WolfISMS

Wolf's Informations-Sicherheits-Management-System

Benutzerdokumentation

Version 4.01

Stand: November 2026

© 2012–2026 WolfInfoSec GmbH

Inhaltsverzeichnis

1. Einleitung 7
1.1 Systemvoraussetzungen 7
1.2 Anmeldung 7
1.3 Navigation im Menü 8
1.4 Detailansichten und Seitenleiste 9
1.5 Erklärtexte (Tooltips) 9
1.6 Die Oberfläche seit v4.00 10
2. Modulübersicht 11
3. Benutzerrollen und Berechtigungen 13
3.1 Berechtigungsübersicht 13
3.2 Hinweise zu Berechtigungen 14
3.3 Mehrere Besitzer 14
4. Home / Dashboard 15
Beschreibung 15
Funktionen 15
Hinweise 15
5. Controls 17
Beschreibung 17
Funktionen 17
6. Rechtsregister 19
Beschreibung 19
Funktionen 19
7. Datenschutz 21
Beschreibung 21
Verzeichnis von Verarbeitungstätigkeiten 21
Schwellwertanalyse 21
Datenschutz-Folgenabschätzung 21
Funktionen 22
Hinweise 22
8. Risiken 23
Beschreibung 23
Funktionen 23
KI-Assistent für Risiken 25

© 2012–2026 WolfInfoSec GmbH

9. Assets....26
Beschreibung....26
Funktionen....26
KI-Assistent für Assets....27
10. Zugriffsmatrix....29
Beschreibung....29
Berechtigungsstufen....29
Zugriffsverfahren....29
Funktionen....30
Hinweise....31
11. Changemanagement....32
Beschreibung....32
Ablauf eines Changes....32
Funktionen....32
12. Maßnahmen....34
Beschreibung....34
Funktionen....34
13. Projekte....36
Beschreibung....36
Funktionen....36
14. Incidents (Vorfälle)....37
Beschreibung....37
Funktionen....37
Meldepflichten und Meldefristen....38
15. Schwachstellen....40
Beschreibung....40
Funktionen....40
16. Audit....42
Beschreibung....42
Aufbau....42
Prüfliste und Gap-Assessment....43
Funktionen....44
Hinweise....45
17. Managementbewertung....46
Beschreibung....46

© 2012–2026 WolfInfoSec GmbH

Aufbau einer Bewertung 46
Funktionen 46
Hinweise 47
18. Aufgaben 48
Beschreibung 48
Funktionen 48
Hinweise 49
Abwesenheit und Vertretung 49
19. Operational Plan (Wiederkehrende Aufgaben) 50
Beschreibung 50
Funktionen 50
20. Dokumente 52
Beschreibung 52
Versionen und Versionsverlauf 52
Aus Word übernehmen 53
Funktionen 53
21. BPMN-Prozessmodellierung 56
Beschreibung 56
Funktionen 56
22. Playbooks 57
Beschreibung 57
Funktionen 57
23. Lieferanten 59
Beschreibung 59
Funktionen 59
Sicherheitsfragebogen 60
24. Personal 62
Beschreibung 62
Funktionen 62
Hinweise 63
On-/Offboarding 63
Schulungen 64
25. Policy Portal 65
Beschreibung 65
Funktionen 65

© 2012–2026 WolfInfoSec GmbH

26. Kontakte....67
Beschreibung....67
Funktionen....67
27. BCM – Business Continuity Management....69
Beschreibung....69
Funktionen....69
28. REST-API und API-Key-Verwaltung....71
Beschreibung....71
API-Key-Verwaltung (/admin/api_keys)....71
Bereiche und Endpunkte....71
29. Ziele....73
Beschreibung....73
Funktionen....73
30. Externe Links....75
Beschreibung....75
Funktionen....75
31. Berichte....76
Beschreibung....76
Übersicht der Berichte....76
Funktionen....76
Hinweise....77
32. Administration....78
Beschreibung....78
Benutzer und Organisation....78
Kataloge und Stammdaten....79
System und Betrieb....79
33. Häufige Fragen (FAQ)....82
Ich sehe ein Modul nicht – was ist zu tun?....82
Ich kann plötzlich nichts mehr speichern – woran liegt das?....82
Kann ein Eintrag mehrere Besitzer haben?....82
Warum kann ich keinen weiteren Eintrag mehr anlegen?....82
Wie ändere ich mein Passwort?....82
Was bedeutet „Read Only“?....83
Wie exportiere ich Daten nach Excel?....83
Wie funktioniert der Dokumenten-Workflow?....83

© 2012–2026 WolfInfoSec GmbH

Wie komme ich an eine frühere Fassung eines Dokuments?....83
Wie übernehme ich ein Word-Dokument?....83
Was ist eine Lesebestätigung und wo bestätige ich sie?....83
Wozu dient die Zugriffsmatrix und wie oft muss ich sie prüfen?....83
Warum ist meine Zugriffsmatrix leer?....84
Kann ich BPMN-Diagramme aus anderen Tools importieren?....84
Wie werden Lieferantenrisiken berechnet?....84
Wie richte ich die Zwei-Faktor-Authentifizierung (2FA) ein?....84
Wie arbeite ich mit dem KI-Assistenten für Dokumente?....84
Warum kann ich einen Anhang nicht hochladen?....84
Welche KI-Assistenten gibt es?....84
Welche Daten verlassen dabei das System?....85
Was macht die KI bei Assets und Gap-Assessments?....85
Warum sehen die Farben der Oberfläche anders aus als früher?....85
Wer bekommt meine Aufgaben, wenn ich abwesend bin?....85
Wo trage ich RTO, RPO und MAZ ein?....85
Wo finde ich die Berichte für das Audit?....85
Warum passiert nichts, wenn ich eine Aktion im neuen Tab öffne?....85
Warum zeigt die Seitenleiste nur fünf Einträge?....85
Warum steht eine Verknüpfung auch beim anderen Eintrag?....86
Wie lasse ich ein Dokument ins Englische übersetzen?....86
Wo sind die Schaltflächen zum Verknüpfen geblieben?....86
Warum hat nicht jedes Feld ein ⓘ?....86
Mein Konto ist gesperrt – was nun?....86
Wie schalte ich den Dunkelmodus ein?....86
Wo sind die Kacheln über den Listen geblieben?....86
Warum kann ich in den Listen nicht mehr blättern?....86
Wie schreibe ich ein Playbook?....87
Warum sehe ich das Modul Datenschutz nicht?....87
Wer pflegt den AVV eines Lieferanten?....87
34. Glossar....88

© 2012–2026 WolfInfoSec GmbH

1. Einleitung

WolfISMS ist ein webbasiertes Informations-Sicherheits-Management-System (ISMS), das speziell für die Anforderungen von KMU im regulierten Umfeld entwickelt wurde. Es unterstützt die Umsetzung von ISO/IEC 27001:2022, NIS-2, DSGVO sowie branchenspezifischer Anforderungen (Luftfahrt, CRA).

Das System ist modular aufgebaut: Jedes Modul deckt einen spezifischen ISMS-Bereich ab und ist über das seitliche Navigationsmenü erreichbar, in dem die Module nach Themen gruppiert sind (siehe „Navigation im Menü“). Alle Bereiche sind rollenbasiert geschützt – Benutzer sehen und bearbeiten nur das, wofür sie berechtigt sind.

1.1 Systemvoraussetzungen

WolfISMS läuft vollständig im Webbrowser. Es ist keine lokale Installation erforderlich.

Voraussetzung	Anforderung
Browser	Chrome 90+, Firefox 88+, Edge 90+, Safari 14+
Verbindung	Internes Netzwerk oder VPN (HTTPS)
Anmeldung	Benutzername (E-Mail) + Passwort, optional Microsoft- oder Google-SSO
Bildschirm	Empfohlen: mindestens 1280 × 800 Pixel

1.2 Anmeldung

Rufen Sie die System-URL in Ihrem Browser auf und geben Sie E-Mail-Adresse und Passwort ein. Nach erfolgreicher Anmeldung gelangen Sie automatisch zum Dashboard (Home). Bei Fragen zur Anmeldung wenden Sie sich an Ihren Systemadministrator.



Passwort ändern: Klicken Sie oben rechts auf Ihren Namen → „Passwort ändern“. Das neue Passwort muss die Mindestanforderungen erfüllen (mindestens 10 Zeichen, Groß- und Kleinbuchstaben, Zahl).

Passwort vergessen: Auf der Anmeldeseite steht ein Link „Passwort vergessen". Sie geben Ihre E-Mail-Adresse ein und erhalten eine Nachricht mit einem Link, über den Sie selbst ein neues Passwort setzen – er gilt zwei Stunden. Die Seite bestätigt den Versand immer gleich, unabhängig

© 2012–2026 WolfInfoSec GmbH

davon, ob die Adresse bekannt ist; das ist Absicht, damit sich hier keine Konten aufspüren lassen. Melden Sie sich über Microsoft oder Google an, verwaltet Ihr Unternehmen das Passwort – dann hilft dieser Weg nicht weiter.

Single Sign-On: Hat Ihr Unternehmen die Anmeldung über Microsoft oder Google freigeschaltet, erscheint auf der Loginseite eine zusätzliche Schaltfläche. Sie melden sich dann mit Ihrem Firmenkonto an; ein eigenes WolfISMS-Passwort ist in diesem Fall nicht erforderlich. Zugelassen sind nur die von Ihrem Administrator freigegebenen E-Mail-Domains.

Direkte Anmeldung über Microsoft: Ist die Microsoft-Anmeldung eingerichtet, leitet WolfISMS Sie beim Aufruf der Seite gleich dorthin weiter – Sie sehen das Passwortformular gar nicht mehr. Brauchen Sie es doch einmal, etwa weil Microsoft nicht erreichbar ist oder Ihr Konto noch kein Single Sign-On nutzt, klicken Sie auf der Anmeldeseite auf „Anmeldung mit E-Mail und Passwort (Notfallzugang)“. Nach dem Abmelden und nach einer fehlgeschlagenen Anmeldung bleibt die Seite stehen, damit Sie den Hinweis lesen und das Konto wechseln können.

Zwei-Faktor-Authentifizierung (2FA): Wenn vom Administrator aktiviert, werden Sie nach dem Passwort-Login aufgefordert, einen TOTP-Code einzugeben. Beim ersten Mal scannen Sie den angezeigten QR-Code mit einer Authenticator-App (z. B. Google Authenticator oder Microsoft Authenticator). Über Ihren Benutzer-Bereich (oben rechts → Ihr Name) können Sie 2FA jederzeit einrichten oder deaktivieren.

Gesperrte Konten:
Ein Benutzerkonto kann vom Administrator deaktiviert werden, ohne es zu löschen. Eine Anmeldung ist dann weder mit Passwort noch über SSO möglich. Wenden Sie sich in diesem Fall an Ihren Administrator.

1.3 Navigation im Menü

Seit v3.91 ordnet die Seitenleiste die Module in Gruppen, die dem Ablauf eines ISMS folgen: von den Vorgaben über den Bestand und die Risiken bis zum laufenden Betrieb und zur Überprüfung. Ganz oben stehen die beiden Einträge, die fast jeder braucht.

Gruppe	Module
Mein Arbeitsbereich	Policy Portal, Aufgaben
Governance & Compliance	Controls, SoA, Rechtsregister, Datenschutz, Dokumente, Ziele
Organisation & Inventar	Assets, Zugriffsmatrix, Lieferanten, Personal, Prozesslandkarte, Netzwerkzonen
Risiko & Maßnahmen	Risiken, Maßnahmen, Schwachstellen
Betrieb & Resilienz	Changemanagement, Kontakte, Incidents, Playbooks, BCM
Planung & Überprüfung	Projekte, Operational Plan, Audit, Managementbewertung, Berichte
(ohne Überschrift)	Links – abgesetzt durch eine Linie

- **Auf- und zuklappen**: Ein Klick auf die Überschrift einer Gruppe klappt sie zu oder wieder auf. Ihr Browser merkt sich, welche Gruppen Sie zugeklappt haben – auf einem anderen Gerät oder in einem anderen Browser ist das Menü wieder ganz geöffnet
- **Aktuelle Seite**: Der Menüpunkt der Seite, auf der Sie sich befinden, ist hervorgehoben. Seine Gruppe ist immer offen, auch wenn Sie sie vorher zugeklappt hatten

© 2012–2026 WolfInfoSec GmbH

- **Nur, was Sie nutzen können**: Sie sehen nur Module, für die Sie ein Recht haben und die Ihre Lizenz enthält. Eine Gruppe ohne solches Modul fehlt samt Überschrift; wer nur das Policy Portal nutzt, sieht gar keine Überschriften
- **Reihenfolge**: Die Gruppen stehen fest. Innerhalb einer Gruppe legt Ihr Administrator die Reihenfolge der Einträge fest
- **Symbole**: Seit v4.00 steht vor jedem Modul eine kleine farbige Kachel mit Symbol; die Farbe zeigt die Gruppe. Die Seite, auf der Sie sich befinden, ist farbig hinterlegt
- **Kompakte Darstellung**: Der Listen-Knopf oben in der Seitenleiste, links neben «, rückt die Einträge enger zusammen und verkleinert die Symbole – praktisch auf kleinen Bildschirmen. Ist sie eingeschaltet, ist der Knopf blau. Ihr Browser merkt sich die Wahl, ebenso wie das Einklappen der Leiste mit «

1.4 Detailansichten und Seitenleiste

Öffnen Sie einen einzelnen Eintrag – ein Risiko, ein Asset, ein Dokument –, steht links der Inhalt und rechts eine Seitenleiste. Seit v3.94 ist sie in allen Modulen gleich aufgebaut.

- **Oben:** Eigenschaften wie Status, Besitzer und Abteilung sowie die Metadaten – wer den Eintrag angelegt und zuletzt geändert hat, wann, und gegebenenfalls Reviewer und Review-Datum
- **Darunter:** die Verknüpfungen, je Bereich mit Anzahl und, wenn Sie sie ändern dürfen, dem Link „Verwalten“. Eine Linie schließt jeden Abschnitt unter seinem letzten Eintrag ab
- **Höchstens fünf Einträge:** hat ein Abschnitt mehr, folgt „mehr … (+N)“ und führt auf dieselbe Seite wie „Verwalten“. Wer nicht verwalten darf, sieht die vollständige Liste
- **Beide Richtungen:** eine Verknüpfung steht auch beim anderen Eintrag. Ein Change, der ein Asset nennt, erscheint also auch am Asset. Solche Abschnitte haben keinen „Verwalten“-Link – geändert wird die Verknüpfung dort, wo sie angelegt wurde – und erscheinen nur, wenn es Einträge gibt und Sie das andere Modul lesen dürfen
- **Aktionsleiste:** Seit v3.95 enthält die Leiste über dem Inhalt nur noch Aktionen wie Bearbeiten, Review, Export und die KI-Assistenten. Die Schaltflächen zum Verknüpfen – etwa Controls, Prozesse und Dokumente am Dokument, Risiken, Incidents und Controls am Asset oder Maßnahmen, Assets und Lieferanten am Risiko – sind entfallen; verknüpft wird über „Verwalten“ im jeweiligen Abschnitt der Seitenleiste. Was schon in der Überschrift steht, wiederholt die Tabelle darunter nicht mehr, Besitzer, Verantwortliche und Abteilung stehen bei den Metadaten. Bei Maßnahmen steht die Priorität im Kopf neben dem Status

Detailansicht	Zusätzlich angezeigt seit v3.94
Assets	Elternassets, Changes, Lieferanten, Schwachstellen
Risiken	Changes, Schwachstellen
Incidents	Changes, Schwachstellen
Maßnahmen	Projekte, Schwachstellen, BCM-Übungen
Dokumente	Risiken, Changes und Dokumente, die auf dieses verweisen
BPMN-Prozesse	Liste „Verknüpfte Dokumente“ unter dem Diagramm

1.5 Erklärtexte (Tooltips)

Seit v3.97 steht neben vielen Formularfeldern und Spaltenüberschriften ein kleines ⓘ. Es erklärt kurz, was ein Feld bedeutet oder bewirkt – zum Beispiel den Unterschied zwischen

© 2012–2026 WolfInfoSec GmbH

Wahrscheinlichkeit vor und nach Maßnahme, was RTO, RPO und MAZ meinen oder welche Meldefristen ein Häkchen bei DSGVO oder NIS-2 auslöst. Auch die Buttons – etwa Review, Vererbung O→I, die KI-Assistenten oder die Symbolknöpfe – zeigen ihren Erklärtext ohne ⓘ direkt am Button. Auch die Einträge der linken Seitenleiste erklären kurz, wofür das Modul da ist; in der eingeklappten Leiste steht der Modulname davor.

- **Maus:** Zeiger auf das ⓘ bzw. kurz auf den Button halten.
- **Tastatur:** mit der Tabulatortaste auf das ⓘ springen; Esc schließt den Text.
- **Tablet und Smartphone:** das ⓘ antippen, einen Button lange drücken – er wird dabei nicht ausgelöst; ein Tipp daneben schließt den Text.

Ein Klick auf das ⓘ ändert nichts am Formular und sortiert auch keine Tabelle. Die Texte erscheinen in der eingestellten Sprache. Die Administration kann die Tooltips für alle abschalten.

1.6 Die Oberfläche seit v4.00

Mit v4.00 hat WolfISMS ein neues, ruhigeres Erscheinungsbild bekommen. Die Funktionen sind dieselben geblieben; anders aussehen vor allem die Listen der Module, die Knöpfe und die Seitenleiste.

- **Listen:** Jeder Eintrag ist eine Zeile – links ein farbiger Punkt für Status oder Stufe, daneben Nummer und Name, darunter die wichtigsten Angaben, rechts Besitzer und gegebenenfalls eine farbige Markierung. Ein Klick auf die Zeile öffnet die Detailansicht. Lange Namen werden nicht mehr abgeschnitten, sondern umbrechen
- **Suchen:** Das Suchfeld über der Liste filtert schon beim Tippen. Mehrere Wörter grenzen ein – jedes muss im Eintrag vorkommen. Das Kreuz im Feld leert die Suche. Geblättert wird nicht mehr: die Liste zeigt alle Einträge
- **Filtern:** Kacheln mit Zahlen über der Liste – etwa je Risikostufe oder Phase – filtern mit einem Klick, ein zweiter Klick hebt den Filter auf. Pillen wie „Status“ oder „Kategorie“ öffnen ein Auswahlmenü. Jeder gesetzte Filter erscheint als Chip mit ×; ein Klick darauf entfernt ihn, „Alle entfernen“ setzt alle zurück
- **Umschalten:** Wo ein Modul mehrere Arten von Einträgen führt – etwa BIA, Notfallpläne und Übungen im BCM oder die Kontaktarten –, wechseln Sie über die Segmente über der Liste
- **Sortieren:** rechts in der Filterzeile; ein zweiter Klick auf dieselbe Sortierung kehrt die Richtung um
- **Knöpfe:** Der wichtigste Knopf einer Seite – etwa „Neu“ oder „Speichern“ – ist blau gefüllt, die übrigen sind schlicht grau, Löschen ist rot. Seltener gebrauchte Aktionen wie Export oder Import stecken im Drei-Punkte-Menü neben dem Hauptknopf
- **Überschrift:** Haupt- und Detailansichten zeigen ihren Titel in einer weißen Kachel
- **Infokacheln:** Statistik- und Kategoriekacheln über den Listen sind zunächst ausgeblendet; Ihr Administrator kann sie unter Design & Farben für alle einschalten
- **Hell und dunkel:** Der Knopf mit Mond bzw. Sonne oben rechts neben der Sprachflagge schaltet zwischen hellem und dunklem Modus um. Die Wahl gilt für Ihr Konto auf jedem Gerät; ohne eigene Wahl gilt die Vorgabe Ihres Administrators. Risikomatrix, Ampelkacheln und Tachos behalten auch im Dunkelmodus ihre Farben
- **Version:** Rechts in der Fußzeile steht, welche WolfISMS-Version läuft – hilfreich bei Fragen an den Support

© 2012–2026 WolfInfoSec GmbH

2. Modulübersicht

Das System besteht aus folgenden Modulen. Welche Bereiche Ihnen offenstehen, hängt von den zugewiesenen Benutzerrechten ab und davon, welche Module Ihr Administrator unter Administration → Module eingeschaltet hat; dort wird auch ihre Reihenfolge innerhalb der Menügruppen festgelegt. Einige Bereiche hängen zusätzlich an der Edition Ihrer Lizenz: Ziele, Personal, Kontakte, Berichte, Projekte, Operational Plan, Audit, Managementbewertung, Schwachstellen, Rechtsregister, Playbooks, BCM und die Zugriffsmatrix gehören zur Edition Advanced und zu Enterprise, Single Sign-On und REST-API zum Zusatzpaket „+“. Die KI-Funktionen gibt es in jeder bezahlten Edition, also schon in Essentials. Welche Edition Ihre Installation nutzt, sagt Ihnen Ihr Administrator.

