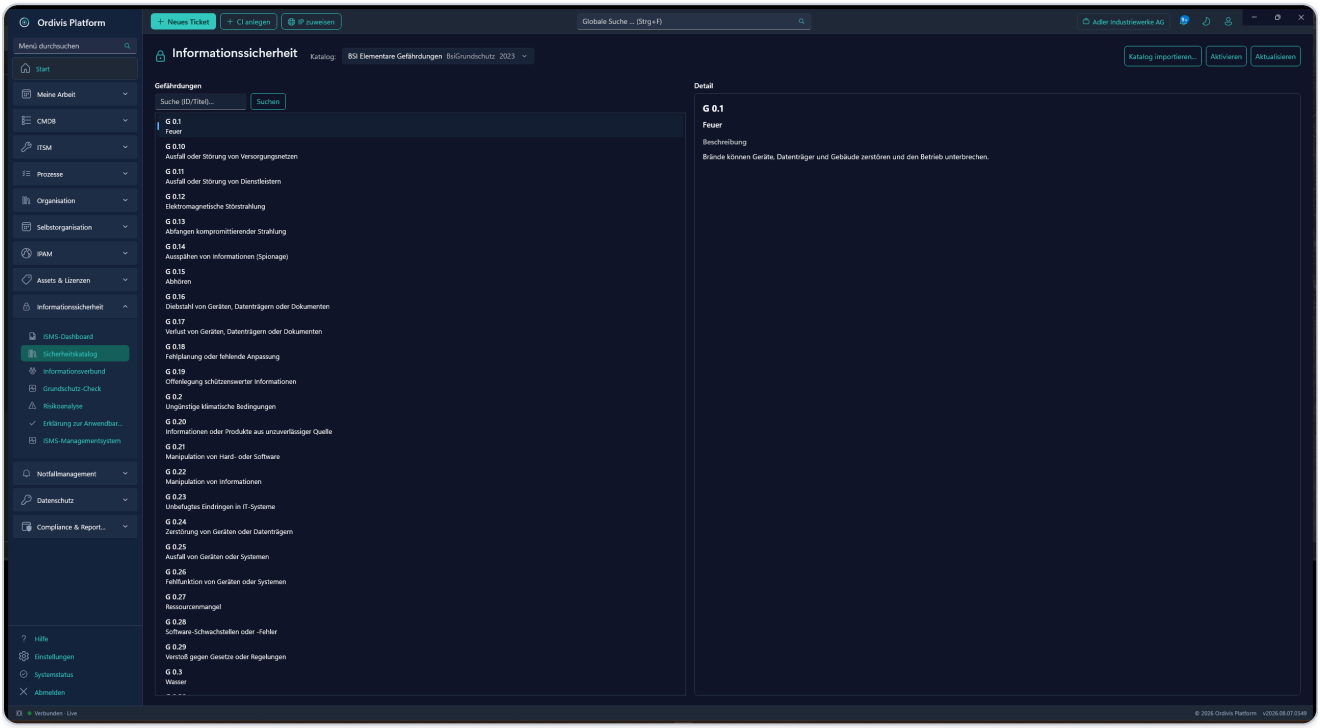

Abb. 1 – Sicherheitskatalog, hier mit dem Katalog *BSI Elementare Gefährdungen*: links die Einträge, rechts das Detail. Über *Katalog* wechseln Sie zu ISO/IEC 27001.

- **BSI IT-Grundschutz:** Bausteine, Anforderungen, Vererbungs-Engine.
- **ISO/IEC 27001:** 93 Annex-A-Controls + Klauseln 4–10 werden mit der Auslieferung geseedet und je Framework aktiviert (verdrängt BSI nicht).

> **Hinweis:** Ordivis Platform enthält **keinen ISO-Normtext**, sondern Titel und eigene Erläuterungen zu jedem Control. Den Normtext beziehen Sie separat beim Herausgeber.

2.1 BSI Grundschutz++ automatisch aktuell halten

Der Katalog **BSI Grundschutz++** kann automatisch mit der offiziellen BSI-Quelle abgeglichen werden:

- Ein täglicher Hintergrund-Job vergleicht den aktiven Katalog per Prüfsumme mit der veröffentlichten Fassung.
- Bei einer Abweichung wird der Katalog-Verantwortliche (`security.catalog.manage`) per In-App-Benachrichtigung und E-Mail informiert – **kein stiller Wechsel**.
- Die neue Fassung wird erst **nach Bestätigung** übernommen; eigene Anpassungen (Tailoring) bleiben erhalten. So bleibt der Katalogstand jederzeit revisionssicher nachvollziehbar.