Modul	URL / Berechtigung	Hauptfunktionen
Home / Dashboard	/home · alle angemeldeten Nutzer	Risikomatrix, Lieferantenrisiko, offene Incidents, Framework-Erfüllung, Meine Aufgaben
Controls	/normen · norm	ISO 27001, NIS-2, BSI-Grundschutz: Kapitelübersicht, Umsetzungsstatus, Verlinkung
SoA	/berichte?berdetail=2 · norm	Erklärung zur Anwendbarkeit nach ISO/IEC 27001 Anhang A; nur sichtbar, wenn ISO/IEC 27001 installiert ist
Berichte	/berichtsuebersicht · alle (Karten je nach Recht)	Alle Berichte und Exporte an einer Stelle, gegliedert nach ISO/IEC 27001
Rechtsregister	/rechtsregister · norm	Gesetzliche Anforderungen, Compliance-Status, Themenbereichsfilter, Excel-Export
Datenschutz	/datenschutz · datenschutz	Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO), Schwellwertanalyse, Datenschutz-Folgenabschätzung, AVV-Angaben der Lieferanten
Risiken	/risiko · risk	Risikoregister, 5×5-Matrix, Behandlungsoptionen, Verknüpfung Assets/Maßnahmen
Assets	/assets · assets	IT- und Informationsassets, CIA-Bewertung, Kritikalität, Klassifizierung, Hierarchie
Zugriffsmatrix	/zugriffsmatrix · assets	Soll-Berechtigungen je Asset und Rolle, Genehmigung, Rezertifizierung, Rollenkatalog
Changemanagement	/change · assets	Änderungsanträge mit Umsetzungs-, Test- und Rückfallplan, Freigabegremium, Nachbetrachtung, Änderungskalender
Maßnahmen	/massnahmen · mass	Maßnahmenverfolgung, Status, Fortschrittsbalken, Verknüpfung Risiken/Controls/Assets
Projekte	/projekte · mass	ISMS-Rahmen nach ISO/IEC 27001 A.5.8: Steckbrief, Abschnitte, Rollen, Sicherheits-Gates, Ampel, Fortschritt aus Maßnahmen
Incidents	/incidents · incidents	Vorfallmanagement, Meldepflicht DSGVO/NIS-2/CRA mit Fristen und Meldevorlagen, Ursachenanalyse, Eskalation
Schwachstellen	/schwachstellen · schwachstellen	Schwachstellenregister mit CVSS-Score und Schweregrad, Quellen, Verknüpfung zu Assets, Incidents, Risiken und Maßnahmen
Audit	/audit · audit	Auditplanung (intern/extern), Abweichungen mit Typ, Frist und Verantwortlichem, Maßnahmen, Anhänge und Links

© 2012–2026 WolfInfoSec GmbH

Modul	URL / Berechtigung	Hauptfunktionen
Managementbewertung	/managementreview · audit	Leitungsbewertung nach ISO 27001 Kap. 9.3 mit Live-KPIs und Risikolage, PDF- und PowerPoint-Export
Aufgaben	/aufgaben · alle	Meine offenen Aufgaben aus allen Modulen, Zeitraumfilter, Überfälligkeiten
Operational Plan	/op_plan · master (Menü) / alle (eigene Aufgaben)	Wiederkehrende Aufgaben (Fristenkalender) mit automatischer Nachweiskette
Dokumente	/dokumente · dok	Dokumentenverwaltung, Workflow Prüfen/Freigeben, Versionierung, BPMN, KI-Assistent
BPMN	/bpmn · dok	Prozessmodellierung, Editor, Import/Export von .bpmn-Dateien
Playbooks	/playbooks · play	Playbooks nach ISO/IEC 27035: Steckbrief, Abschnitte, Ablaufschritte, Rollen, Übungen, Ampel, Dateien und Links
Lieferanten	/vendor · vendor	Lieferantenregister, automatisches Risikoscoring, Tier-Klassifizierung, Score-Historie
Personal	/personal · pers	Personalverzeichnis, Schulungsdokument-Lesestatus, Abteilungsübersicht, On-/Offboarding
Policy Portal	/portal · alle angemeldeten Nutzer	Mitarbeiterportal für Richtlinien mit Lesebestätigung
Kontakte	/kontakte · kontakte	Adressbuch: Mitarbeiter, Dienstleister, Behörden, Interessensgruppen
Prozesslandkarte	/prozesslandkarte · prozesslandkarte	Prozesse als Karte: Führungs-, Kern- und Unterstützungsprozesse mit Verantwortlichen und Prozessdokument
Netzwerkzonen	/netzwerkzonen · netzwerkzonen	Netzsegmentierung als Karte: Zonen nach Vertrauensstufe, VLAN, Adressbereich, Schutzbedarf
BCM	/bcm · bcm	Business Impact Analyse je Asset, Notfallpläne, BCM-Übungen
Ziele	/ziele · ziele	Unternehmensziele, Informationssicherheitsziele, KPI-Tracking mit Zielwert und Verlauf
Externe Links	/custom · custom	Zentrale Sammlung von Links zu externen Systemen (Ticketsystem, KPI-System, SharePoint)
Administration	/admin · admin	Benutzerverwaltung, Berechtigungen, Aktivitätsprotokoll, Stammdaten, Abteilungen
REST-API	/api/v1 · admin	Datensätze aus sechs Bereichen per API anlegen und abfragen, API-Key-Verwaltung (/admin/api_keys)

© 2012–2026 WolfInfoSec GmbH

3. Benutzerrollen und Berechtigungen

Jeder Benutzer erhält eine individuelle Kombination aus Berechtigungen. Die Vergabe erfolgt durch den Administrator unter /admin/change_user.

3.1 Berechtigungsübersicht

Recht	Kürzel	Beschreibung
Administrator	admin	Vollzugriff auf alle Bereiche inkl. Benutzerverwaltung, Stammdaten, Aktivitätsprotokoll
Read Only	readonly	Lesezugriff über das Policy Portal, keine Bearbeitungsmöglichkeit
Master	master	Erweiterte Rechte: Aufgaben aller Benutzer sehen, Freigabe-Workflows, Portal-Reset, Rollen anlegen und löschen
KI-Nutzung	ki	KI-Assistenten nutzen (Ja/Nein); Administratoren dürfen immer
Assets	assets	Assets anlegen, bearbeiten, exportieren – schließt Zugriffsmatrix und Changemanagement ein
Dokumente	dok	Dokumente und BPMN bearbeiten, Workflow-Teilnahme (Prüfen/Freigeben)
Maßnahmen & Projekte	mass	Maßnahmen und Projekte anlegen und bearbeiten; Playbook-Links verwalten
Risiken	risk	Risiken anlegen, bearbeiten, verknüpfen
Lieferanten	vendor	Lieferanten anlegen, bearbeiten, exportieren
Audit	audit	Audit-Fragen bewerten und exportieren – schließt die Managementbewertung ein
Controls & Rechtsreg.	norm	Controls und Rechtsregister bearbeiten, verknüpfen, exportieren
Datenschutz	datenschutz	Verarbeitungsverzeichnis und DSFA lesen (1) und bearbeiten (2); pflegt auch die AVV-Angaben der Lieferanten
Personal	pers	Personalverzeichnis und Lesestatus einsehen
Playbooks	play	Playbooks schreiben, Playbook-Dateien hochladen und löschen
Incidents	incidents	Incidents anlegen, bearbeiten, verknüpfen, exportieren
Schwachstellen	schwachstellen	Schwachstellen lesen (1) und anlegen, bearbeiten, löschen (2)
Kontakte	kontakte	Kontaktdaten lesen (1) und anlegen/bearbeiten/löschen (2)
Prozesslandkarte	prozesslandkarte	Prozesslandkarte lesen (1) und bearbeiten (2)
Netzwerkzonen	netzwerkzonen	Netzwerkzonen lesen (1) und bearbeiten (2)
BCM	bcm	BIA, Notfallpläne und BCM-Übungen lesen (1) und bearbeiten (2)

© 2012–2026 WolfInfoSec GmbH

Recht	Kürzel	Beschreibung
Ziele	ziele	Unternehmensziele, Sicherheitsziele und KPIs lesen (1) und bearbeiten (2)
Externe Links	custom	Zugriff auf das Modul Externe Links

3.2 Hinweise zu Berechtigungen

- Die meisten Rechte kennen drei Stufen: 0 = kein Zugriff, 1 = Lesen, 2 = Bearbeiten.
- Benutzer ohne spezifische Rechte können Home, Aufgaben und Policy Portal nutzen.
- readonly überschreibt alle anderen Bearbeitungsrechte – der Benutzer kann nichts ändern.
- master wird für Review-Freigaben, die Gesamtaufgaben-Ansicht, die Pflege von Rollen und die Lesepflicht-Matrix des Policy Portals benötigt.
- admin allein reicht für alle Bereiche – weitere Rechte sind dann nicht nötig.
- **Rechte und Rollen sind zweierlei**: Die Rechte oben entscheiden, was Sie sehen und ändern dürfen. Eine Rolle – Informationssicherheitsbeauftragter, Datenschutzbeauftragter, IT-Leitung – beschreibt dagegen Ihre Funktion. Sie steuert die Spalten der Zugriffsmatrix und die Lesepflicht im Policy Portal, verleiht aber selbst keine Berechtigung
- Drei Module haben kein eigenes Recht: die Zugriffsmatrix und das Changemanagement nutzen das Recht assets, die Managementbewertung das Recht audit.
- ki ist ein Ja/Nein-Recht und standardmäßig aus: Ohne es fehlen alle KI-Knöpfe, auch wenn Sie das Modul bearbeiten dürfen. Administratoren brauchen es nicht.

Wenn die Lizenz abgelaufen ist:
Alle Module bleiben sichtbar und lesbar, aber Speichern und Bearbeiten sind gesperrt – das System verhält sich dann wie ein Nur-Lese-Zugang. Administratoren und Master-Benutzer behalten ihren Schreibzugriff, damit eine neue Lizenz eingespielt werden kann.

3.3 Mehrere Besitzer

Risiken, Assets, Dokumente, Maßnahmen, Projekte, Controls, Lieferanten, Incidents, Schwachstellen und Changes können mehrere Besitzer (in Maßnahmen und Projekten: Verantwortliche) haben. Im Formular wählen Sie sie aus einer Liste mit Kästchen; das Suchfeld darüber filtert nach Namen, die bereits gewählten Personen stehen oben, und die Fußzeile zählt die Auswahl.

- **Gleiche Rechte:** Jeder Besitzer darf den Eintrag ändern und löschen – wie bisher der eine Besitzer. Masteruser dürfen immer.
- **Hauptbesitzer:** Der zuerst eingetragene Besitzer bleibt es, solange er ausgewählt ist. Er erscheint in Sortierung und Exporten an erster Stelle; in Listen und Detailansicht stehen alle Besitzer, durch Semikolon getrennt.
- **Keine Auswahl:** Wählen Sie niemanden aus, werden Sie selbst Besitzer.
- **Aufgaben:** Fällige Maßnahmen und Change-Termine erscheinen unter „Meine Aufgaben“ und in der Erinnerungsmail bei jedem Besitzer.

© 2012–2026 WolfInfoSec GmbH

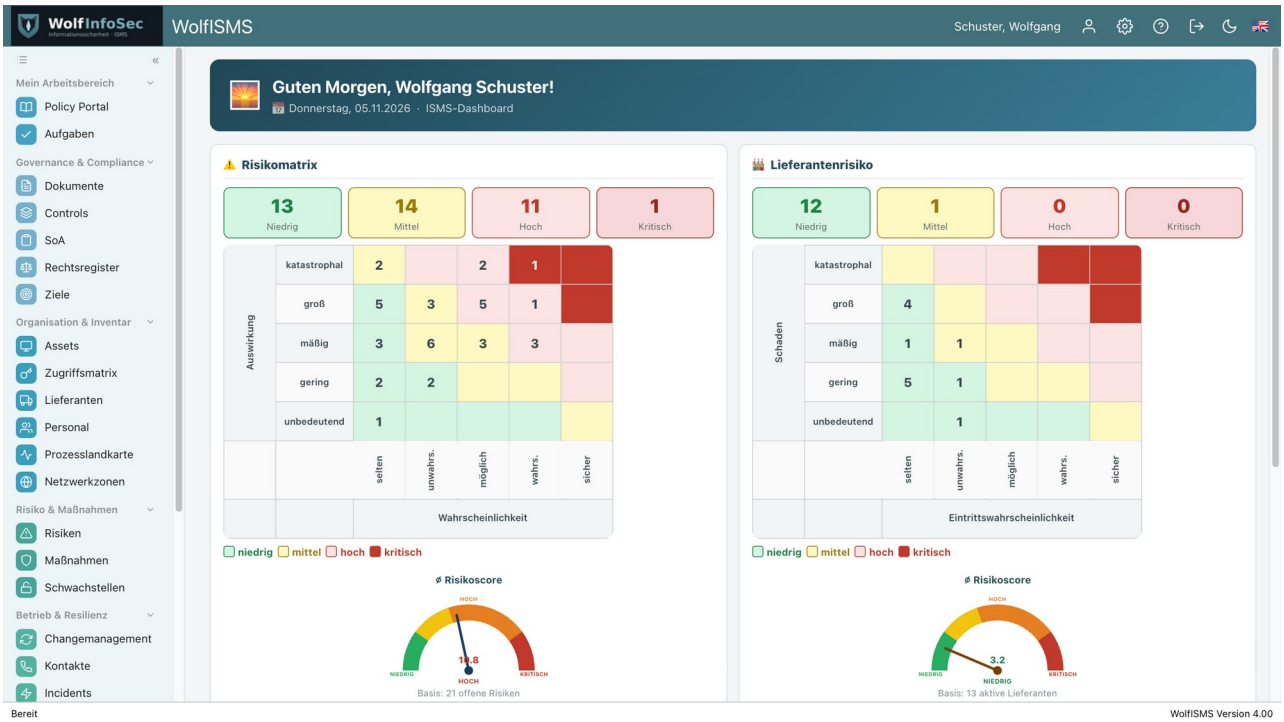
4. Home / Dashboard

Beschreibung

Das Dashboard ist die Startseite nach der Anmeldung und bietet einen kompakten Überblick über den aktuellen ISMS-Zustand. Es zeigt Risikomatrizen, offene Vorfälle, den Framework-Erfüllungsgrad und die eigenen offenen Aufgaben.

Funktionen

- **Begrüßungsbanner**: Personalisierte Tageszeit-Begrüßung mit aktuellem Datum
- **Risikomatrix (ISMS)**: 5×5-Matrix der erfassten Risiken – farbcodiert (grün/gelb/rot/dunkelrot). Ein Klick auf eine Zelle öffnet die gefilterte Risikoliste
- **Risikomatrix (Lieferanten)**: Separate 5×5-Matrix des automatisch berechneten Lieferantenrisikos. Ein Klick öffnet die gefilterte Lieferantenliste
- **Legende**: Farbschlüssel für die Risikostufen: Niedrig / Mittel / Hoch / Kritisch
- **Offene Incidents**: Liste der bis zu 15 aktuell offenen Vorfälle mit Prioritätsfarbmarkierung (kritisch = rot)
- **Framework-Erfüllung**: Fortschrittsbalken je Framework (ISO 27001, NIS-2 etc.) mit Ampelfarbe (≥ 80 % grün, ≥ 50 % orange, < 50 % rot)
- **Meine Aufgaben**: Alle offenen Aufgaben der nächsten 7 Tage aus Maßnahmen und Reviews – überfällige Einträge rot hervorgehoben



Hinweise

Das Dashboard ist schreibgeschützt – es dient ausschließlich der Übersicht. Klicks auf Einträge führen zum jeweiligen Modul.

© 2012–2026 WolfInfoSec GmbH

© 2012–2026 WolfInfoSec GmbH

5. Controls

Beschreibung

Das Controls-Modul bildet das Herzstück der Compliance-Dokumentation. Es erfasst alle Anforderungen aus ISO/IEC 27001, NIS-2 und BSI-Grundschutz, zeigt deren Umsetzungsstatus und ermöglicht die Verknüpfung mit Dokumenten und Maßnahmen.

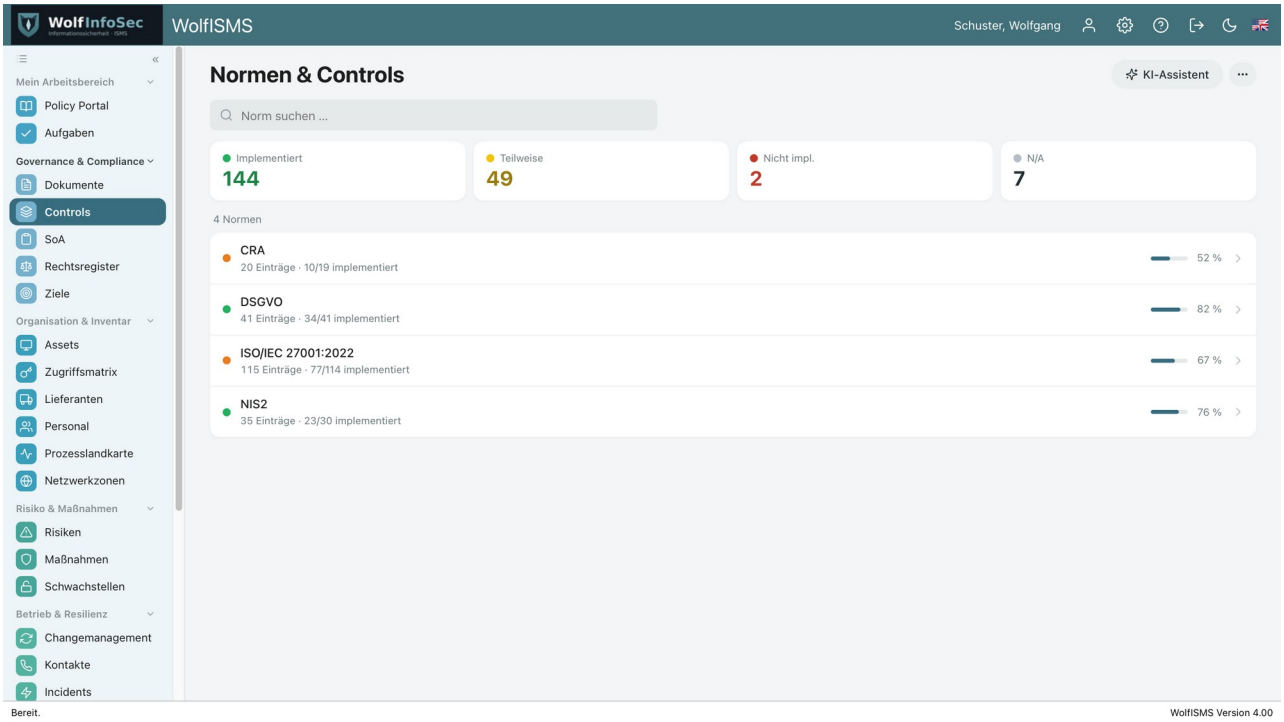
Funktionen

- **Framework-Kacheln**: Übersichtskacheln je Framework mit Statuszusammenfassung
- **Kapitelübersicht**: Tabellarische Darstellung aller Kapitel mit Anzahl der Anforderungen und Umsetzungsgrad
- **Eintragsliste**: Vollständige Liste aller Controls mit Filter nach Framework, Kapitel und Status; die Suche filtert beim Tippen, geblättert wird nicht mehr
- **Detailansicht**: Vollständige Anforderungsdetails mit Beschreibung, Umsetzungshinweisen, Reviewer und Änderungshistorie
- **Umsetzungsstatus**: Je Anforderung lassen sich Anwendbarkeit, Begründung und Umsetzungshinweise pflegen; daraus ergibt sich der Erfüllungsgrad des Frameworks
- **Bearbeiten (norm)**: Formulareditor mit Richtext für Beschreibung und Umsetzungshinweise
- **Löschen:** Einzelne Controls dürfen seit v3.95 nur Administratoren löschen – die Schaltfläche sehen nur sie, in der Kapitelliste wie in der Detailansicht. Bearbeiten bleibt allen mit Schreibrecht auf Controls möglich; ein ganzes Framework zu löschen war schon bisher Administratoren vorbehalten
- **Verknüpfen (norm)**: Verlinkung einzelner Anforderungen mit Dokumenten, Maßnahmen, Risiken und Assets. Risiken und Assets werden dabei auf der Gegenseite eingetragen: die Anforderung erscheint anschließend auch am Risiko bzw. am Asset
- **Seitenleiste:** Seit v3.94 stehen alle Verknüpfungen eines Controls – Dokumente, Maßnahmen, Risiken und Assets – mit Anzahl und „Verwalten“ in der rechten Seitenleiste. Die Tabellen unter der Beschreibung entfallen; Status, Fortschritt oder Score eines verknüpften Eintrags sehen Sie nach einem Klick darauf
- **Statement of Applicability**: seit v3.93 ein eigener Menüpunkt „SoA“ in der Gruppe Governance & Compliance, direkt unter Controls. Er erscheint, sobald eine Fassung von ISO/IEC 27001 installiert ist und Sie Leserecht auf Controls haben. Die Nr. jeder Zeile führt zur Detailansicht des Controls; „SoA als Dokument ablegen“ steht rechts neben der Überschrift (mit dem Recht, Dokumente anzulegen). In Controls selbst gibt es die Schaltfläche nicht mehr
- **Mehrere Fassungen von ISO/IEC 27001:** Sind zwei Fassungen eingespielt, etwa 2022 und 2024, zeigen SoA und Bericht standardmäßig die neueste; ein Umschalter im Kopf der Seite wechselt zur anderen. Auch „SoA als Dokument ablegen“ nimmt die gerade angezeigte Fassung
- **Konformitätsbericht**: Auswertung des Erfüllungsgrads über alle Kapitel eines Frameworks
- **NIS-2-Fragebogen**: Geführte Selbsteinschätzung zur NIS-2-Betroffenheit
- **Excel-Export**: Vollständiger Export aller Controls inkl. Status als Controls.xlsx
- **Charts**: Kreisdiagramme: ISO-27001-Status, NIS-2-Status, Gesamtstatus
- **Kommentare**: Diskussionsfaden je Control; Bearbeiten und Löschen nur durch den Ersteller oder einen Administrator
- **Weitere Links**: In der Detailansicht lassen sich eigene Links zur Anforderung hinterlegen – Intranetseite, Ticket oder das Dokument im DMS. Erlaubt sind gewöhnliche Web-Adressen; ausgefallene Link-Schemata weist WolfISMS ab
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er beantwortet Fragen („Was muss ich zum Thema Patchen alles machen?“), prüft ein Control,

© 2012–2026 WolfInfoSec GmbH

beschreibt die Umsetzung, prüft Nachweise, prüft Ausschlüsse auf Anhaltspunkte, zeigt Lücken, ordnet Controls zwischen Frameworks zu und überträgt den Stand verwandter Controls. Einen Ausschluss schlägt er nie vor. Gespeichert wird erst, was Sie bestätigen.

- **Verwandte Controls:** Controls verschiedener Frameworks, die dasselbe Thema regeln – etwa ISO 27001 A.8.8, BSI OPS.1.1.3 und NIS-2 Art. 21 Abs. 2 e –, lassen sich miteinander verknüpfen. Die Verknüpfung gilt in beide Richtungen und steht in der Detailansicht, in der Verknüpfungsansicht und in der Abdeckung je Framework



6. Rechtsregister

Beschreibung

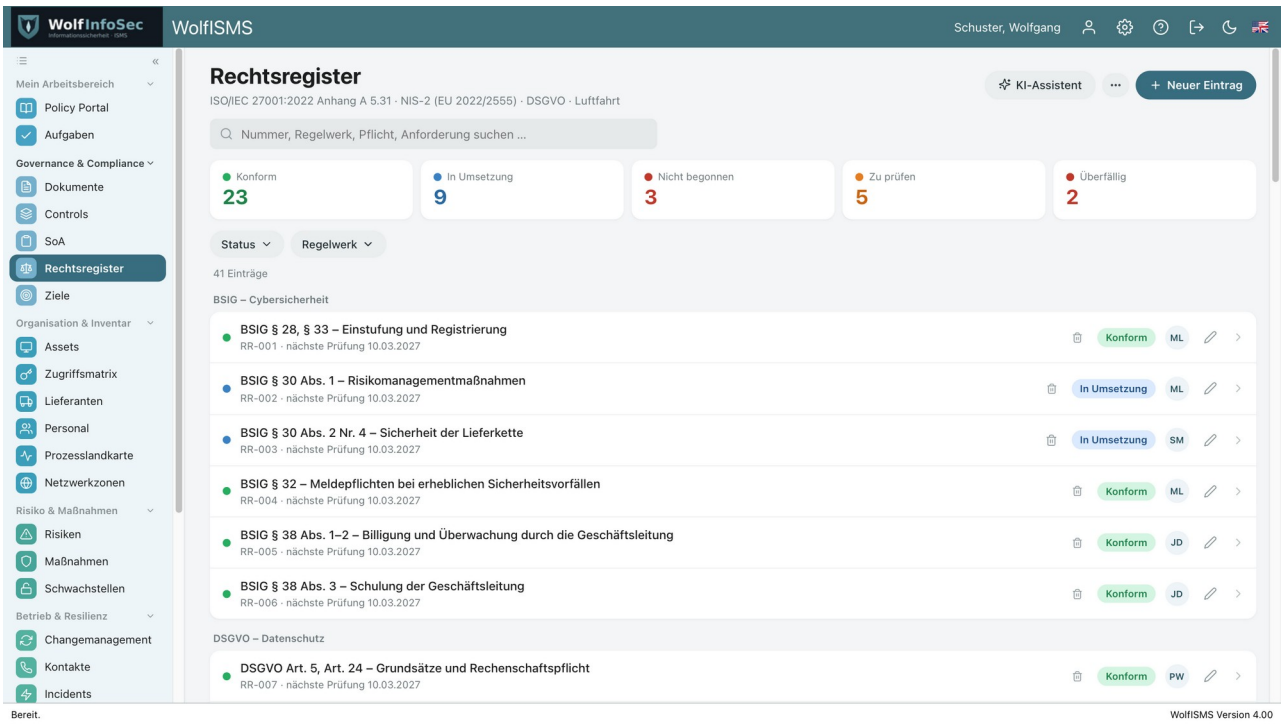
Das Rechtsregister erfasst alle für das Unternehmen relevanten gesetzlichen und regulatorischen Anforderungen (ISO/IEC 27001 A.5.31, NIS-2, DSGVO). Es ist mit 48 Einträgen aus EU- und deutschem Recht vorbelegt.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet.

Funktionen

- **Übersicht**: Gefilterte Liste aller Rechtsgrundlagen mit Suche nach Themenbereich, Kürzel und Status
- **Detailansicht**: Seit v4.00 ein fester Satz von zehn Feldern – Nummer, Rechtsgrundlage (Kürzel, Fundstelle, Titel), Kategorie, Anforderung, Anwendbarkeit, Umsetzung mit verknüpften Maßnahmen, Dokumenten und Controls, Verantwortlich, Status, offene Punkte mit Frist sowie letzte und nächste Prüfung. Ältere Einträge wurden beim ersten Start einmalig in diese Felder übernommen
- **Neu / Bearbeiten (norm)**: Erfassung und Pflege mit Status Zu prüfen, Offen, In Arbeit, Konform oder Nicht geltend
- **Themenbereichs-Kacheln**: Schnellfilter nach Themenbereich (z. B. Datenschutz, Informationssicherheit, Luftfahrt)
- **Status-Chart**: Kreisdiagramm der Compliance-Status-Verteilung
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er beantwortet Fragen, legt Einträge an, findet fehlende Rechtsgrundlagen, prüft Einträge, beschreibt die Umsetzung, prüft Nachweise, geht fällige Prüfungen durch, sucht nach Rechtsänderungen und schreibt einen Lagebericht. Ausdrücklich keine Rechtsberatung: neue Einträge stehen immer auf „Zu prüfen“, und „Nicht geltend“ oder „Konform“ schlägt die KI nie vor. Im Internet sucht sie nur, wenn Ihr Administrator ein Modell mit Websuche eingestellt hat. Gespeichert wird erst, was Sie bestätigen.
- **Excel-Export**: Export aller Einträge als .xlsx

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
Mein Arbeitsbereich
Policy Portal
Aufgaben
Governance & Compliance
Dokumente
Controls
SoA
Rechtsregister
Ziele
Organisation & Inventar
Assets
Zugriffsmatrix
Lieferanten
Personal
Prozesslandkarte
Netzwerkzonen
Risiko & Maßnahmen
Risiken
Maßnahmen
Schwachstellen
Betrieb & Resilienz
Changemanagement
Kontakte
Incidents
Rechtsregister
ISO/IEC 27001:2022 Anhang A 5.31 · NIS-2 (EU 2022/2555) · DSGVO · Luftfahrt
KI-Assistent
Neuer Eintrag
Nummer, Regelwerk, Pflicht, Anforderung suchen ...
Konform
23
In Umsetzung
9
Nicht begonnen
3
Zu prüfen
5
Überfällig
2
Status
Regelwerk
41 Einträge
BSIG – Cybersicherheit
BSIG § 28, § 33 – Einstufung und Registrierung
RR-001 · nächste Prüfung 10.03.2027
Konform
ML
BSIG § 30 Abs. 1 – Risikomanagementmaßnahmen
RR-002 · nächste Prüfung 10.03.2027
In Umsetzung
ML
BSIG § 30 Abs. 2 Nr. 4 – Sicherheit der Lieferkette
RR-003 · nächste Prüfung 10.03.2027
In Umsetzung
SM
BSIG § 32 – Meldepflichten bei erheblichen Sicherheitsvorfällen
RR-004 · nächste Prüfung 10.03.2027
Konform
ML
BSIG § 38 Abs. 1–2 – Billigung und Überwachung durch die Geschäftsleitung
RR-005 · nächste Prüfung 10.03.2027
Konform
JD
BSIG § 38 Abs. 3 – Schulung der Geschäftsleitung
RR-006 · nächste Prüfung 10.03.2027
Konform
JD
DSGVO – Datenschutz
DSGVO Art. 5, Art. 24 – Grundsätze und Rechenschaftspflicht
RR-007 · nächste Prüfung 10.03.2027
Konform
PW
Bereit.
WolfISMS Version 4.00

7. Datenschutz

Beschreibung

Seit v4.01 führt das Modul Datenschutz das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO, prüft je Verarbeitung, ob eine Datenschutz-Folgenabschätzung (DSFA) nötig ist, und führt die DSFA selbst. Sie finden es im Menü unter Governance & Compliance. Verarbeitungen hängen an Assets, Controls, Maßnahmen und Lieferanten – so sieht man, welche Systeme welche Personendaten verarbeiten und welche Maßnahmen sie schützen.

Verfügbarkeit: in jeder Edition, auch in der freien Version. Benutzerrecht: datenschutz (0 = kein Zugriff, 1 = Lesen, 2 = Bearbeiten), standardmäßig aus – auch für Benutzer, die es schon vor dem Update gab. Ihr Administrator vergibt es; Administratoren selbst brauchen es nicht. URL: /datenschutz

Verzeichnis von Verarbeitungstätigkeiten

- **Als Verantwortlicher (Art. 30 Abs. 1):** Bezeichnung, Beschreibung, Zweck, Rechtsgrundlagen (Art. 6 und Art. 9 zur Auswahl, bei berechtigtem Interesse mit Begründung), Betroffene und Datenkategorien (Vorschlagslisten, eigene Werte möglich), Löschfrist mit Auslöser, gemeinsame Verantwortlichkeit und zuständige Abteilung
- **Als Auftragsverarbeiter (Art. 30 Abs. 2):** je Auftraggeber aus den Kundenkontakten, mit den Kategorien der Verarbeitung, Datum und Dokument des AV-Vertrags – ohne Zweck, Rechtsgrundlage und Löschfrist, die legt der Auftraggeber fest
- **Empfänger:** intern (Abteilung), Lieferant, Behörde oder Sonstige, jeweils mit Land. Liegt das Land außerhalb von EU und EWR, ist es ein Drittland; dann wählen Sie die Garantie – Angemessenheitsbeschluss, Data Privacy Framework, Standardvertragsklauseln, BCR oder Ausnahme nach Art. 49. Ein Drittland ohne Garantie wird markiert
- **Verknüpfungen:** Assets, Controls, Maßnahmen und Unterauftragsverarbeiter
- **Status:** Entwurf → in Prüfung → Freigegeben. Freigeben lässt sich eine Verarbeitung als Verantwortlicher erst mit Zweck, Rechtsgrundlage und einer Schwellwertanalyse mit Ergebnis und Begründung, als Auftragsverarbeiter erst mit Auftraggeber. Ohne Wiedervorlage setzt die Freigabe sie auf heute + 12 Monate
- **Hinweis Art. 9:** wählen Sie Gesundheits-, biometrische oder andere besondere Daten, ohne eine Rechtsgrundlage aus Art. 9 anzugeben, weist die Seite darauf hin

Schwellwertanalyse

Je Verarbeitung als Verantwortlicher beantworten Sie zwei Fragen: Fällt sie unter die Muss-Liste der Aufsichtsbehörden nach Art. 35 Abs. 4 (vorbelegt mit der Liste der DSK, von Ihrem Administrator ergänzbar)? Und welche der neun Kriterien aus den Leitlinien WP 248 treffen zu – etwa vertrauliche Daten, schutzbedürftige Betroffene, große Menge, systematische Überwachung oder Scoring? WolfISMS schlägt ein Ergebnis vor: ist ein Eintrag der Muss-Liste getroffen oder treffen zwei oder mehr Kriterien zu, ist in der Regel eine DSFA erforderlich. Das Ergebnis legen Sie fest und begründen es; weicht es vom Vorschlag ab, steht das in der Seite.

Datenschutz-Folgenabschätzung

Ist eine DSFA nötig, legen Sie sie aus der Detailansicht der Verarbeitung an. Abschnitt 1 ist aus der Verarbeitung vorbelegt. Die DSFA steht im Modul unter dem Reiter „DSFA“.

© 2012–2026 WolfInfoSec GmbH

- **Feste Abschnitte nach Art. 35 Abs. 7:** systematische Beschreibung, Notwendigkeit und Verhältnismäßigkeit, Risiken für die Rechte und Freiheiten, Abhilfemaßnahmen, Stellungnahme des Datenschutzbeauftragten, Standpunkt der Betroffenen und Ergebnis – Restrisiko tragbar oder Konsultation der Aufsichtsbehörde nach Art. 36
- **Risikotabelle:** je Risiko die Quelle, der mögliche Schaden für die Betroffenen, Wahrscheinlichkeit und Schwere (je 1 geringfügig bis 4 groß) vor und nach den Maßnahmen. Der Wert ist das Produkt und wird immer berechnet. Das Restrisiko zählt nur Maßnahmen, die umgesetzt sind – sonst weist die Seite darauf hin
- **Status:** Entwurf → in Bearbeitung → Stellungnahme DSB → Abgeschlossen. Abschließen lässt sie sich erst mit Stellungnahme, Ergebnis und Restwerten für jedes Risiko
- **Überprüfung:** ändert sich die Verarbeitung nach dem Abschluss, zeigt die DSFA, dass sie zu überprüfen ist (Art. 35 Abs. 11)
- **Ins Risikoregister:** ein DSFA-Risiko übertragen Sie mit einem Klick über den KI-Assistenten für Risiken; danach verweist es auf den Eintrag im Risikoregister. Abhilfemaßnahmen legt der KI-Assistent für Maßnahmen an und verknüpft sie

Funktionen

- **Liste:** drei Reiter – als Verantwortlicher, als Auftragsverarbeiter, DSFA – mit Suche und Status; „Anlegen“ zum Aufklappen
- **Neu / Bearbeiten (datenschutz):** Verarbeitungen und DSFA anlegen und pflegen; ändern und löschen dürfen Besitzer und Masteruser
- **Excel-Export:** je Verzeichnis als .xlsx, zum Beispiel für die Aufsichtsbehörde
- **AVV-Angaben der Lieferanten:** siehe Kapitel Lieferanten
- **KI-Assistent (ab Essentials):** Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er legt eine Verarbeitung aus Ihrer Beschreibung an (auch als Auftragsverarbeiter), findet Assets mit Personenbezug, zu denen es noch keine Verarbeitung gibt, prüft einen Eintrag auf Lücken und Widersprüche, schlägt die Schwellwertanalyse vor, entwirft eine DSFA und erstellt die Anlage zu den technischen und organisatorischen Maßnahmen (Art. 32) als Word-Datei für AV-Verträge. Gespeichert wird erst, was Sie bestätigen.

Hinweise

WolfISMS und sein KI-Assistent leisten keine Rechtsberatung. Rechtsgrundlage, Löschfrist und das Ergebnis der Schwellwertanalyse sind Vorschläge; freigeben, eine DSFA abschließen und die Stellungnahme des Datenschutzbeauftragten schreiben tun Menschen.

© 2012–2026 WolfInfoSec GmbH

8. Risiken

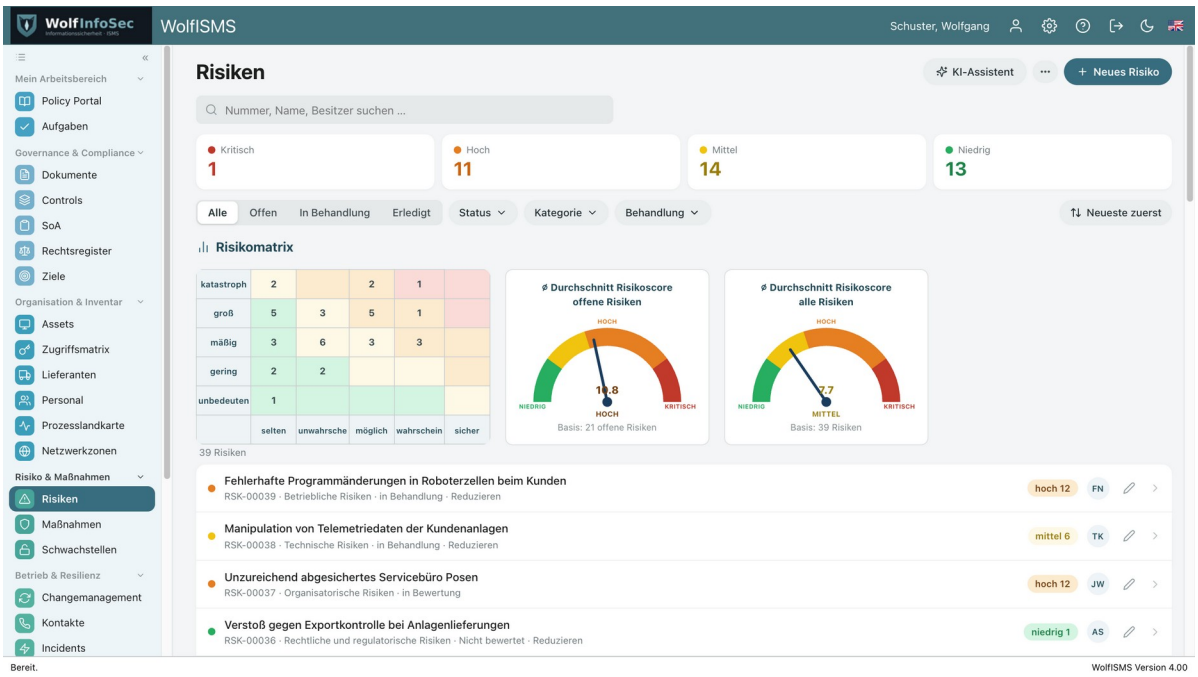
Beschreibung

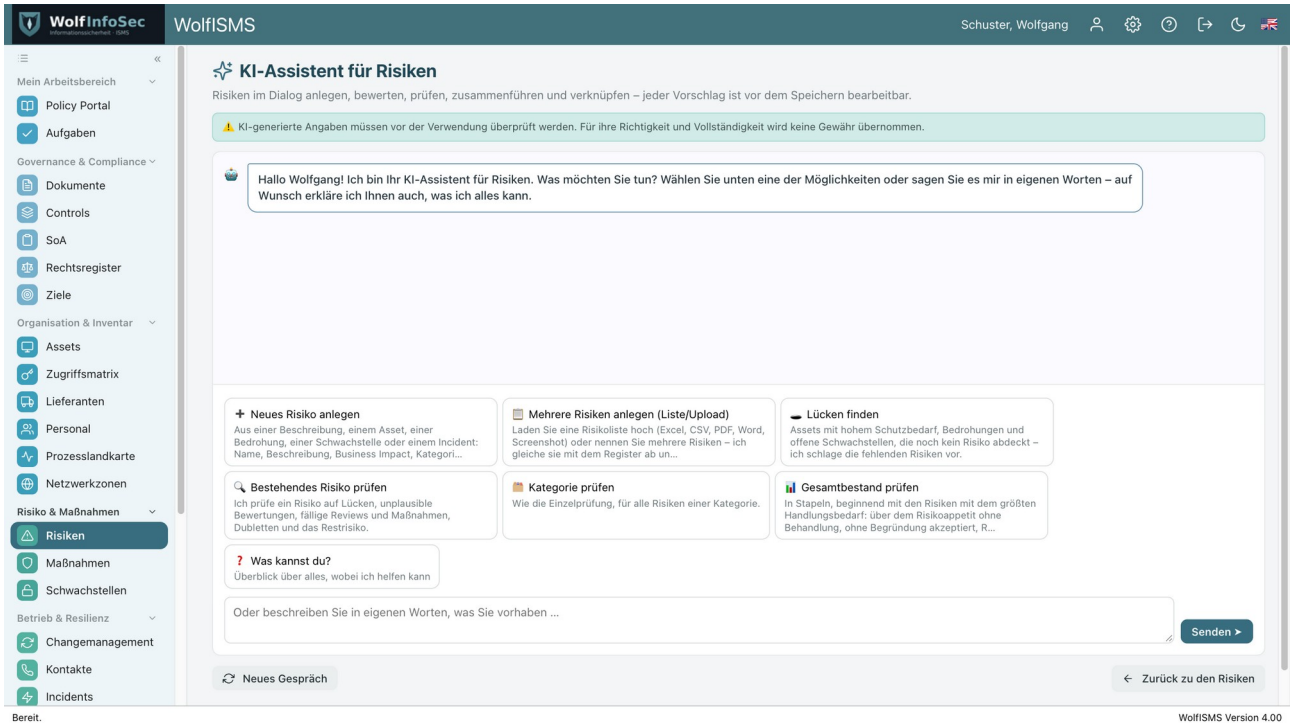
Das Risikomodul unterstützt den vollständigen Risikomanagementprozess gemäß ISO 27001 Kapitel 6.1. Risiken werden bewertet, Behandlungsoptionen festgelegt und mit Assets, Maßnahmen, Bedrohungen und Schwachstellen verknüpft.