Konfiguration: `Security:BsiCatalog` (Auto-Prüfung an/aus, Quell-URL).

2.2 Referenzen des BSI – fertige Begründungen und Rahmenwerk-Zuordnungen

💻 **Client:** *Informationssicherheit ▸ Referenzen des BSI* · 🔑 `security.check.read` zum Lesen, `security.catalog.manage` zum Einlesen, `security.check.write` zum Bestätigen

Die BSI-Bibliothek enthält mehr als den Katalog. Zwei weitere Schichten nimmt Ordivis seit diesem Release **auf** – vorher hat es sie nur erzeugt:

Komponentendefinitionen beschreiben je Produkt, welche Anforderungen es umsetzt und **wie**. Für Keycloak, Netzarchitektur, Passwortrichtlinie, Lieferkettensicherheit und das GA-Lotse-Grundmodul liegen sie fertig vor. Wer eine dieser Komponenten betreibt, findet die Begründung zu den betroffenen Anforderungen bereits ausformuliert vor, statt sie selbst zu schreiben.

Rahmenwerk-Zuordnungen verbinden ISO 27001 Annex A und den früheren IT-Grundschutz mit Grundschutz++. Wer beides betreibt – für die öffentliche Verwaltung der Regelfall, sobald eine Zertifizierung dazukommt –, sieht damit, welche Umsetzung beide Rahmenwerke beantwortet.

🔒 **Pflichtreihenfolge** – ohne eingelesenen Katalog gibt es nichts, worauf sich die Verweise beziehen könnten.

1. Öffnen Sie *Informationssicherheit ▸ Referenzen des BSI*.
2. Wählen Sie unter *Komponentendefinitionen* eine Quelle und klicken Sie auf *Aus der BSI-Bibliothek laden*. Ohne Weg ins Internet laden Sie die Datei stattdessen als Datei hoch.
3. Wiederholen Sie das unter *Rahmenwerk-Zuordnungen*.
4. Geben Sie unten die Kennung einer Anforderung ein (z. B. `BER.1.4`) und klicken Sie auf *Suchen*.
5. Prüfen Sie den vorgeschlagenen Text und klicken Sie auf *Bestätigt*, wenn er für Ihre Installation zutrifft.

✅ **Ergebnis:** Der bestätigte Text steht als Umsetzung dieser Institution zur Verfügung. Solange er nicht bestätigt ist, bleibt er sichtbar als *Vorschlag* markiert.

⚠️ **Ein Vorschlag ist keine Umsetzung.** Das BSI sagt ausdrücklich, dass Komponentendefinitionen Referenzen sind und „nicht das Handeln der für die Informationssicherheit verantwortlichen Stelle" ersetzen. Ordivis übernimmt deshalb nichts von selbst.

⚠️ **Nicht jeder Verweis passt zu Ihrem Katalogstand.** Die oberen Schichten des BSI verweisen auf den Stand, gegen den sie geschrieben wurden. Was sich in Ihrem Katalog nicht wiederfindet, wird **gezählt und angezeigt** statt weggelassen – eine Meldung „vollständig", die einen Teil verschweigt, wäre schlimmer als die ehrliche Zahl. Gemessen an der Fassung vom 13.08.2026 lösen sich 34 von 43 Keycloak-Verweisen auf und 293 von 365 Zuordnungszielen.

⚠️ **Der Beziehungstyp gehört gelesen.** Nur *gleichwertig* trägt eine Umsetzung unverändert von einem Rahmenwerk ins andere. Bei *deckt nur einen Teil ab* und *überschneidet sich teilweise* bleibt Arbeit übrig. Ordivis zeigt den Typ im Klartext und macht daraus **kein** Häkchen – in der ISO-Sammlung sind nur 16 von 96 Zuordnungen gleichwertig.

⚠️ **Entwurfsstand:** Trägt eine Komponentendefinition „Entwurf" im Titel, steht das an der Oberfläche. Die Keycloak-Definition ist im August 2026 genau so eine.

3 Schutzbedarf & Vererbung

Sie definieren den **Schutzbedarf** (Vertraulichkeit, Integrität, Verfügbarkeit) an Objekten. Eine **Vererbungs-Engine** propagiert Schutzbedarf entlang von Abhängigkeiten (z. B. Dienst → Server).

4 Controls & Maßnahmen umsetzen

💻 **Client:** *Informationssicherheit* ▸ *Sicherheitskatalog* · 🌐 **Portal:** *Informationssicherheit* ▸ *ISMS-Arbeitsplatz* · 🔑 `security.report.read` zum Lesen, `security.manage` zum Pflegen

🔒 **Pflichtreihenfolge** — das **Framework** bestimmt, welche Controls und Bausteine überhaupt angeboten werden. BSI-Bausteine und ISO-Controls sind nicht dieselbe Liste; ein Wechsel nach dem Erfassen ordnet die Nachweise nicht um.