Funktionen

- **Risikoübersicht**: Liste mit Suche, Kacheln je Risikostufe (ein Klick filtert) und Filtern nach Phase, Status, Kategorie und Behandlung; die Risikomatrix lässt sich über das Drei-Punkte-Menü ein- und ausblenden
- **Risikobewertung**: Eintrittswahrscheinlichkeit und Auswirkung jeweils vor und nach Maßnahmen (5-stufige Skala)
- **Risikostufen**: Automatische Berechnung: niedrig / mittel / hoch / kritisch
- **Risikobehandlung**: Optionen: Akzeptieren, Reduzieren, Vermeiden, Übertragen, Teilen
- **Verknüpfungen (risk)**: Verknüpfung mit Assets, Maßnahmen, Bedrohungen, Schwachstellen
- **Business Impact**: Freitextfeld für die Beschreibung der Geschäftsauswirkungen (Richtext)
- **Chancen**: Das positive Gegenstück zum Risiko – was sich gewinnen lässt, wenn man es angeht (ISO 27001 Kapitel 6.1.1). Das Feld steht im Formular unter dem Business Impact, erscheint in der Detailansicht und im PDF der Risiko-Managementbewertung und wird dem KI-Assistenten mitgegeben, sofern es gefüllt ist
- **Risiko-Managementreview**: Zusammenstellung der offenen kritischen und hohen Risiken als Vorlage für die Leitungsbewertung – dieselbe Auswertung erscheint im Modul Managementbewertung. Über „PDF-Export" entsteht daraus ein fertiges Dokument für die Sitzung; ist ein PDF-Briefpapier hinterlegt, wird es als Kopf- und Fußzeile verwendet. Detailtexte und Maßnahmen lassen sich vorher ein- und ausblenden
- **Risikoscore-Verlauf**: Unter /risiko/historie zeigt ein Liniendiagramm die Entwicklung dreier Durchschnitts-Scores über die Zeit: ⌀ offene Risiken, ⌀ alle Risiken und ⌀ aktive Lieferanten. Zeitraum wählbar (30 Tage, 90 Tage, 6 Monate, 1 Jahr, Alle). Ein Snapshot wird täglich automatisch erstellt und kann auf der Seite auch manuell ausgelöst werden
- **Excel-Export**: Export des gesamten Risikoregisters als .xlsx
- **Kategorie-Chart**: Kreisdiagramm der Risikoverteilung nach Kategorie
- **Kommentare**: Diskussionsfaden in der Seitenleiste jedes Risikos; jeder angemeldete Benutzer (außer readonly) kann kommentieren und antworten
- **Detailansicht:** Nummer und Name stehen in der Überschrift. Die Seitenleiste zeigt seit v3.94 von oben nach unten die Eigenschaften (Kategorie, Besitzer, Abteilung, Status, Risikobehandlung), die Metadaten, die Bewertung vor und nach Maßnahmen und die Verknüpfungen. Der Hauptbereich beginnt mit Beschreibung, Business Impact und Chancen
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch, in dem die KI mit Ihnen Risiken anlegt, prüft und verknüpft – siehe den Abschnitt KI-Assistent für Risiken

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
Mein Arbeitsbereich
Policy Portal
Aufgaben
Governance & Compliance
Dokumente
Controls
SoA
Rechtsregister
Ziele
Organisation & Inventar
Assets
Zugriffsmatrix
Lieferanten
Personal
Prozesslandkarte
Netzwerkzonen
Risiko & Maßnahmen
Risiken
Maßnahmen
Schwachstellen
Betrieb & Resilienz
Changemanagement
Kontakte
Incidents
Risiken
KI-Assistent
Neues Risiko
Nummer, Name, Besitzer suchen ...
Kritisch 1
Hoch 11
Mittel 14
Niedrig 13
Alle
Offen
In Behandlung
Erledigt
Status
Kategorie
Behandlung
Neueste zuerst
Risikomatrix
katastroph
groß
mäßig
gering
unbedeuten
selten
unwahrsche
möglich
wahrschein
sicher
39 Risiken
ø Durchschnitt Risikoscore offene Risiken
HOCH
NIEDRIG
KRITISCH
Basis: 21 offene Risiken
ø Durchschnitt Risikoscore alle Risiken
MITTEL
Basis: 39 Risiken
Fehlerhafte Programmänderungen in Roboterzellen beim Kunden
RSK-00039 · Betriebliche Risiken · in Behandlung · Reduzieren
hoch 12
FN
Manipulation von Telemetriedaten der Kundenanlagen
RSK-00038 · Technische Risiken · in Behandlung · Reduzieren
mittel 6
TK
Unzureichend abgesichertes Servicebüro Posen
RSK-00037 · Organisatorische Risiken · in Bewertung
hoch 12
JW
Verstoß gegen Exportkontrolle bei Anlagenlieferungen
RSK-00036 · Rechtliche und regulatorische Risiken · Nicht bewertet · Reduzieren
niedrig 1
AS
Bereit.
WolfISMS Version 4.00



KI-Assistent für Risiken

Der KI-Assistent ist ein Gespräch auf einer eigenen Seite: links der Chat, darunter die Antwortmöglichkeiten, rechts der Entwurf, den Sie jederzeit selbst ändern können. Die KI begrüßt Sie, fragt, was Sie vorhaben, und erklärt auf Wunsch, was sie kann. Sie brauchen dafür das Bearbeitungsrecht für Risiken.

- **Neues Risiko anlegen:** aus einer kurzen Beschreibung oder ausgehend von einem Asset, einer Bedrohung, einer Schwachstelle oder einem Incident. Die KI entwirft Name, Beschreibung, Business Impact, Chancen, Kategorie und Bewertung; danach schlägt sie Verknüpfungen zu Bedrohungen, Schwachstellen, Maßnahmen, Lieferanten, Controls, Dokumenten und Incidents vor. Fehlende Maßnahmen und Lieferanten legt sie auf Wunsch mit an
- **Mehrere Risiken anlegen:** eine Risikoliste hochladen (Excel, CSV, PDF, Word, Bildschirmfoto) oder im Chat aufzählen; der Assistent gleicht sie mit dem Register ab und geht sie nacheinander durch
- **Lücken finden:** Assets mit hohem Schutzbedarf, Bedrohungen und offene Schwachstellen, die noch kein Risiko abdeckt – der Assistent schlägt die fehlenden Risiken vor
- **Prüfen:** ein einzelnes Risiko, alle Risiken einer Kategorie oder den Gesamtbestand – auf Lücken, unplausible Bewertungen, fällige Reviews und Maßnahmen, Dubletten und das Restrisiko. Beim Gesamtbestand beginnt er mit den Risiken mit dem größten Handlungsbedarf
- **Nichts ohne Ihr Ja:** jeder Vorschlag hat eine Begründung; Sie haken ab, geben einen Hinweis im Freitext oder überspringen. Geschrieben wird erst mit „Übernehmen“. Haben Sie die Seite verlassen, können Sie beim nächsten Aufruf weitermachen

© 2012–2026 WolfInfoSec GmbH

9. Assets

Beschreibung

Das Asset-Modul verwaltet alle informationsverarbeitenden Assets des Unternehmens. Es unterstützt die Klassifizierung nach Vertraulichkeit, Integrität und Verfügbarkeit (CIA) sowie die Kritikalitätsbewertung. Die Kategorien folgen der OBASHI-Systematik (Ownership, Business Process, Application, System, Hardware, Infrastructure) und werden in dieser Reihenfolge dargestellt; Informationswerte stehen am Ende.

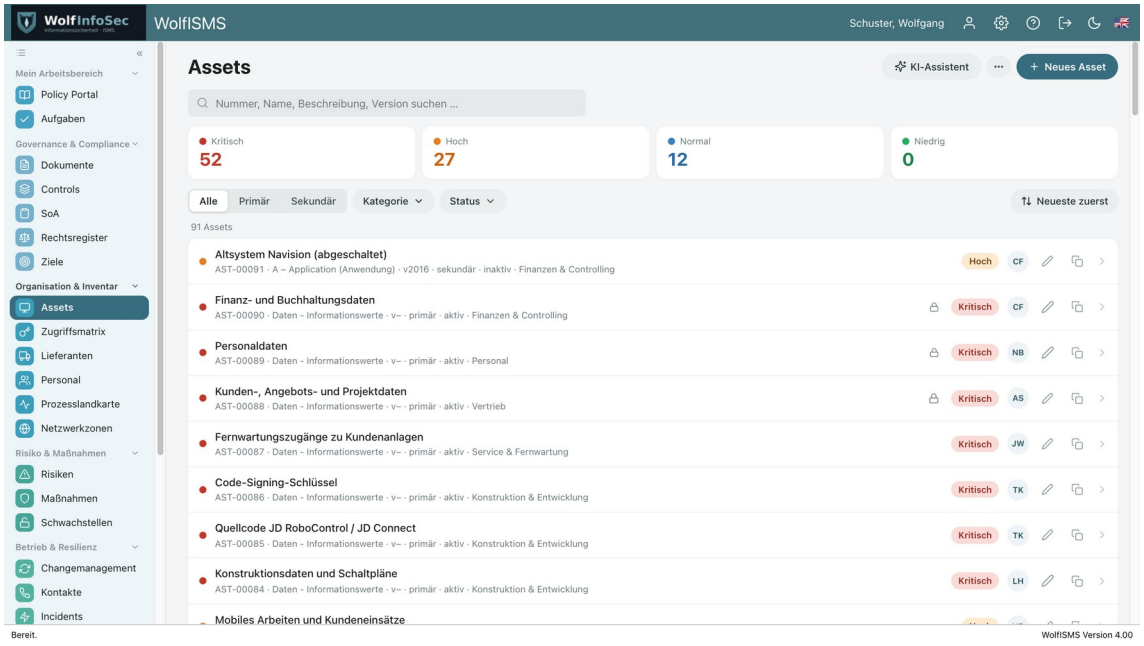
Funktionen

- **Asset-Übersicht**: Liste mit Suche und Filtern nach Typ, Kategorie, Abteilung und Status; die Kategoriekacheln erscheinen, wenn Ihr Administrator die Infokacheln eingeschaltet hat
- **Version**: Freitextfeld für den Release- oder Patchstand eines Assets (z. B. „2024 R2“ oder „15.0.4355“). Es steht zwischen Name und Beschreibung, bildet in der Assetliste und im Excel-Export eine eigene Spalte und lässt sich über die Suche finden und über die Spaltenüberschrift sortieren. Auch die Verknüpfungslisten zeigen die Version: die Tochterassets im Assetmodul und „Assets verknüpfen“ in Risiken, Lieferanten, Incidents und Schwachstellen.
- **CIA-Bewertung**: Einstufung nach Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität (CIAA, je 1–5)
- **Bemerkungen zum Schutzbedarf:** Seit v3.95 hat jedes der vier Schutzziele ein eigenes Feld „Bemerkung – warum diese Stufe?“. Die Detailansicht zeigt die Bemerkung klein unter der Stufe in der jeweiligen CIA-Karte. Schlägt der KI-Assistent den Schutzbedarf vor, schreibt er seine Begründung bei der Übernahme dort hinein, und wird ein Schutzziel vererbt, vermerkt die Bemerkung, von welchem Elternasset und wann (z. B. „Vom Elternasset AST00012 geerbt (hoch) am 17.10.2026.“). Beim Kopieren eines Assets gehen die Bemerkungen mit
- **Klassifizierung**: Öffentlich / Intern / Vertraulich / Streng vertraulich
- **Kritikalität**: Bewertung der Geschäftskritikalität des Assets
- **Personenbezug**: Kennzeichnung, ob das Asset personenbezogene Daten verarbeitet (DSGVO-relevant)
- **Teilassets und Hierarchie**: Hierarchische Verknüpfung von Unter-Assets (z. B. Server → Applikationen); die Übersicht stellt die Über- und Unterordnung eingerückt dar
- **Tochterasset hinzufügen:** Die Schaltfläche in der Detailansicht und in der Baumansicht legt seit v3.95 ein neues Asset an, das nach dem Speichern als Tochterasset verknüpft ist. Das Formular ist vorbelegt: Typ „sekundär“, als Kategorie die nächste OBASHI-Ebene unter dem Elternasset und der Schutzbedarf des Elternassets samt Vererbungsvermerk in den Bemerkungen. Aus der Baumansicht geht es nach dem Speichern dorthin zurück
- **CIA-Vererbung**: CIA-Werte können von frei wählbaren Quell-Assets übernommen werden (Button „CIA aus Quellen übernehmen“) – es wird jeweils der höhere Wert gesetzt. Zusätzlich lassen sich Werte an Teilassets weitergeben (Button „Vererben“, OBASHI-Top-Down-Prinzip); bestehende höhere Einstufungen bleiben erhalten
- **Kritikalitätsformel**: Automatische Berechnung nach dem Maximumprinzip (BSI-Standard 200-2): die Kritikalität ist die höchste Stufe aus Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Wert. Ein einzelnes hohes Schutzziel wird so nicht durch niedrige übrige Werte verdünnt – dieselbe Regel, nach der die Vererbung den Schutzbedarf weitergibt. Von Hand setzen lässt sich die Kritikalität nicht
- **Abteilungszuordnung**: Die Abteilung wird aus der zentral gepflegten Abteilungs- und Teamliste ausgewählt statt frei eingetippt
- **Review-Datum**: Geplantes Überprüfungsdatum mit automatischer Aufgabenerzeugung
- **Wiederanlaufziele**: RTO, RPO und MAZ für die Business Continuity, gewählt aus festen Stufen von 1 Stunde bis 30 Tage (RPO auch 0 – kein Datenverlust). Die RTO darf die MAZ nicht

© 2012–2026 WolfInfoSec GmbH

übersteigen. Die Werte erscheinen in der Detailansicht, im Excel-Export und -Import und in der BIA des BCM-Moduls

- **Excel-Export**: Vollständiger Asset-Export als .xlsx
- **Excel-Import**: Eine exportierte Mappe lässt sich unverändert wieder einlesen (/assets/import). Schlüssel ist die Asset-Nummer in Spalte A: eine bekannte Nummer aktualisiert das Asset, eine unbekannte oder leere legt auf Wunsch ein neues an. Leere Zellen ändern nichts, ein Wert außerhalb der zugehörigen Auswahlliste wird gemeldet und die Zeile übersprungen – es wird nichts geraten. Ohne das Häkchen „Übernehmen" bleibt es bei einer Vorschau. Die Kritikalität wird aus CIAA und Wert berechnet (Maximumprinzip) und deshalb nicht eingelesen, und geändert wird nur, was Sie auch im Formular ändern dürften
- **Kommentare**: Diskussionsfaden in der Seitenleiste jedes Assets für Rückfragen und Abstimmungen
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch, in dem die KI mit Ihnen Assets anlegt, prüft, den Schutzbedarf vorschlägt und Verknüpfungen bis hin zu den Risiken findet – siehe den Abschnitt KI-Assistent für Assets. Die früheren Knöpfe „KI-Risikoanalyse“ und „KI-Schutzbedarf“ sind darin aufgegangen



KI-Assistent für Assets

Aufgebaut wie der KI-Assistent für Risiken: ein Gespräch auf einer eigenen Seite, links der Chat, rechts der bearbeitbare Entwurf. Sie brauchen das Bearbeitungsrecht für Assets; was dabei in anderen Modulen entsteht, etwa ein Lieferant oder ein Risiko, verlangt auch dort das Recht.

- **Neues Asset anlegen:** aus einer kurzen Beschreibung schlägt die KI Name, Beschreibung, OBASHI-Kategorie, Typ, Version, Klassifizierung, Schutzbedarf und Wiederanlaufziele vor, je mit Begründung. Danach folgen Verknüpfungen – untergeordnete Assets, Lieferanten, Risiken, Schwachstellen, Controls und Incidents. Fehlende Lieferanten legt sie auf Wunsch mit an
- **Mehrere Assets anlegen:** eine Asset-Liste hochladen (Excel, CSV, PDF, Word, Bildschirmfoto) oder im Chat aufzählen; Besitzer und Abteilung fragt der Assistent einmal für alle
- **Prüfen:** ein einzelnes Asset, alle Assets einer OBASHI-Ebene oder den Gesamtbestand – auf Lücken und unplausible Werte, mit Vorschlägen für Ergänzungen und Verknüpfungen. Beim Gesamtbestand beginnt er mit den Assets ohne Verknüpfungen, Schutzbedarf, Besitzer oder Zeitziele
- **Schutzbedarf:** die vorgeschlagene Stufe je Schutzziel steht mit Begründung im Entwurf; übernommen wird die Begründung als Bemerkung des Schutzziels

- **Nichts ohne Ihr Ja:** geschrieben wird erst mit „Übernehmen“; jeden Bereich der Verknüpfungen können Sie auch überspringen

© 2012–2026 WolfInfoSec GmbH

10. Zugriffsmatrix

Beschreibung

Die Zugriffsmatrix dokumentiert, welche Rolle auf welches Asset zugreifen darf. Sie ist die Soll-Vorgabe für die Rechtevergabe und der Nachweis für ISO/IEC 27001 A.5.15 (Zugangssteuerung) und A.5.18 (Zugangsrechte einschließlich Rezertifizierung). Kategorie und Schutzbedarf der Assets werden live aus dem Assetmanagement gelesen – die Matrix kann deshalb nicht vom Asset-Inventar abweichen.

Verfügbarkeit: Die Zugriffsmatrix gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In den übrigen fehlt der Menüpunkt; Rollen lassen sich dort weiterhin unter Administration → Rollen pflegen. Fehlt das Modul im Menü, hat der Administrator es unter Administration → Module abgeschaltet – die erfassten Daten bleiben dabei erhalten und sind nach dem Wiedereinschalten unverändert da.

Berechtigungsstufen

Grundlage ist das Prinzip Deny-by-default: Ohne ausdrückliche Festlegung gilt „kein Zugriff". Jede Abweichung davon ist zu begründen und zu genehmigen.

Code	Stufe	Bedeutung
n	Kein Zugriff (none)	Standard. Jede Abweichung ist zu begründen und zu genehmigen
r	Lesen (read)	Lesender Zugriff auf Daten und Konfiguration, keine Veränderung möglich
rw	Schreiben (read/write)	Anlegen und Ändern eigener bzw. fachlich zugeordneter Datensätze (inkl. r)
f	Vollzugriff fachlich (full access)	Zusätzlich Löschen, Freigeben, Stammdatenpflege, Massenexport (inkl. rw)
a	Administrativ / privilegiert (admin)	Technische Systemverwaltung, Rechtevergabe, Umgehung fachlicher Kontrollen. Nur über ein separates Admin-Konto mit MFA
e	Notfallzugriff (emergency / break-glass)	Inaktives, versiegeltes Konto. Aktivierung nur nach dokumentiertem Notfallverfahren, Nachbewertung innerhalb von 24 h

Die Codes haben sich nach v3.51 geändert.
Bis einschliesslich 3.51 hiessen die Stufen –, L, S, V, A und N. Die neuen Codes sind die englischen Kürzel und in beiden Sprachfassungen gleich, damit ein Export unabhängig von der Sprache des Exportierenden gelesen werden kann. Die Umstellung der vorhandenen Daten erledigt WolfISMS einmalig von selbst, und eine ältere Excel-Mappe lässt sich unverändert weiter importieren – die alten Kürzel werden beim Import erkannt. Achten Sie dabei auf die Gross- und Kleinschreibung: „N" war der Notfallzugriff, „n" ist heute „kein Zugriff".

Zugriffsverfahren

Je Asset wird zusätzlich festgehalten, wie der Zugriff authentifiziert wird. Das ist der Nachweis für ISO/IEC 27001 A.5.17 (Authentifizierungsinformation) und A.8.5 (sichere Authentifizierung).

© 2012–2026 WolfInfoSec GmbH

Verfahren	Bedeutung
Login	Anmeldung mit Benutzername und Passwort im System selbst
SSO	Anmeldung über den zentralen Identity Provider
MFA	Zusätzlicher zweiter Faktor
Zertifikat	Client-Zertifikat

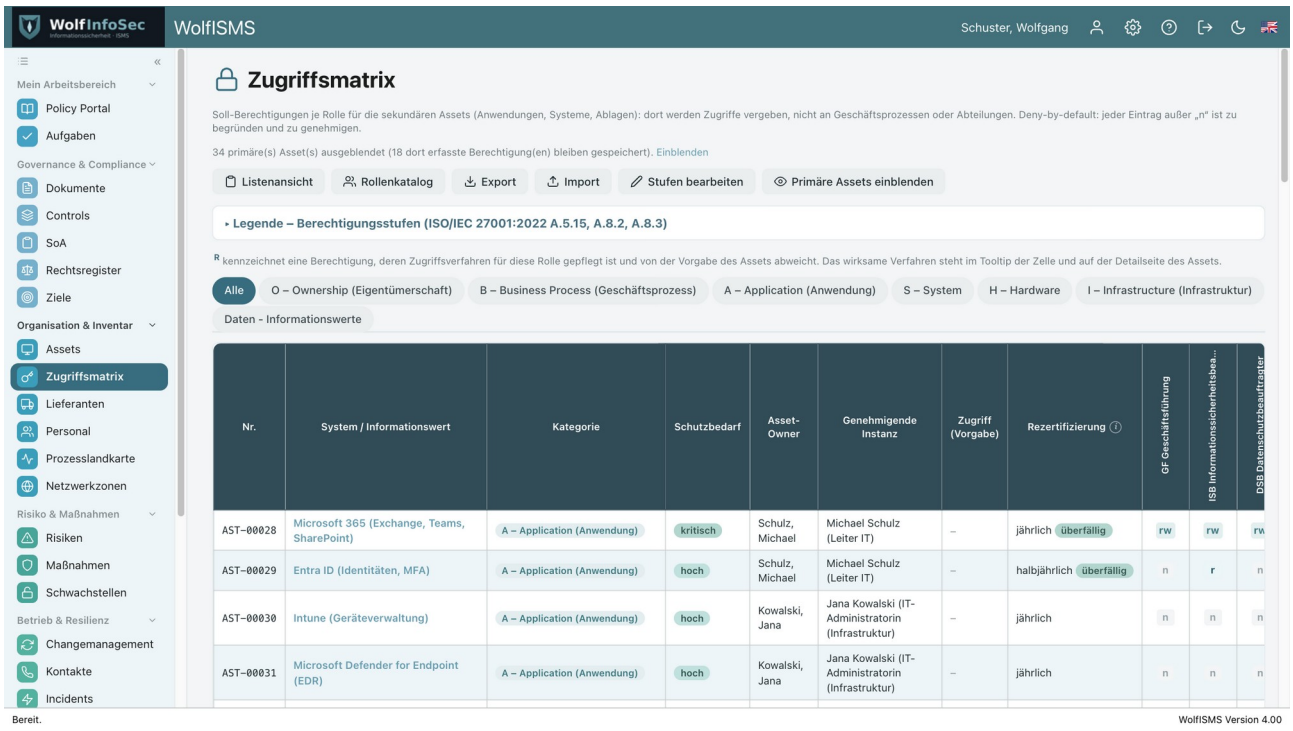
Mehrfachauswahl ist ausdrücklich vorgesehen: MFA und Zertifikat treten in der Praxis zusätzlich zu Login oder SSO auf, nicht an deren Stelle. Am Asset steht die Vorgabe, die für alle Rollen gilt; einzelne Rollen können davon abweichen – etwa wenn für den administrativen Zugang MFA verlangt wird, für den lesenden nicht.

Funktionen

- **Kreuztabelle**: Matrix Asset × Rolle mit Kategorie-Tabs. Die Stufen lassen sich direkt in der Tabelle ändern und gesammelt speichern. Seit v3.99 zeigt sie nur sekundäre Assets – Anwendungen, Systeme, Ablagen –, an denen Berechtigungen technisch vergeben werden; der Schalter „Primäre Assets einblenden“ holt Geschäftsprozesse und Informationswerte dazu. Vorhandene Einträge zu primären Assets bleiben erhalten
- **Detailpflege je Asset**: Je Berechtigung werden Stufe, Genehmiger, Genehmigungsdatum, letzte und nächste Überprüfung sowie eine fachliche Begründung (Need-to-know) erfasst
- **Vorgaben je Asset**: Am Asset stehen die genehmigende Instanz, das vorgesehene Zugriffsverfahren, die Rezertifizierungsfrequenz und die Auflagen bzw. kompensierenden Maßnahmen. Sie gelten für alle Rollen, solange eine Rolle nichts Eigenes hinterlegt hat
- **Rezertifizierung**: Wählbare Frequenz vierteljährlich, halbjährlich oder jährlich. Fällige und überfällige Prüfungen werden farblich gekennzeichnet
- **Privilegierte Rechte**: Die Stufen a und e gelten als privilegiert und werden in Listen und Kennzahlen gesondert ausgewiesen
- **Listenansicht**: Filterbare Liste aller Berechtigungen nach Rolle, Stufe, privilegiert und Rezertifizierungsstatus – die schnellste Sicht für eine Prüfung
- **Rollenkatalog**: Pflege der Rollen mit Kürzel, Organisationseinheit, Kennzeichen „privilegiert“, Aktiv-Status, Sortierung und Beschreibung; dazu die Kennzahl, wie viele privilegierte Berechtigungen eine Rolle besitzt
- **Excel-Export**: Export in fünf Blättern: Anleitung & Legende, Rollenkatalog, Zugriffsmatrix, Berechtigungen und ISO-27001-Mapping
- **Excel-Import**: Import einer ausgefüllten Mappe mit Vorschau: vor dem Speichern wird angezeigt, was übernommen und was übersprungen wird

Benutzerrecht: assets (0 = kein Zugriff, 1 = Lesen, 2 = Bearbeiten) – URL: /zugriffsmatrix

© 2012–2026 WolfInfoSec GmbH



Hinweise

Rollen anlegen und löschen:
Die Katalogfelder einer Rolle darf jeder Benutzer mit Bearbeitungsrecht auf Assets pflegen. Die Rollenbezeichnung selbst sowie das Anlegen und Löschen von Rollen sind Master- und Admin-Benutzern vorbehalten, weil Rollen unternehmensweit auch in der Benutzerverwaltung und im Personalmodul verwendet werden. Eine Rolle, die noch irgendwo zugewiesen ist, lässt sich nicht löschen – sie kann stattdessen auf „nicht aktiv" gesetzt werden. Dieselbe Rollenliste steht unter Administration → Rollen; dort werden die Rollen zusätzlich den Benutzerkonten zugeordnet.

Import aus einer fremden Mappe:
Die Zuordnung beim Import erfolgt über die Rollenbezeichnung, nicht über das Kürzel. Hinter „R01" kann in einer fremden Datei eine ganz andere Rolle stehen als im eigenen Katalog. Nicht zuordenbare Zeilen und Spalten werden gemeldet und übersprungen, statt falsch zugeordnet zu werden.

© 2012–2026 WolfInfoSec GmbH

11. Changemanagement

Beschreibung

Das Changemanagement steuert Änderungen an Systemen, Anwendungen und Konfigurationen, bevor sie passieren: Wer etwas ändern will, stellt einen Änderungsantrag (Change) mit Begründung, Zeitfenster und den Plänen für Umsetzung, Test und Rückfall. Ein Gremium gibt ihn frei, danach wird umgesetzt und zum Schluss nachbetrachtet. So entsteht der Nachweis, den ISO/IEC 27001 A.8.32 (Änderungssteuerung) verlangt.

Das Modul nutzt das Recht assets: Wer Assets lesen darf, sieht die Changes, wer Assets bearbeiten darf, legt sie an und führt sie durch. Wer als Genehmiger benannt ist, stimmt auch mit reinem Leserecht ab.

Ablauf eines Changes

- **1. Entwurf**: Titel, Beschreibung und Begründung, Typ, Kategorie, Priorität, Risiko und Auswirkung der Änderung, geplantes Zeitfenster mit erwarteter Ausfallzeit, Umsetzer sowie Umsetzungs-, Test- und Rückfallplan. Jeder Change bekommt eine Nummer im Format CHG-00001.
- **2. Gremium benennen**: Unter „Freigabegremium“ tragen Sie die Genehmiger ein, jeweils mit Rolle und Stufe (1 bis 3). Eine höhere Stufe stimmt erst ab, wenn alle der Stufe darunter zugestimmt haben.
- **3. Einreichen**: Ab jetzt stimmen die Genehmiger ab. Sobald alle zugestimmt haben, ist der Change genehmigt; eine einzige Ablehnung lehnt ihn ab. Ein abgelehnter oder zurückgezogener Change lässt sich überarbeiten – die Abstimmung beginnt dann von vorn.
- **4. Umsetzen**: „Umsetzung starten“, danach „Umsetzung beendet“. Geht etwas schief, führt „Zurückrollen“ den Rückfallplan aus.
- **5. Nachbetrachtung**: Nach der Umsetzung oder dem Zurückrollen ist innerhalb von 14 Tagen festzuhalten, wie es gelaufen ist – Datum, Ergebnis und Bemerkung. Erst dann lässt sich der Change abschließen.

Typ	Bedeutung
Standard	Vorab genehmigte Routineänderung – braucht kein Gremium und ist mit dem Einreichen genehmigt
Normal	Gewöhnliche Änderung mit Freigabe durch das Gremium
Wesentlich	Größere Änderung mit Freigabe durch das Gremium
Notfall	Darf sofort umgesetzt werden; das Gremium stimmt nachträglich ab

Funktionen

- **Liste**: alle Changes mit Kennzahlen, Filter nach Status, Typ, Kategorie und Risiko sowie Volltextsuche.
- **Detailansicht**: Stammdaten, die drei Pläne, das Freigabegremium mit dem Stand jeder Stimme, die Schaltflächen für den nächsten möglichen Schritt und die Historie aller Statuswechsel.
- **Verknüpfungen**: Assets, Risiken, Maßnahmen, Incidents und Dokumente lassen sich mit einem Change verbinden.
- **Änderungskalender**: alle Changes mit geplantem Beginn im Monatsüberblick – so fallen Überschneidungen auf.

© 2012–2026 WolfInfoSec GmbH

- **Aufgaben**: das geplante Zeitfenster, eine offene Stimme im Gremium und eine fällige Nachbetrachtung erscheinen unter „Meine Aufgaben“ und in der Erinnerungsmail.
- **Bearbeiten und Löschen**: durch einen der Besitzer oder einen Master-Benutzer. Der Status wechselt nur über die Schritte, nicht über das Formular.
- **Excel-Export**: Schaltfläche „Excel“ in der Filterleiste, übernimmt die Filter. Das Blatt „Kennzahlen“ zeigt je Typ die offenen, abgeschlossenen, abgelehnten und zurückgerollten Changes sowie die durchgeführten, überfälligen und erfolgreichen Nachbetrachtungen, das Blatt „Changes“ alle Termine, das Freigabegremium mit Stufe, Rolle und Votum und die Nachbetrachtung. Überfällige Nachbetrachtungen sind rot markiert
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er entwirft und prüft Changes (frei oder ausgehend von einer Maßnahme, Schwachstelle, einem Incident oder Risiko), begleitet einen Statusschritt, schlägt das Gremium vor, bereitet die Nachbetrachtung vor, geht Ihre offenen Changes durch, findet Kollisionen im Änderungskalender und schreibt einen Lagebericht. Abstimmen tut der Assistent nie. Gespeichert wird erst, was Sie bestätigen.

Benutzerrecht: assets (0 = kein Zugriff, 1 = Lesen, 2 = Bearbeiten) – URL: /change

© 2012–2026 WolfInfoSec GmbH

12. Maßnahmen

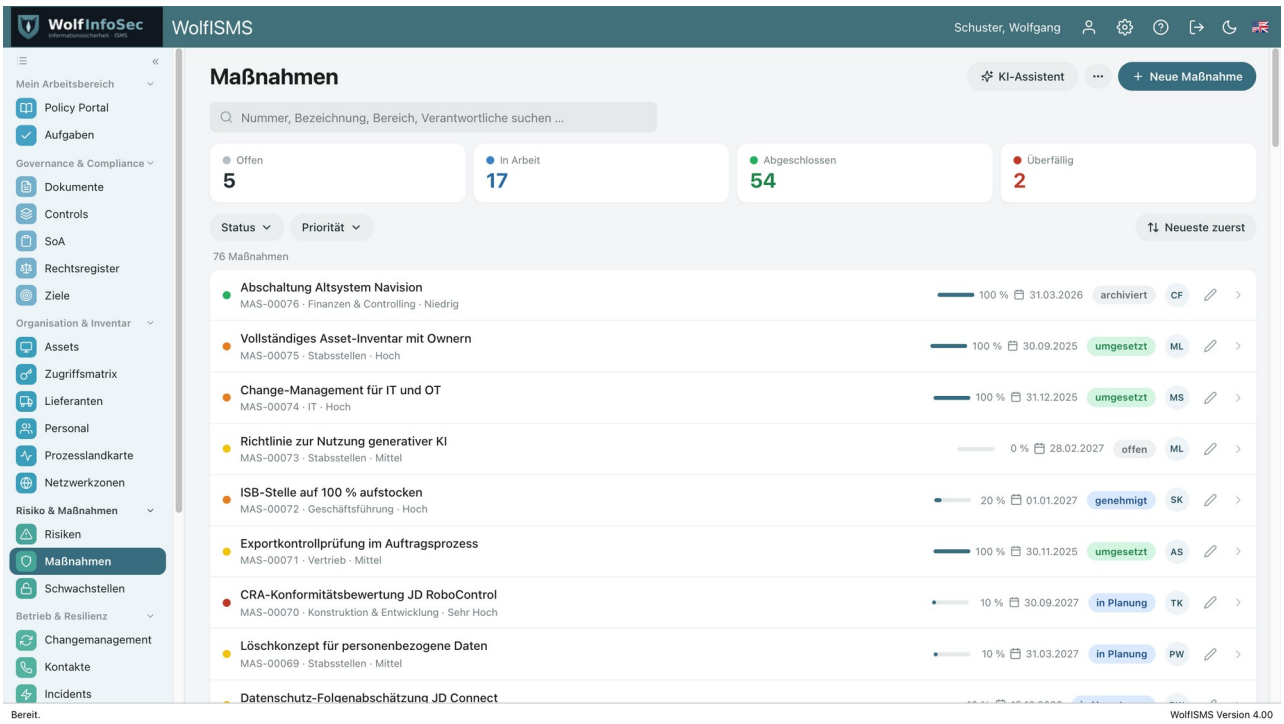
Beschreibung

Das Maßnahmen-Modul verfolgt alle Sicherheits- und Compliance-Maßnahmen. Es verbindet Controls, Risiken, Lieferanten und Incidents mit konkreten Umsetzungsaufgaben.

Funktionen

- **Status-Tabs**: Schnellfilter: Alle / Offen / In Arbeit / Erledigt / Abgebrochen
- **Fortschrittsbalken**: Prozentualer Umsetzungsgrad mit Ampelfarbe je Maßnahme
- **Detailansicht**: Vollständige Maßnahmenbeschreibung, Besitzer, Abteilung, Enddatum, Richtext-Inhalt
- **Anhänge**: Upload und Verwaltung von Anhängen (Dokumente, Nachweise) im PDF-Format
- **Verknüpfungen (mass)**: Verlinkung mit Risiken, Controls, Lieferanten, Incidents und Assets – ein Asset zeigt seine Maßnahmen direkt und über Risiken, Schwachstellen, Changes und Incidents
- **Managementbewertungen**: Eine Maßnahme, die aus einer Leitungsbewertung hervorgeht, zeigt in der Detailansicht, zu welchen Bewertungen sie gehört. Sichtbar ist das für Benutzer mit dem Recht Audit – dort liegt die Managementbewertung. Über „Verknüpfungen verwalten" lässt sich die Zuordnung seit v3.71 auch von der Maßnahme aus setzen und lösen; dafür wird das Bearbeitungsrecht Audit benötigt
- **Review**: Geplantes Review-Datum mit automatischer Aufgabenerzeugung
- **Excel-Export**: Gesamtexport oder gefiltert nach Status als .xlsx
- **Status-Chart**: Kreisdiagramm der Maßnahmen nach Status
- **Ticketnummer**: Trägt eine Maßnahme eine Ticketnummer – meist vom angebundenen Ticketsystem über die REST-API gesetzt –, steht sie in der Liste und in der Detailansicht als Link und öffnet das Ticket in einem neuen Tab. Übernommen werden dabei nur Linkziel und Beschriftung; fremde Auszeichnungen werden nicht durchgereicht
- **Kommentare**: Diskussionsfaden je Maßnahme
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er legt Maßnahmen an – frei oder aus einem Risiko, Control, einer Abweichung, einem Incident, einer Schwachstelle, einem Lieferanten oder dem Rechtsregister, auch mehrere aus einem Bericht oder Maßnahmenplan –, findet, was noch keine Maßnahme hat, prüft, führt zusammen, fragt in der Statusrunde den Stand Ihrer fälligen Maßnahmen ab, belegt die Umsetzung mit einem Nachweis und schlägt eine Umsetzungsreihenfolge vor. Gespeichert wird erst, was Sie bestätigen.

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
Mein Arbeitsbereich
Policy Portal
Aufgaben
Governance & Compliance
Dokumente
Controls
SoA
Rechtsregister
Ziele
Organisation & Inventar
Assets
Zugriffsmatrix
Lieferanten
Personal
Prozesslandkarte
Netzwerkzonen
Risiko & Maßnahmen
Risiken
Maßnahmen
Schwachstellen
Betrieb & Resilienz
Changemanagement
Kontakte
Incidents
Maßnahmen
KI-Assistent
Neue Maßnahme
Nummer, Bezeichnung, Bereich, Verantwortliche suchen ...
Offen 5
In Arbeit 17
Abgeschlossen 54
Überfällig 2
Status
Priorität
Neueste zuerst
76 Maßnahmen
Abschaltung Altsystem Navision
MAS-00076 · Finanzen & Controlling · Niedrig
100 % 31.03.2026 archiviert CF
Vollständiges Asset-Inventar mit Ownern
MAS-00075 · Stabsstellen · Hoch
100 % 30.09.2025 umgesetzt ML
Change-Management für IT und OT
MAS-00074 · IT · Hoch
100 % 31.12.2025 umgesetzt MS
Richtlinie zur Nutzung generativer KI
MAS-00073 · Stabsstellen · Mittel
0 % 28.02.2027 offen ML
ISB-Stelle auf 100 % aufstocken
MAS-00072 · Geschäftsführung · Hoch
20 % 01.01.2027 genehmigt SK
Exportkontrollprüfung im Auftragsprozess
MAS-00071 · Vertrieb · Mittel
100 % 30.11.2025 umgesetzt AS
CRA-Konformitätsbewertung JD RoboControl
MAS-00070 · Konstruktion & Entwicklung · Sehr Hoch
10 % 30.09.2027 in Planung TK
Löschkonzept für personenbezogene Daten
MAS-00069 · Stabsstellen · Mittel
10 % 31.03.2027 in Planung PW
Datenschutz-Folgenabschätzung JD Connect
Bereit.
WolfISMS Version 4.00

13. Projekte

Beschreibung

Das Projektmodul führt Vorhaben nach dem ISMS-Rahmen aus ISO/IEC 27001 A.5.8 „Informationssicherheit im Projektmanagement“: Jedes Projekt nennt Klassifizierung und Sicherheitsverantwortung, beschreibt Sicherheitsanforderungen und Risiken, durchläuft Sicherheits-Gates und endet mit einer geordneten Übergabe samt Lessons Learned. Der Fortschritt errechnet sich aus den verknüpften Maßnahmen.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet.