1. Wählen Sie das **Framework** (BSI oder ISO 27001).
2. Öffnen Sie einen **Control/Baustein**.
3. Erfassen Sie **Umsetzungsstatus**, Verantwortliche und Nachweise.
4. Verknüpfen Sie die betroffenen **CIs/Assets**.
5. Speichern Sie.

✅ **Ergebnis:** Der Umsetzungsstand fließt in die Erklärung zur Anwendbarkeit (SoA) und in den Grundschutz-Check ein – Sie erfassen ihn einmal und weisen ihn mehrfach nach.

Tipp: Ein Nachweis ohne Datei ist im Audit keiner. Hängen Sie das Dokument an, das die Umsetzung belegt, statt sie nur zu behaupten.

5 ISMS-Kontext & Geltungsbereich (ISO 27001, 4.2/4.3/5.2)

Jeder **Informationsverbund** trägt seinen ISO-Kontext als dokumentierte Information: die **Geltungsbereichs-Erklärung** (Grenzen und Anwendbarkeit, 4.3), die **interessierten Parteien** samt Anforderungen (4.2) und die **Informationssicherheits-Leitlinie** (5.2). Sie pflegen diese Felder über die Schaltfläche **„ISMS-Kontext"** auf der Verbund-Seite – sie sind die Grundlage für Scope-Statement und Zertifizierungsnachweis.

6 Risiken & Risikobehandlungsplan (ISO 27001, 6.1.3 / 8.3)

Erfassen und bewerten Sie **Risiken** (Eintrittswahrscheinlichkeit × Auswirkung), hinterlegen Maßnahmen und verfolgen deren Wirkung. Über **„Behandlungsplan"** legen Sie je Risiko die Behandlungsstrategie fest (Vermeiden / Reduzieren / Übertragen / Akzeptieren) und **verknüpfen die umsetzenden Annex-A-Controls**.

> **Wichtig:** Bei der Strategie **„Reduzieren"** muss mindestens ein Annex-A-Control verknüpft sein – sonst gilt das Risiko als unbehandelt, und die Anwendung lehnt das Speichern ab (ISO 27001, 6.1.3). Die formale **Restrisiko-Akzeptanz** durch die Leitung wird gesondert dokumentiert.

6.1 Risiken aus anderen Quellen

Zwei Analysen entstehen nicht von Hand, sondern werden befüllt. Sie tragen sprechende Namen und liegen im jeweiligen Informationsverbund:

Analyse	Quelle	Bewertung
Kontinuitäts-Gaps (BCM)	offene Wiederanlauf-Unterdeckungen (RTA > RTO) aus dem BCM-Modul	Schadenshöhe aus der BIA
Schwachstellen (Scan)	gemeldete CVE-/WID-Befunde eines angebundenen Werkzeugs	Schadenshöhe aus dem CVSS-Basiswert

Beide Wege sind **idempotent**: Derselbe Befund am selben Objekt aktualisiert sein Risiko, statt ein zweites anzulegen. Dieselbe Schwachstelle auf zwei Rechnern ergibt dagegen **zwei** Risiken – sie werden getrennt behandelt und getrennt geschlossen.

Die Abbildung CVSS → Schadenshöhe folgt den CVSS-v3-Schweregradbändern (≥ 9,0 → 5; ≥ 7,0 → 4; ≥ 4,0 → 3; > 0 → 2). **Fehlt der Wert, wird 3 („mittel") angesetzt** – ein Befund ohne Bewertung ist unbekannt, nicht harmlos.

> **Was NICHT übertragen wird:** Nur die Referenz kommt an – Kennung, Titel, betroffenes Bauteil, CVSS und Fundzeitpunkt. Keine Exploit-Details. Ein Betriebsdatenbestand ist kein Ort für Anleitungen.

Ein Befund wird nur dann an ein **Zielobjekt** gehängt, wenn dieses Objekt in diesem Verbund tatsächlich im Betrachtungsbereich liegt. Sonst bleibt er ein Risiko der Analyse mit dem Rechnernamen im Text – ein Zielobjekt aus einem fremden Verbund zu verknüpfen wäre fachlich falsch.

7 Erklärung zur Anwendbarkeit (SoA) (ISO 27001, 6.1.3 d)

Das **Statement of Applicability** ist das zentrale Zertifizierungs-Artefakt. Die SoA-Matrix führt **alle 93 Annex-A-Controls** und wird automatisch vorbefüllt (Standard: anwendbar, Umsetzungsstatus aus dem Grundschutz-Check abgeleitet). Je Control halten Sie fest: **anwendbar ja/nein**, **Begründung** für Ein- oder Ausschluss, Umsetzungsstatus und Verantwortliche.