Funktionen

- **Projektübersicht:** Liste aller Projekte mit Fortschritt, ISMS-Ampel, Besitzer und Status; Kacheln je Phase filtern mit einem Klick, die Suche beim Tippen
- **Steckbrief:** Auftraggeber, Sicherheitsverantwortung und die höchste Klassifizierung der Informationen im Projekt, dazu Besitzer, Status und Zeitraum
- **Feste Abschnitte:** Ziel und Nutzen, Umfang und Abgrenzung, Klassifizierung und Ablage, Sicherheitsanforderungen an das Ergebnis, Risikobewertung zu Projektbeginn, Ergebnis und Stand, Übergabe in den Betrieb, Lessons Learned, Restrisiko nach Projektende – jeder mit einem Hinweis, was nach ISO/IEC 27001 A.5.8 hineingehört
- **Projektrollen:** Rolle und Person – ein Benutzer oder, für Externe, ein Name. Vorgeschlagen sind Auftraggeber, Projektleitung und Sicherheitsverantwortung
- **Phasen und Sicherheits-Gates:** je Projekt frei festgelegte Gates mit Termin, Kriterium, Stand (offen, bestanden, bestanden mit Auflage, nicht bestanden), Auflage und Nachweis. Als Vorschlag stehen G0 Initiierung, G1 Anforderungen & Risiko, G2 Test & Freigabe und G3 Übergabe & Abschluss bereit
- **ISMS-Ampel:** die Seitenleiste zeigt, was in der aktuellen Phase noch fehlt – grün, gelb oder rot. Sie ist ein Hinweis, keine Sperre
- **Verknüpfungen (mass):** Maßnahmen – aus ihnen errechnet sich der Fortschritt als Durchschnitt (0 –100 %) –, dazu Risiken, Assets, Dokumente (Vorgaben) und Lieferanten
- **Excel-Export:** Projektliste mit Fortschrittsangaben als .xlsx
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er legt ein Projekt aus einer Idee oder einem hochgeladenen Projektauftrag an, macht den ISMS-Check, leitet Sicherheitsanforderungen ab, bewertet die Risiken, begleitet ein Gate-Review und den Abschluss und geht Ihre Projekte mit Handlungsbedarf durch. Gespeichert wird erst, was Sie bestätigen.

© 2012–2026 WolfInfoSec GmbH

14. Incidents (Vorfälle)

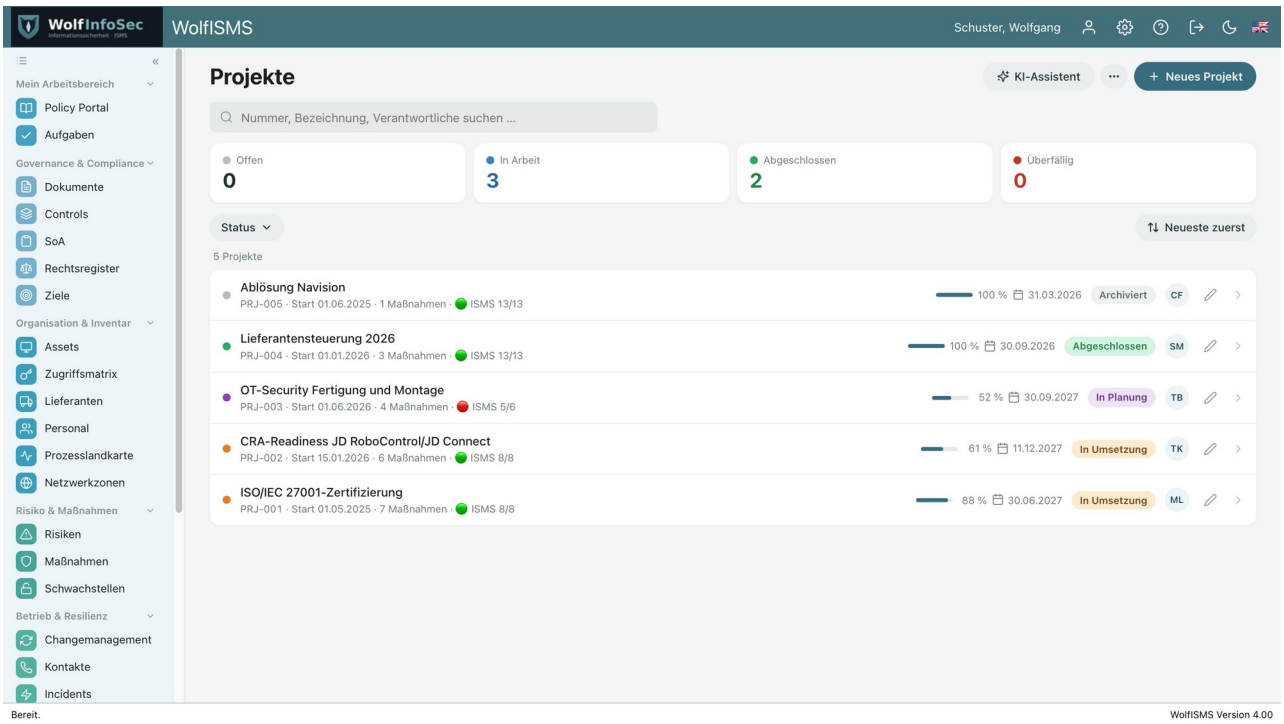
Beschreibung

Das Incident-Modul unterstützt den gesamten Vorfallmanagement-Prozess. Neben der Erfassung und Verfolgung werden Meldepflichten nach DSGVO, NIS-2 und CRA automatisch gekennzeichnet.

Funktionen

- **Kategorie-Kacheln**: Übersicht der Vorfälle nach Kategorie (z. B. Malware, Phishing, Datenabfluss); die Kategorien pflegt Ihr Administrator unter Administration → Kategorien
- **Meldepflicht-Badges**: Automatische Kennzeichnung meldepflichtiger Vorfälle nach DSGVO / NIS-2 / CRA
- **Vorfallnummer**: Automatischer Vorschlag im Format INC-YYYY-NNN
- **Eskalation**: Eskalationsstelle und Eskalationsdatum erfassbar
- **Ursachenanalyse**: Felder für Rootcause, Schwachstellen und Verbesserungsmaßnahmen
- **Verknüpfungen (incidents)**: Verlinkung mit Maßnahmen, Risiken, Assets und Lieferanten
- **Kritische Vorfälle**: Offene Vorfälle mit Priorität „Kritisch“ werden rot hervorgehoben
- **Excel-Export**: Vollständiger Incident-Export als .xlsx
- **Ticketsystem-Link**: Hat Ihr Administrator ein Ticketsystem hinterlegt, führt die Nummer in der Incident-Liste direkt zum zugehörigen Ticket
- **Charts**: Kreisdiagramme: Status, Kategorie, Typ
- **REST-API**: Vorfälle lassen sich von externen Systemen automatisiert anlegen und abfragen – siehe Kapitel 28
- **Kommentare**: Diskussionsfaden je Incident für die Abstimmung während der Bearbeitung
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er erfasst einen Vorfall mit Ihnen, prüft und führt zusammen, bewertet die Meldepflicht nach NIS-2, DSGVO und CRA, bereitet die Meldung einer Stufe vor und erfasst sie, erarbeitet Ursache und Lehren, schlägt Verknüpfungen vor und geht Ihre offenen Vorfälle durch – fällige Meldefristen zuerst. Melden tut der Assistent nie; das tun Sie im Portal der Behörde. Er ersetzt die frühere KI-Analyse in der Detailansicht. Gespeichert wird erst, was Sie bestätigen.

© 2012–2026 WolfInfoSec GmbH



Meldepflichten und Meldefristen

Ist an einem Vorfall DSGVO, NIS-2 oder CRA angehakt, zeigt die Detailansicht seit v3.90 den Abschnitt „Meldepflichten“: je Regelwerk die Meldestufen mit Frist und Stand, dazu Vorlagen für den Meldetext und die bereits abgegebenen Meldungen.

Regelwerk	Meldestufe	Frist
NIS-2 (§ 32 BSIG)	Erstmeldung (Frühwarnung)	24 Stunden nach Kenntnis
NIS-2 (§ 32 BSIG)	Meldung	72 Stunden nach Kenntnis
NIS-2 (§ 32 BSIG)	Zwischenmeldung	auf Ersuchen des BSI
NIS-2 (§ 32 BSIG)	Abschlussmeldung	ein Monat nach der 72-Stunden-Meldung
DSGVO	Meldung an die Aufsichtsbehörde (Art. 33)	72 Stunden nach Kenntnis
DSGVO	Benachrichtigung der Betroffenen (Art. 34)	unverzüglich, wenn voraussichtlich ein hohes Risiko besteht
CRA (Art. 14)	Frühwarnung / Meldung / Abschlussbericht	24 Stunden / 72 Stunden / ein Monat nach der Meldung

- **Bewertung**: Je Regelwerk erfassen Sie den Zeitpunkt der Kenntnis – mit Uhrzeit, denn die Fristen laufen in Stunden –, die Entscheidung „zu prüfen“, „meldepflichtig“ oder „nicht meldepflichtig“ und eine Begründung. Bei „nicht meldepflichtig“ ist sie Pflicht; Art. 33 Abs. 5 DSGVO verlangt, auch nicht gemeldete Verletzungen zu dokumentieren. Ohne Bewertung gilt der Erkennungstag 00:00 Uhr als Kenntniszeitpunkt
- **Stand je Stufe**: Restzeit bis zur Frist, „überfällig seit …“, „gemeldet“ – gegebenenfalls mit „verspätet um …“ –, „bei Bedarf“ für Stufen ohne feste Frist und „entfällt“, wenn der Vorfall als nicht meldepflichtig bewertet ist

© 2012–2026 WolfInfoSec GmbH

- **Meldevorlage**: enthält den vorgeschriebenen Inhalt der Stufe, vorbefüllt aus dem Vorfall – Organisation, Ansprechpartner, Beschreibung, betroffene Assets, Maßnahmen, das Aktenzeichen einer früheren Meldung. Offene Punkte sind mit […] markiert. Den Text kopieren Sie ins Meldeportal der Behörde
- **Meldung erfassen**: Zeitpunkt, Stelle, Aktenzeichen und den übermittelten Text festhalten. Die Felder „Meldung Datum“ und „Meldestelle“ des Vorfalls werden dabei nachgeführt
- **Überblick**: Die Startseite der Incidents zeigt eine Leiste mit den offenen und überfälligen Meldefristen; „Alle anzeigen“ führt zur Liste aller offenen Pflichtmeldungen, sortiert nach Frist. Archivierte Vorfälle zählen nicht mit
- **Aufgaben und Erinnerungsmail:** Seit v3.94 stehen offene und überfällige Meldefristen auch unter „Meine Aufgaben“ und in der Aufgaben-Erinnerungsmail – bei allen Besitzern des Vorfalls, bei Abwesenheit beim Vertreter. Ist eine Meldung erfasst oder der Vorfall als nicht meldepflichtig bewertet, verschwindet die Frist dort
- **Berechtigung**: Sehen kann den Abschnitt jeder mit Leserecht auf Incidents. Bewerten und Meldungen erfassen dürfen die Besitzer des Vorfalls und Master-Benutzer

Arbeitshilfe, keine Rechtsberatung
Ob ein Vorfall erheblich im Sinne von NIS-2 ist oder ein Risiko für die Betroffenen besteht, entscheiden Sie in der Bewertung. Die Fristen berechnet WolfISMS aus Ihren Angaben.

© 2012–2026 WolfInfoSec GmbH

15. Schwachstellen

Beschreibung

Das Schwachstellenmodul führt die technischen Schwachstellen der Organisation an einer Stelle zusammen – gleich ob sie aus einem Schwachstellenscan, einem Penetrationstest, einer Herstellerwarnung oder einer internen Meldung stammen. Jeder Eintrag trägt eine fortlaufende Nummer im Format WEA-NNNNN, einen Titel, eine Beschreibung, einen Score, eine Quelle und einen Status. Der Schweregrad wird nicht eingetragen, sondern aus dem Score abgeleitet.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet. Dasselbe gilt für den KI-Abgleich gegen bekannte Schwachstellen.

Der übliche Weg führt von der Meldung über die Bewertung zur Behandlung: Sie erfassen den Fund, verknüpfen ihn mit den betroffenen Assets und legen aus der Schwachstelle heraus eine Maßnahme an, die beides in einem Schritt verbindet.

Funktionen

- **Kennzahlen**: sechs Kacheln über der Liste zeigen Gesamtzahl, offene Schwachstellen und die offenen Funde je Schweregrad (kritisch, hoch, mittel, niedrig)
- **Score und Schweregrad**: der CVSS-Wert reicht von 0,0 bis 10,0. Kritisch ab 9,0, hoch ab 7,0, mittel ab 4,0, darunter niedrig; 0,0 ist eine reine Information. Ohne Score bleibt der Eintrag als „ohne Score" gekennzeichnet
- **Status**: Neu, in Bewertung, Bestätigt, in Behandlung, Risiko akzeptiert, Behoben und Verworfen/Fehlalarm. Die letzten drei gelten als erledigt, alle übrigen als offen
- **Behebungsfrist**: Je Schweregrad legt Ihr Administrator fest, wie viele Tage eine Schwachstelle offen bleiben darf (Vorgabe: kritisch 7, hoch 30, mittel 90, niedrig 180 Tage, ohne Score 30). Liste und Detailansicht zeigen die Fälligkeit ab dem Erfassungsdatum, die Kachel „Überfällig“ zählt die überschrittenen. Ändert sich der Score, gilt sofort die Frist des neuen Schweregrads
- **Quelle**: Schwachstellenscan, Penetrationstest, Hersteller-Advisory, CERT/BSI-Warnung, Interne Meldung, Audit, Bug Bounty oder Sonstige – damit erkennbar bleibt, woher ein Fund stammt
- **Filter und Suche**: Auswahl nach Status, Quelle und Schweregrad, dazu eine Freitextsuche über Nummer, Titel und Beschreibung. Jede Spaltenüberschrift sortiert die Liste
- **Besitzer**: jede Schwachstelle hat einen oder mehrere Verantwortliche. Ändern und Löschen bleiben ihnen und den Masterusern vorbehalten – wie in den übrigen Modulen
- **Verknüpfungen**: Assets, Incidents, Risiken und Maßnahmen werden in der Detailansicht über „Verwalten" zugeordnet. Die Seitenleiste verlinkt jeden verknüpften Eintrag; bei Assets steht die Version dabei, damit gleichnamige Systeme unterscheidbar bleiben
- **Maßnahme anlegen**: aus der Liste und aus der Detailansicht heraus lässt sich eine Maßnahme erzeugen, die sofort mit der Schwachstelle verknüpft ist. Dafür wird zusätzlich das Recht Maßnahmen benötigt
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er erfasst Schwachstellen – frei, aus einer CVE-Nummer oder einem Advisory –, übernimmt Scan- und Pentestberichte, prüft die Versionen Ihrer Assets gegen bekannte CVEs (früher eine eigene Schaltfläche), bewertet neue Funde nacheinander (Triage), geht fällige durch, belegt die Behebung und schreibt einen Lagebericht. Gespeichert wird erst, was Sie bestätigen.

© 2012–2026 WolfInfoSec GmbH

- **Nummernvorschlag**: das Formular schlägt die nächste freie Nummer vor; sie lässt sich überschreiben, etwa um die Kennung des meldenden Systems zu übernehmen
- **Zweisprachigkeit**: Titel und Beschreibung werden in der Sprache gespeichert, in der Sie die Oberfläche bedienen – die englische Fassung steht in eigenen Feldern neben der deutschen
- **REST-API**: ein Schwachstellenscanner legt seine Funde automatisiert an und holt sich den Behandlungsstand später zurück – siehe Kapitel 28
- **Excel-Export**: Schaltfläche „Excel“ in der Filterleiste, übernimmt die gesetzten Filter. Das erste Blatt „Patchstand“ zählt die offenen Schwachstellen je Schweregrad, dazu wie viele länger als 30 bzw. 90 Tage offen sind, die älteste und das durchschnittliche Alter – gerechnet ab der Erfassung. Das zweite Blatt enthält die Liste mit den betroffenen Assets und dem Status der verknüpften Maßnahmen

© 2012–2026 WolfInfoSec GmbH

16. Audit

Beschreibung

Das Audit-Modul plant interne und externe Audits und verfolgt ihre Feststellungen bis zur erledigten Maßnahme. Ein Audit ist ein Termin mit Zeitraum, Auditor, Framework-Bezug und Status; darunter hängen die Abweichungen – die Feststellungen des Auditors – mit Typ, Verantwortlichem und Frist.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet.

Das Modul ist mit v3.72 neu entstanden. Bis v3.71 war es ein Selbstcheck mit Fragenkatalogen zu ISO 27001, NIS-2, VdS, Cyber Essentials, DSGVO und TISAX. Diese Kataloge sind entfallen: Wie weit ein Framework umgesetzt ist, steht im Controls-Modul – je Anforderung mit Umsetzungsstatus, Kapitelübersicht und Konformitätsbericht. Die Antworten der früheren Fragenkataloge bleiben in der Datenbank erhalten, sind in der Oberfläche aber nicht mehr sichtbar.

Aufbau

Das Modul hat zwei Reiter. „Audits" führt die Termine, „Alle Abweichungen" zeigt die Feststellungen aus allen Audits in einer gemeinsamen Liste.

Feld eines Audits	Bedeutung
Nummer	AUD-00001, AUD-00002 … Beim Speichern wird die nächste freie Nummer vergeben; sie lässt sich überschreiben
Bezeichnung	Pflichtangabe, z. B. „Internes Audit ISMS 2026" oder „Überwachungsaudit ISO 27001"
Zeitraum	Von (Pflichtangabe) und Bis. Ein Enddatum vor dem Beginn wird abgewiesen
Status	geplant, fest oder durchgeführt
Art	intern, extern oder Gap-Assessment
Auditor	Auditor oder Zertifizierungsstelle (Freitext)
Framework	Bezugsnorm des Audits, z. B. ISO/IEC 27001 (Freitext)
Beschreibung	Umfang, Ziel und Ablauf des Audits

Feld einer Abweichung	Bedeutung
Nummer	ABW-00001, ABW-00002 … wie beim Audit vergeben und überschreibbar
Feststellung	Bezeichnung und Beschreibung dessen, was der Auditor festgestellt hat
Typ	Empfehlung, Nebenabweichung oder Hauptabweichung
Status	offen, in Arbeit, umgesetzt oder nicht umgesetzt

© 2012–2026 WolfInfoSec GmbH

Feld einer Abweichung	Bedeutung
Verantwortlich	Benutzer, der die Feststellung abarbeitet
Fällig bis	Frist. Ist sie überschritten und die Feststellung noch nicht umgesetzt, steht das Datum rot
Framework / Kapitel	Framework-Bezug und die verletzte Anforderung, z. B. ISO/IEC 27001 und A.8.16
Maßnahmen	Die verknüpften Maßnahmen aus dem Maßnahmenmodul

Jede Abweichung gehört zu genau einem Audit und wird aus dessen Detailansicht heraus angelegt.

Prüfliste und Gap-Assessment

Ein Audit lässt sich gegen ein Framework führen. Dazu übernehmen Sie die Anforderungen eines Frameworks – ISO/IEC 27001, NIS2 oder jede andere, die im Controls-Modul gepflegt ist – als Prüfliste in das Audit und bewerten sie dort Punkt für Punkt. Wollen Sie nur wissen, wo Ihr Unternehmen gegenüber eines Frameworks steht, legen Sie ein Audit der Art „Gap-Assessment" an: Die Prüfliste ist dieselbe, nur der Anlass ist ein anderer.

Die Schaltfläche „Prüfliste" im Auditdetail führt Sie hin. Beim ersten Mal wählen Sie das Framework und, wenn Sie mögen, einzelne Kapitel; ohne Auswahl kommt das vollständige Framework. In der Voreinstellung werden nur die Anforderungen übernommen, die im Controls-Modul als anwendbar gekennzeichnet sind. Später ergänzen Sie weitere Kapitel jederzeit – bereits vergebene Bewertungen bleiben dabei stehen.

Jeder Prüfpunkt bekommt eine Bewertung:

Bewertung	Bedeutung
erfüllt	Die Anforderung ist umgesetzt und nachgewiesen
weitgehend erfüllt	Umgesetzt, mit kleineren Lücken
teilweise erfüllt	Im Ansatz vorhanden, Wesentliches fehlt
nicht erfüllt	Nicht umgesetzt – hier liegt eine Lücke
nicht anwendbar	Für Ihr Unternehmen nicht einschlägig; der Punkt geht nicht in die Wertung ein
offen	Noch nicht geprüft

Zu jedem Punkt gehören zwei Textfelder: die Feststellung – was Sie vorgefunden haben – und der Nachweis, also worauf sich Ihr Urteil stützt (Dokument, Aufzeichnung, Interview). Gespeichert wird die ganze angezeigte Liste auf einmal.

Aus den Bewertungen rechnet WolfISMS den Erfüllungsgrad: erfüllt zählt voll, weitgehend erfüllt zu drei Vierteln, teilweise erfüllt zur Hälfte, nicht erfüllt gar nicht. Offene und nicht anwendbare Punkte bleiben außen vor, damit eine halb ausgefüllte Liste kein falsches Bild zeichnet. Sie sehen den Wert oben in der Prüfliste, kapitelweise im Auditdetail und als Spalte in der Auditübersicht.

© 2012–2026 WolfInfoSec GmbH

Prüfliste und Controls-Modul bleiben getrennt.
Die Bewertung im Audit ändert den Umsetzungsstatus im Controls-Modul nicht. Das ist Absicht: Im Controls-Modul steht, wie weit Ihr ISMS ist, in der Prüfliste steht, was ein bestimmtes Audit an einem bestimmten Tag festgestellt hat. Auch der Wortlaut der Anforderung wird beim Aufbau der Prüfliste kopiert – ein Auditbericht muss zeigen, wogegen geprüft wurde, selbst wenn die Anforderung später geändert wird.

Wo Sie eine Lücke gefunden haben, machen Sie daraus mit der Schaltfläche „Anlegen" in der Spalte Abweichung eine Feststellung. Framework-Punkt, Anforderung, Ihre Feststellung und der Nachweis stehen darin bereits, der Typ wird aus der Bewertung vorgeschlagen – nicht erfüllt ergibt eine Hauptabweichung, teilweise erfüllt eine Nebenabweichung. Ergänzen Sie noch Verantwortlichen und Frist, und die Abweichung läuft wie jede andere weiter, bis zur Maßnahme. In der Prüfliste steht ab dann die Nummer der Abweichung neben dem Prüfpunkt.

GAP-Analyse durchführen: Für ein Gap-Assessment mit Prüfliste steht in der Prüfliste und in der Detailansicht die Schaltfläche „GAP-Analyse durchführen“. Sie führt Sie Schritt für Schritt durch die Prüfliste: Jedes Kapitel ist ein Schritt, jede Anforderung eine Seite mit Bewertung, Feststellung und Nachweis. Mit „Speichern & weiter“ geht es zur nächsten Anforderung; einzelne Anforderungen oder ganze Kapitel lassen sich überspringen, und „Speichern & später fortsetzen“ merkt sich die Stelle. Die Übersicht zeigt je Kapitel den Stand und den Erfüllungsgrad; „Fortschritt zurücksetzen“ beginnt von vorn, ohne Bewertungen und Feststellungen zu löschen. Gespeichert wird in dieselben Felder wie in der Prüfliste.

KI-Assistent (ab Essentials): Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er plant ein Audit samt Prüfkatalog und Prüffragen – die Prüffragen gibt es jetzt für alle Audit-Arten –, schlägt Bewertungen für Prüfpunkte vor, bereitet Abweichungen auf, entwirft den Auditbericht, plant das Auditprogramm, verfolgt offene Feststellungen nach und prüft die Audit-Bereitschaft. Bewertungen bleiben Vorschläge, der Auditor entscheidet; Korrekturmaßnahmen entstehen im Maßnahmen-Assistenten. Gespeichert wird erst, was Sie bestätigen.

Funktionen

- **Kennzahlen**: Kacheln über der Liste – Audits gesamt und je Status, offene Abweichungen, offene Hauptabweichungen und überfällige Feststellungen. Die letzten beiden Kacheln färben sich, sobald sie nicht auf null stehen
- **Filter und Suche**: Nach Status und Art filtern, Freitextsuche über Nummer, Bezeichnung und Auditor. Jede Spalte der Tabelle lässt sich auf- und absteigend sortieren
- **Auditdetail**: Zeigt die Kopfdaten, die Abweichungen des Audits, alle daraus abgeleiteten Maßnahmen und darunter die Anhänge und Links
- **Prüfliste**: Die Anforderungen eines Frameworks als Prüfpunkte im Audit, fünfstufig bewertet, mit Feststellung und Nachweis je Punkt. Daraus errechnet sich der Erfüllungsgrad – siehe den Abschnitt Prüfliste und Gap-Assessment
- **Abweichung aus einem Prüfpunkt**: Aus einem nicht oder nur teilweise erfüllten Prüfpunkt wird auf Knopfdruck eine Abweichung mit Framework-Bezug, Feststellung und vorgeschlagenem Typ
- **Alle Abweichungen**: Der zweite Reiter listet die Feststellungen aller Audits mit eigenen Kennzahlen und Filtern nach Typ, Status – auch „nur offene" – und Freitext
- **Maßnahmen verknüpfen**: Eine Abweichung wird mit vorhandenen Maßnahmen verknüpft. Kopiert wird nichts: die Maßnahme bleibt im Maßnahmenmodul und wird dort wie jede andere verfolgt
- **Maßnahme anlegen**: Aus der Abweichung heraus entsteht eine neue Maßnahme, die sofort verknüpft ist. Dafür wird zusätzlich das Bearbeitungsrecht für Maßnahmen benötigt

© 2012–2026 WolfInfoSec GmbH

- **Risiko anlegen:** Seit v3.95 entsteht aus einer Abweichung auch ein Risiko – über „ Risiko anlegen“ in ihrer Detailansicht oder den Schnellknopf ⚠ in der Abweichungsliste. Das Formular ist vorausgefüllt: Name aus der Feststellung, Besitzer ist der Verantwortliche, die Beschreibung nennt Feststellung, Audit und Framework, als Behandlung ist „Reduzieren“ gewählt, Wahrscheinlichkeit und Auswirkung sind nach dem Typ vorgeschlagen (Hauptabweichung 4 × 4, Nebenabweichung 3 × 3, Empfehlung 2 × 2). Das Risiko ist sofort mit der Abweichung verknüpft und übernimmt deren Maßnahmen; eine später an der Abweichung angelegte Maßnahme kommt auch an ihre Risiken, soweit Sie diese ändern dürfen. Vorhandene Risiken verknüpfen Sie über „Verwalten“ im Abschnitt Risiken der Seitenleiste; am Risiko erscheint die Abweichung als Rückverweis „Audit-Abweichungen“. Dafür brauchen Sie das Bearbeitungsrecht für Audit und für Risiken
- **Anhänge**: PDF-Dateien am Audit – Auditplan, Auditbericht, Nachweise. Es gelten dieselben Regeln wie überall: echte PDF-Dateien bis 16 MB
- **Links**: Verweise aus dem Audit heraus, z. B. auf das Zertifikat, ein Ticket oder den Bericht im DMS
- **Excel-Export**: Drei Tabellenblätter – Audits, Abweichungen und Prüflisten – mit Nummern, Zeiträumen, Fristen, Verantwortlichen, den verknüpften Maßnahmen und Risiken und den Bewertungen. Die Prüfliste eines einzelnen Audits lässt sich zusätzlich aus der Prüfliste heraus ausgeben
- **Auditbericht (PDF)**: in der Detailansicht eines Audits, seit v3.90. Enthält Kopfdaten, eine Zusammenfassung mit Erfüllungsgrad und der Zahl der Abweichungen, Gegenstand und Umfang, das Prüfergebnis je Kapitel mit allen Prüfpunkten, die Abweichungen mit Ursachenanalyse, Übertragbarkeit und Wirksamkeitsprüfung, die Korrekturmaßnahmen, die Anhänge als mitgeltende Unterlagen und einen Freigabeblock. „Kurzbericht“ lässt die einzelnen Prüfpunkte weg. Ist das Audit noch nicht durchgeführt, weist der Bericht sich als Zwischenstand aus

Hinweise

Das Modul setzt das Recht Audit voraus: ab Stufe 1 lesen, ab Stufe 2 bearbeiten. Dasselbe Recht steuert die Managementbewertung.

Wird ein Audit gelöscht, verschwinden auch seine Abweichungen, seine Prüfliste, Anhänge und Links; die verknüpften Maßnahmen bleiben bestehen. Die Sicherheitsabfrage weist darauf hin, die Meldung danach nennt die Anzahl der mitgelöschten Feststellungen.

© 2012–2026 WolfInfoSec GmbH

17. Managementbewertung

Beschreibung

Die Managementbewertung ist die Bewertung des ISMS durch die oberste Leitung nach ISO/IEC 27001 Kapitel 9.3. Das Modul führt die dafür geforderten Eingaben an einer Stelle zusammen: Was Sie selbst beschreiben, erfassen Sie als Text; was das System bereits weiß – Zielerreichung, Risikolage und Vorfälle – wird beim Öffnen automatisch aus den anderen Modulen zusammengestellt.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite. Fehlt das Modul im Menü, hat der Administrator es unter Administration → Module abgeschaltet – die erfassten Daten bleiben dabei erhalten und sind nach dem Wiedereinschalten unverändert da.

Aufbau einer Bewertung

Jede Bewertung hat einen Betrachtungszeitraum (von/bis). Beim Anlegen wird das Enddatum automatisch auf ein Jahr nach dem Startdatum vorbelegt. Die Bewertung enthält folgende Abschnitte:

- Status von Maßnahmen aus früheren Managementbewertungen
- Änderungen bei externen und internen Themen, die für das ISMS relevant sind
- Änderungen bei den Bedürfnissen und Erwartungen interessierter Parteien
- Veränderungen an Geschäftsfeldern und Organisation, die das ISMS betreffen
- Nichtkonformitäten und Korrekturmaßnahmen – dazu seit v3.90 die Live-Liste der Haupt- und Nebenabweichungen aus dem Audit-Modul: alle offenen sowie die umgesetzten aus Audits des Zeitraums, mit Frist, Status und Wirksamkeitsprüfung
- Ergebnisse aus Überwachung und Messung
- Ergebnisse interner Audits – dazu seit v3.90 die Live-Liste der Audits im Betrachtungszeitraum mit Erfüllungsgrad und Zahl der Abweichungen
- Erreichung der Informationssicherheitsziele – wird als Live-Liste der KPIs aus dem Modul Ziele eingeblendet, mit den Werten des Betrachtungszeitraums
- Ergebnisse der Risikobeurteilung und Status des Behandlungsplans – Live-Liste der offenen Risiken mit Stufe „kritisch“ und „hoch“
- Auswertung der Vorfälle im Betrachtungszeitraum
- Rückmeldungen von interessierten Parteien
- Chancen zur fortlaufenden Verbesserung
- **Beschlossene Maßnahmen** – die mit der Bewertung verknüpften Einträge aus dem Modul Maßnahmen (Ergebnisse der Bewertung nach Kapitel 9.3.3)

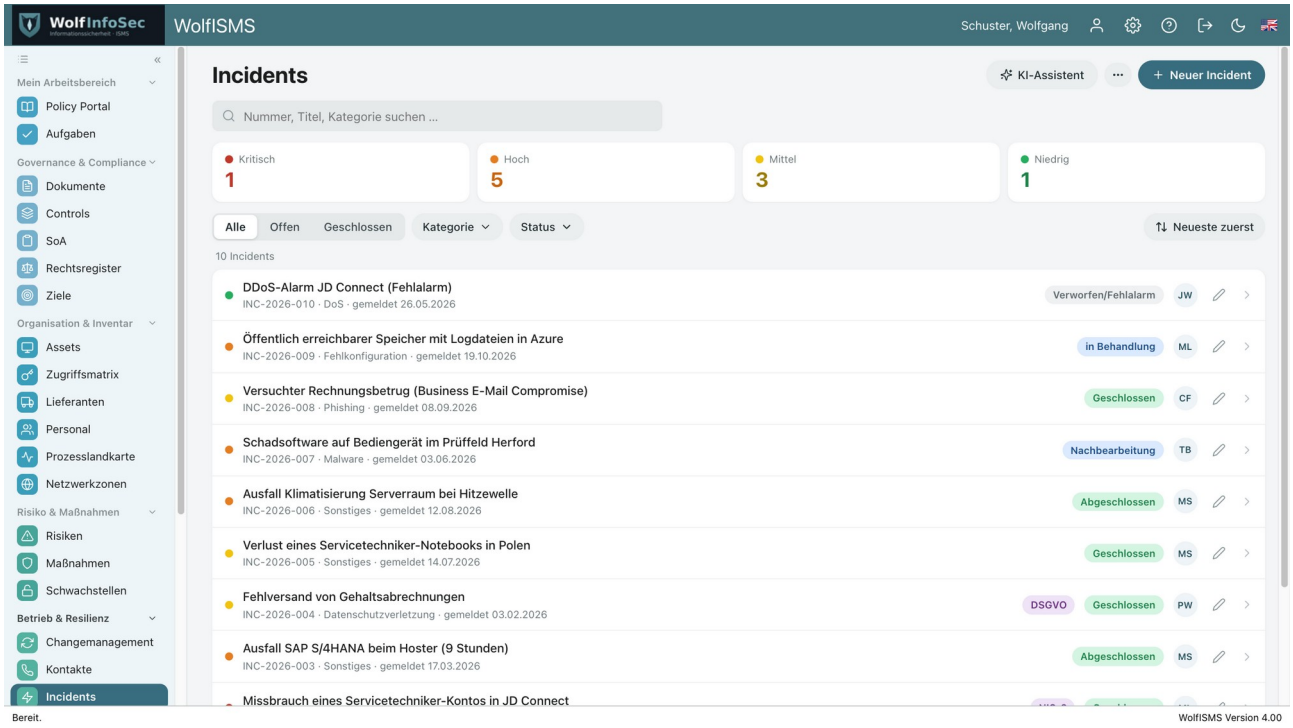
Funktionen

- **Übersicht**: Liste aller Bewertungen mit Titel, Zeitraum, Ersteller und Änderungsdatum
- **Bearbeiten**: Alle Textabschnitte werden im Richtext-Editor gepflegt
- **Live-Abschnitte**: KPI-, Risiko-, Incident- und Audit-Abschnitte werden bewusst nicht mitgespeichert, sondern bei jedem Öffnen neu berechnet – die Bewertung zeigt damit immer den aktuellen Stand
- **PDF-Export**: Erzeugt das vollständige Bewertungsdokument. Ist im System ein PDF-Briefpapier hinterlegt, wird es als Kopf- und Fußzeile verwendet
- **PowerPoint-Export**: Erzeugt eine Präsentation der Bewertung für die Leitungssitzung

© 2012–2026 WolfInfoSec GmbH

- **Beschlossene Maßnahmen**: Der Abschnitt zeigt die verknüpften Maßnahmen mit Nummer, Bezeichnung, Status, Priorität, Enddatum, Fortschritt und Verantwortlichem, dazu die Summe aus Aufwand und Kosten. Über „Verknüpfungen verwalten" werden vorhandene Maßnahmen zugeordnet oder gelöst; „Neue Maßnahme" legt eine Maßnahme an, die sofort verknüpft ist. Gepflegt wird sie anschließend im Modul Maßnahmen, dort liegen auch Aufwand, Kosten, Anhänge und die übrigen Verknüpfungen. Der Abschnitt erscheint auch im PDF- und im PowerPoint-Export
- **Zweisprachigkeit**: Anzeige in Deutsch oder Englisch je nach Benutzereinstellung

Benutzerrecht: audit (0 = kein Zugriff, 1 = Lesen, 2 = Bearbeiten) – URL: /managementreview



Hinweise

Damit die Abschnitte „Erreichung der Informationssicherheitsziele“ und „Ergebnisse der Risikobeurteilung“ gefüllt sind, müssen im Modul Ziele KPIs mit Werten im Betrachtungszeitraum gepflegt sein und im Risikomodul offene Risiken der Stufen kritisch oder hoch vorliegen. Andernfalls bleiben die Abschnitte leer – das ist kein Fehler, sondern spiegelt den Datenstand wider.

© 2012–2026 WolfInfoSec GmbH

18. Aufgaben

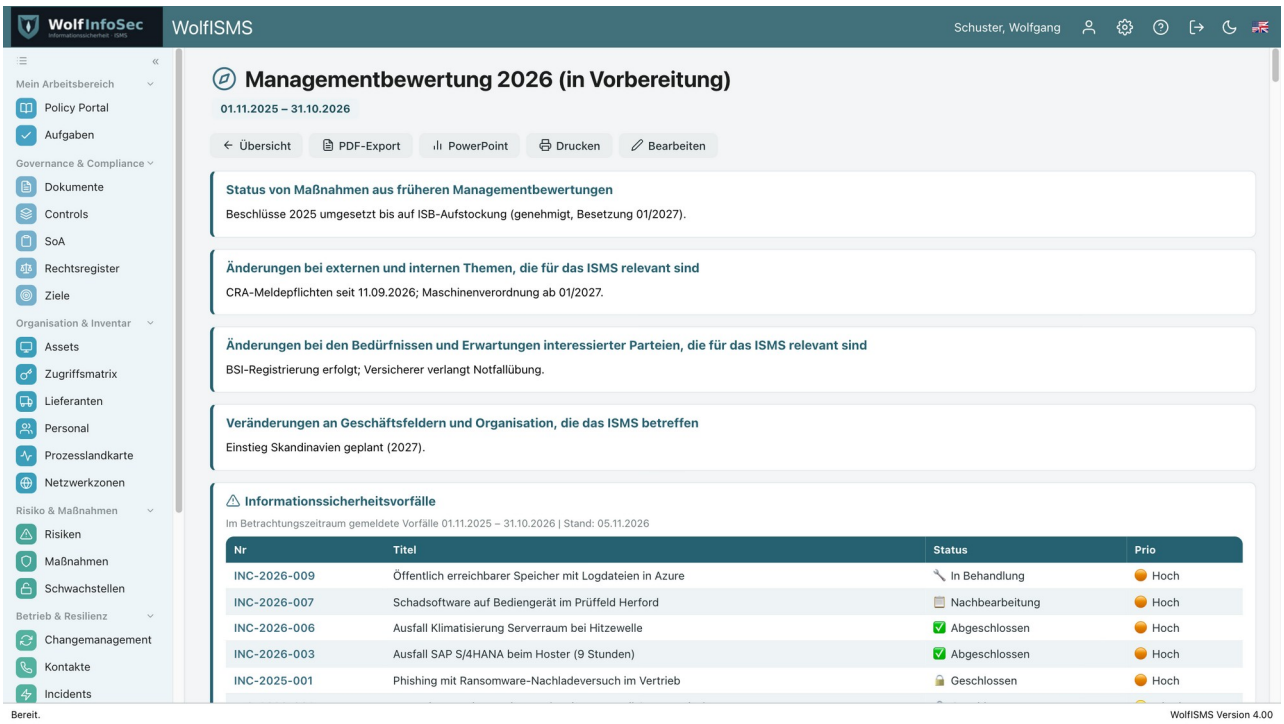
Beschreibung

Das Aufgaben-Modul führt alle offenen Aufgaben des angemeldeten Benutzers aus allen anderen Modulen an einem zentralen Ort zusammen. Benutzer mit master-Recht sehen auch die Aufgaben aller anderen Benutzer.