> **Wichtig:** Ein **Ausschluss ohne Begründung** ist unzulässig und wird abgewiesen. Die vollständige SoA lässt sich als **versioniertes PDF** exportieren.

8 ISMS-Betrieb & -Bewertung (ISO 27001, Klauseln 6.2/7.5/9/10)

Die Seite **„ISMS-Managementsystem"** bündelt die Management-System-Schicht, die ISO von einer reinen Control-Checkliste unterscheidet:

- **Ziele & Kennzahlen (6.2/9.1):** messbare ISMS-Ziele mit KPI, Zielwert und Fortschritt.
- **Internes Audit (9.2):** Audit-Findings (Nichtkonformität / Beobachtung / Verbesserungspotential); ein Finding lässt sich in eine Nichtkonformität überführen.
- **Managementbewertung (9.3):** Inputs (Audit-Ergebnisse, Risiken, Ziele) und Beschlüsse/Outputs, mit **Freigabe durch die Leitung**.
- **Nichtkonformitäten & Korrekturmaßnahmen (10.1/10.2):** Ursachenanalyse → Korrekturmaßnahme → **Wirksamkeitsprüfung**. Eine Nichtkonformität kann erst **nach dokumentierter Wirksamkeitsprüfung** geschlossen werden.
- **Dokumentenlenkung (7.5):** Register der verbindlich dokumentierten Information mit Version, Owner und Freigabestatus.

9 Zertifizierungs-Readiness & Berichte (ISO 27001)

Das **Readiness-Dashboard** zeigt eine **„Stage-1-bereit"-Ampel**: SoA-Vollständigkeit, Abdeckung der Management-System-Klauseln 4–10, offene Nichtkonformitäten und die Pflichtdokumenten-Checkliste – inklusive Hinweis auf offene Lücken. Als PDF erzeugen Sie: **SoA**, **Risikobehandlungsplan**, **Internes-Audit-Bericht** und **Management-Review-Protokoll**.

10 Export & Nachweise

Der **OSCAL-Export** stellt Kontroll- und Umsetzungsdaten in einem maschinenlesbaren Standardformat bereit. Profile bündeln relevante Controls je Anwendungsbereich.

11 Abgrenzung zu BCM & DR

Das ISMS betrachtet **Sicherheit** (Schutzziele, Controls, Risiken). **Geschäftsfortführung** und **Wiederanlauf** behandeln die Module BCM (ID-29) und DR-Planung (ID-30) – eng verzahnt.

12 Rollen & Rechte (Auszug)

Recht	Erlaubt
`security.check.read`	ISMS-Daten ansehen (Katalog, Verbünde, SoA, Readiness)
`security.scope.manage`	Informationsverbünde und ISMS-Kontext pflegen
`security.assessment.manage`	Schutzbedarf und SoA-Einträge pflegen
`security.risk.manage`	Risiken und Risikobehandlungsplan pflegen
`security.audit.manage`	Grundschutz-Check, ISMS-Ziele, Audits, Nichtkonformitäten, Dokumente
`security.risk.accept`	Restrisiko akzeptieren, Managementbewertung freigeben
`security.report.generate`	Berichte (SoA, RTP, Audit, Review) erzeugen
`security.catalog.manage`	Kataloge und Frameworks verwalten

13 Das dokumentierte ISMS – Anlage mit Vorlagen

Ein zertifizierungsfähiges ISMS braucht neben dem Modul auch eine Reihe **freigegebener Dokumente** (Leitlinie, Scope, Risikoverfahren, Erklärung zur Anwendbarkeit, Auditberichte …). Welche Dokumente die ISO/IEC 27001:2022 verlangt und wie sie aussehen, beschreibt die eigenständige **Anlage *ID-28a ISMS-Dokumentation*** – mit ausformulierten Vorlagen für jedes Pflichtdokument im Ordivis-Corporate-Design.

Verwandte Themen

- **ID-28a – Anlage: ISMS-Dokumentation nach ISO/IEC 27001** – die ausformulierte ISMS-Dokumentation
- **ID-29 – Modul Business Continuity Management** – Fortführung des Geschäftsbetriebs
- **ID-30 – Modul Notfall- & Wiederanlaufplanung (DR)** – technischer Wiederanlauf nach einem Ausfall
- **ID-32 – Modul Datenschutz (Art. 30 DSGVO)** – Schnittmenge mit dem Datenschutz
- **ID-21 – Modul CMDB** – Schutzbedarf an den Configuration Items