Funktionen

- **Zeitraum-Filter**: Heute / 7 Tage / 30 Tage / 90 Tage / Alle
- **Mein / Alle (master)**: Umschalten zwischen eigenen Aufgaben und systemweiter Ansicht
- **Offene Maßnahmen**: Maßnahmen mit Enddatum innerhalb des gewählten Zeitraums
- **Reviews**: Fällige Reviews aus allen Modulen: Maßnahmen, Assets, Dokumente, Risiken, Lieferanten
- **Dokument-Workflows**: Dokumente mit fälliger Prüfung oder ausstehender Freigabe
- **Changes**: geplante Zeitfenster, offene Stimmen im Freigabegremium und fällige Nachbetrachtungen aus dem Changemanagement
- **Meldefristen:** offene und überfällige Pflichtmeldungen zu Sicherheitsvorfällen (NIS-2, DSGVO, CRA) in einer eigenen roten Sektion ganz oben, mit Uhrzeit der Frist, Restzeit („noch 44 Std.“ bzw. „seit 3 Std. überfällig“) und einem Link zur Meldevorlage; dazu eine eigene Kachel. Sichtbar mit Leserecht auf Incidents. Die Erinnerungsmail geht einmal am Tag hinaus und ersetzt bei 24-Stunden-Fristen nicht den Blick auf die Seite
- **Offene Lesebestätigungen**: Richtlinien, die für Ihre Rolle Pflichtlektüre sind und die Sie im Policy Portal noch nicht als gelesen bestätigt haben. Dokumente ohne Lesepflicht erscheinen hier nicht – und wer keiner Rolle angehört, bekommt auch keine Erinnerungsmail dazu
- **Dringlichkeits-Badges**: Kennzeichnung nach Fälligkeitsstufe (heute / diese Woche / überfällig)
- **Überfällige Einträge**: Vergangene Fälligkeitstermine werden rot hervorgehoben
- **Bereichs-Tags**: Farbige Tags zeigen, aus welchem Modul die Aufgabe stammt

© 2012–2026 WolfInfoSec GmbH



Hinweise

Das Aufgaben-Modul ist schreibgeschützt. Aufgaben werden in den jeweiligen Modulen bearbeitet. Zusätzlich versendet das System eine Erinnerungs-E-Mail an fällige Aufgaben; Zeitpunkt und Rhythmus legt Ihr Administrator fest.

Abwesenheit und Vertretung

Vor dem Urlaub tragen Sie auf Ihrer Kontoseite unter „Abwesenheit pflegen“ den Zeitraum und einen Vertreter ein. Während dieser Zeit sieht der Vertreter Ihre Aufgaben zusätzlich unter „Meine Aufgaben“ – mit dem Hinweis, für wen – und bekommt Ihre Erinnerungsmails. Wer für die Datensätze verantwortlich ist, ändert sich dabei nicht, und nach dem Ende der Abwesenheit fällt alles von allein zurück.

- **Nur mit Vertreter**: Ein Zeitraum ohne Vertreter lässt sich nicht speichern – sonst bekäme niemand die Aufgaben. Für keine Abwesenheit lassen Sie alle drei Felder leer.
- **Lesebestätigungen**: bleiben bei Ihnen. Eine Richtlinie kann niemand stellvertretend als gelesen bestätigen.
- **Vertreter ebenfalls abwesend**: Dann gehen die Aufgaben an dessen Vertreter weiter.
- **Für andere**: Administratoren können die Abwesenheit eines Kollegen aus der Benutzerverwaltung heraus eintragen, etwa bei einer Krankmeldung.

© 2012–2026 WolfInfoSec GmbH

19. Operational Plan (Wiederkehrende Aufgaben)

Beschreibung

Das Modul Operational Plan verwaltet wiederkehrende Pflichtaufgaben (z. B. jährliche Managementbewertung, regelmäßiger Backup-Test, quartalsweise Zutrittsprüfung) als Fristenkalender mit lückenloser Nachweiskette.

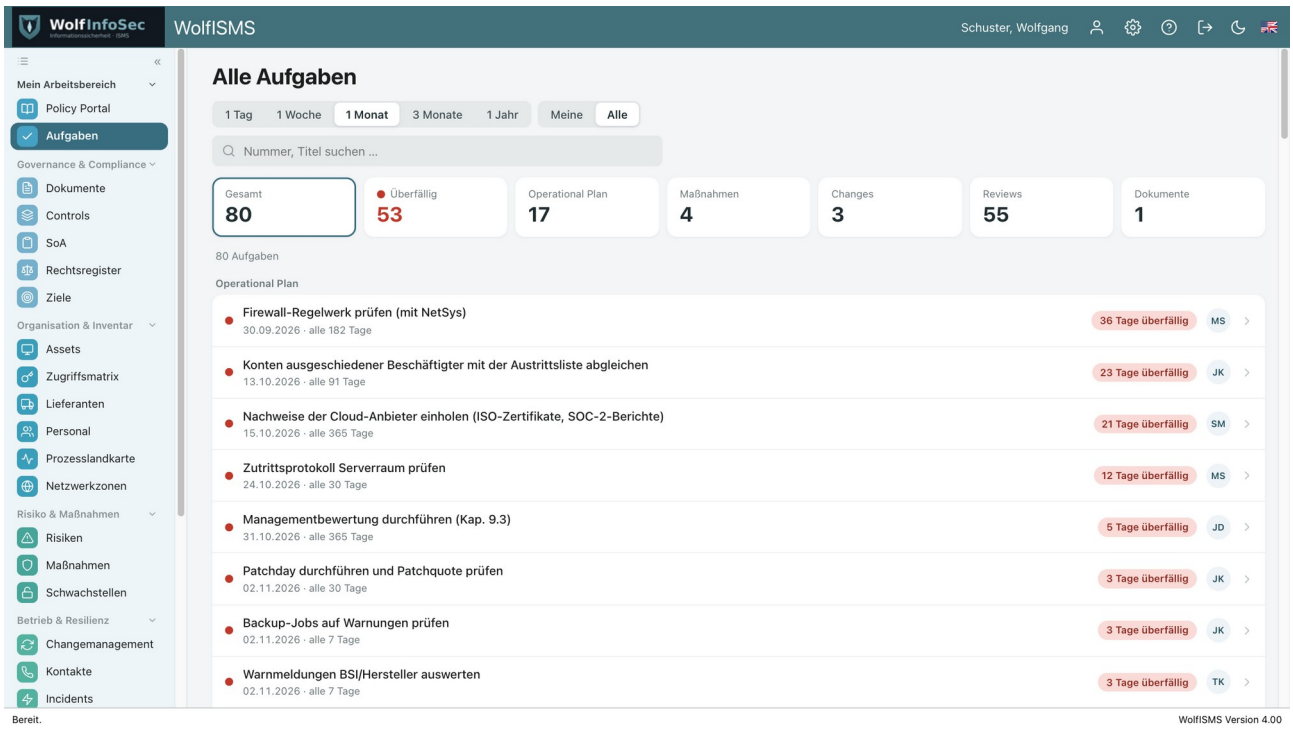
Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite. Fehlt das Modul im Menü, hat der Administrator es unter Administration → Module abgeschaltet – die erfassten Daten bleiben dabei erhalten und sind nach dem Wiedereinschalten unverändert da. Auch die Erinnerungsmails führen dann keine Operational-Plan-Termine mehr auf.

Funktionen

- **Aufgabenliste**: Übersicht aller offenen wiederkehrenden Aufgaben mit nächstem Fälligkeitsdatum, Verantwortlichem und Frequenz
- **Dringlichkeits-Badges**: Farbliche Kennzeichnung nach Fälligkeit (überfällig / heute fällig / in 7 Tagen / in 30 Tagen / im Zeitplan)
- **Status und Erledigt**: Jede offene Instanz hat seit v4.00 einen Status – offen, in Bearbeitung, erledigt. Erst „erledigt“ archiviert die Instanz unveränderlich als Nachweis und legt die nächste mit dem neuen Fälligkeitsdatum an (Datum + Frequenz in Tagen; bei stark überfälligen Aufgaben ab heute gerechnet)
- **Historie / Nachweiskette**: Alle Instanzen einer wiederkehrenden Aufgabe teilen eine Ketten-ID; darüber lässt sich die vollständige Erledigungshistorie als Nachweis einsehen
- **Mein / Alle (master)**: Master-Benutzer können zwischen eigenen Aufgaben und der systemweiten Ansicht umschalten
- **Löschen (master)**: Nur Master-Benutzer können eine offene Instanz löschen; bereits erledigte Nachweise bleiben davon unberührt
- **Verknüpfter Link**: Optionales Feld für einen Link zu einer externen Anleitung oder einem Formular

Benutzerrecht: Aufruf für alle angemeldeten Benutzer möglich (eigene Aufgaben); Menüeintrag, systemweite Ansicht und Löschen nur mit master-Berechtigung – URL: /op_plan

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
Mein Arbeitsbereich
Policy Portal
Aufgaben
Governance & Compliance
Dokumente
Controls
SoA
Rechtsregister
Ziele
Organisation & Inventar
Assets
Zugriffsmatrix
Lieferanten
Personal
Prozesslandkarte
Netzwerkzonen
Risiko & Maßnahmen
Risiken
Maßnahmen
Schwachstellen
Betrieb & Resilienz
Changemanagement
Kontakte
Incidents
Alle Aufgaben
1 Tag
1 Woche
1 Monat
3 Monate
1 Jahr
Meine
Alle
Nummer, Titel suchen ...
Gesamt
80
Überfällig
53
Operational Plan
17
Maßnahmen
4
Changes
3
Reviews
55
Dokumente
1
80 Aufgaben
Operational Plan
Firewall-Regelwerk prüfen (mit NetSys)
30.09.2026 · alle 182 Tage
36 Tage überfällig
MS
Konten ausgeschiedener Beschäftigter mit der Austrittsliste abgleichen
13.10.2026 · alle 91 Tage
23 Tage überfällig
JK
Nachweise der Cloud-Anbieter einholen (ISO-Zertifikate, SOC-2-Berichte)
15.10.2026 · alle 365 Tage
21 Tage überfällig
SM
Zutrittsprotokoll Serverraum prüfen
24.10.2026 · alle 30 Tage
12 Tage überfällig
MS
Managementbewertung durchführen (Kap. 9.3)
31.10.2026 · alle 365 Tage
5 Tage überfällig
JD
Patchday durchführen und Patchquote prüfen
02.11.2026 · alle 30 Tage
3 Tage überfällig
JK
Backup-Jobs auf Warnungen prüfen
02.11.2026 · alle 7 Tage
3 Tage überfällig
JK
Warnmeldungen BSI/Hersteller auswerten
02.11.2026 · alle 7 Tage
3 Tage überfällig
TK
Bereit.
WolfISMS Version 4.00

20. Dokumente

Beschreibung

Das Dokumentenmodul verwaltet alle ISMS-Dokumente mit vollständigem Freigabe-Workflow. Jede Änderung wird als eigene Version festgehalten, so dass alle Fassungen abrufbar bleiben und eine frühere sich zurückholen lässt; dazu kommen Mehrsprachigkeit (DE/EN), Schreibschutz und die Verknüpfung mit BPMN-Prozessdiagrammen. Ein vorhandenes Word-Dokument lässt sich übernehmen, statt es abzutippen. Der Dokumenttyp für Prozessdokumente heisst „Prozesse"; er hiess früher „Verfahren" und wurde bei der Umstellung automatisch umbenannt.

Versionen und Versionsverlauf

Jede Änderung an einem Dokument wird als eigene Fassung festgehalten. Speichern überschreibt den bisherigen Stand nicht, sondern legt ihn als neue Version daneben – die Fassung davor bleibt vollständig erhalten und ist jederzeit wieder aufrufbar. Die Versionsnummer besteht aus zwei Teilen: die vordere zählt bei jeder Freigabe hoch, die hintere bei jedem Speichern dazwischen. Aus einer freigegebenen v2.0 wird beim Bearbeiten also v2.1, v2.2 … und mit der nächsten Freigabe v3.0.

Nebeneinander gelten dabei zwei Fassungen:

- **Die freigegebene Version** ist die, die zählt. Auf sie zeigen die Verknüpfungen aus allen anderen Bereichen – Controls, Risiken, Prozesslandkarte, Netzwerkzonen und verknüpfte Dokumente –, sie erscheint im Policy Portal und sie löst die Lesebestätigung aus.
- **Der Arbeitsstand** ist die neueste Fassung. An ihr wird gearbeitet, geprüft und freigegeben. Solange sie nicht freigegeben ist, ändert sich für die übrigen Bereiche nichts – niemand arbeitet versehentlich gegen einen Entwurf.

In der Dokumentenliste stehen beide in einer Zeile: oben die Nummer der geltenden Fassung, darunter der laufende Arbeitsstand als Link. Die Detailansicht sagt Ihnen mit einer Leiste über dem Dokument, welche der beiden Sie gerade vor sich haben, und führt mit einem Klick zur anderen.

In der rechten Seitenspalte steht unter „Versionen" der vollständige Verlauf: jede Fassung mit Nummer, Status, Bearbeiter und Datum, jede mit einem Klick zu öffnen. Die geltende Fassung ist als „freigegeben" gekennzeichnet – oder als „aktuell", solange das Dokument die Freigabe noch nie durchlaufen hat –, der laufende Arbeitsstand als „neueste". Das Änderungsprotokoll darunter zeigt die Einträge aller Fassungen, nicht nur die der gerade geöffneten.

Eine frühere Fassung holen Sie mit „Wiederherstellen" zurück. Ihr Inhalt wird dabei nicht über den aktuellen Stand geschrieben, sondern als neue Version übernommen, die Prüfung und Freigabe regulär durchläuft. Die Reihe bleibt damit lückenlos: Auch später ist noch nachvollziehbar, dass an einem bestimmten Tag auf eine ältere Fassung zurückgegangen wurde.

Was mit einer neuen Version mitwandert.
Anhänge, Lesepflicht und Links gehören zur einzelnen Fassung und werden bei jeder neuen Version übernommen – eine alte Version ist deshalb vollständig, wenn Sie sie wieder aufrufen. Die Verknüpfungen zu Controls, Risiken, Prozessen und anderen Dokumenten hängen dagegen am Dokument als Ganzem: Sie bleiben auf der freigegebenen Fassung stehen und wandern erst mit der nächsten Freigabe mit. Kein Bereich verliert dabei seinen Verweis.

© 2012–2026 WolfInfoSec GmbH

Eine abgelöste Fassung ist schreibgeschützt. Bearbeiten, Verknüpfen, Anhänge ändern und der KI-Assistent sind dort gesperrt; Ansehen, Word- und PDF-Export bleiben möglich, damit sich ein vergangener Stand jederzeit als Nachweis ausgeben lässt.

Aus Word übernehmen

Ein Dokument, das es schon gibt, muss nicht abgetippt werden. Über dem Bearbeitungsformular steht der Kasten „Aus Word übernehmen“: Ziehen Sie die Word-Datei hinein oder wählen Sie sie aus und klicken Sie auf „Übernehmen“. Der Inhalt steht danach im Editor. Gespeichert ist damit noch nichts – erst „Speichern“ legt ihn als Dokument beziehungsweise als neue Fassung ab. Der Kasten erscheint sowohl beim Anlegen eines neuen Dokuments als auch beim Bearbeiten eines vorhandenen.

Übernommen werden Überschriften, Aufzählungen und Nummerierungen, Tabellen samt verbundenen Zellen, Links, fetter, kursiver und unterstrichener Text sowie Bilder. Die Bilder wandern in den Dokumententext und gehen beim Word-Export wieder als Bild mit hinaus.

- **Was draußen bleibt**: Kopf- und Fußzeilen der Word-Datei – Seitenzahlen und Briefkopf kommen im ISMS aus der hinterlegten Vorlage –, das Inhaltsverzeichnis der Word-Datei, Text in Textfeldern und in Grafiken sowie Bilder in Formaten, die ein Browser nicht anzeigt (etwa EMF/WMF aus eingefügten Zeichnungen).
- **Was fehlt, wird gesagt**: Über dem Formular steht, aus welcher Datei der Inhalt stammt und was nicht übernommen werden konnte. Fehlt ein größerer Teil des Textes, weist WolfISMS eigens darauf hin – bitte das Ergebnis dann mit der Word-Datei vergleichen.
- **Grenzen**: Gelesen werden .docx-Dateien bis 16 MB; ältere .doc-Dateien speichern Sie in Word bitte zuerst als .docx. Ein einzelnes Bild darf bis zu 2 MB groß sein, alle Bilder zusammen bis zu 8 MB.

Beim Anlegen eines neuen Dokuments schlägt WolfISMS den Namen aus der Datei vor – aus dem Titel in den Dateieigenschaften, ersatzweise aus der ersten Überschrift. Der Text landet in dem Sprachfeld, in dem Sie gerade arbeiten: Wer die Oberfläche auf Englisch bedient, füllt damit den englischen Dokumententext.

Ist die KI eingeschaltet, steht im Kasten der Haken „Text gleich von der KI aufbereiten lassen“ – vorbelegt, aber jederzeit abwählbar. Die KI räumt dann die Umwandlung auf und führt den Text an ISO 27001 und NIS2 heran; ein Balken zeigt, wie weit sie ist. Das Ergebnis steht anschließend im Editor, und „Zurück zum übernommenen Text“ holt die unbearbeitete Fassung wieder hervor. Auch hier gilt: In der Datenbank steht erst etwas, wenn Sie speichern.

Der Import ersetzt den Text im Formular.
Was im Editor steht, wird durch das übernommene Dokument ersetzt; WolfISMS fragt vorher nach. An einer abgelösten Fassung und an einem schreibgeschützten Dokument ist der Import gesperrt – dort ist Bearbeiten ohnehin nicht vorgesehen.

Funktionen

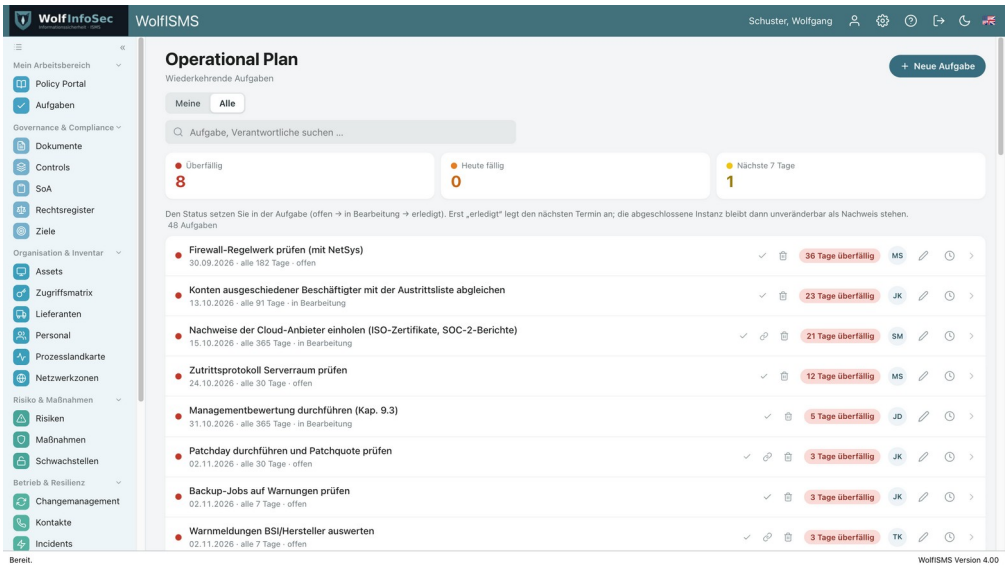
- **Dokumentenliste**: Filter nach Typ, Status, Kategorie; Suche beim Tippen (ohne Blättern)
- **Archiv**: Dokumente, die nicht mehr gelten, aber aufbewahrt werden müssen, werden archiviert. Sie verschwinden damit aus der Liste und sind über die Schaltfläche „Archiv" weiter erreichbar – gelöscht wird nichts
- **Detailansicht**: Vollständiger Dokumenteninhalt mit Metadaten, Anhängen und verknüpften BPMN-Diagrammen

© 2012–2026 WolfInfoSec GmbH

- **Formular einklappen**: Im Bearbeitungsformular lässt sich der Block „Grunddaten" bzw. „Metadaten" über die Überschrift zuklappen. Der Editor wächst dann bis zum unteren Fensterrand mit – bequem bei langen Dokumenten. Der Zustand bleibt im Browser gespeichert
- **Workflow: Prüfen**: Der zugewiesene Prüfer bestätigt den Inhalt (erzeugt ein Prüfdatum)
- **Workflow: Freigeben**: Der freigebende Benutzer (oder ein master-Benutzer) erteilt die formale Freigabe
- **Workflow: Neue Version**: Legt aus der freigegebenen Fassung den nächsten Arbeitsstand an – als vollständige Kopie samt Anhängen, Lesepflicht und Links. Die freigegebene Fassung bleibt unverändert und bleibt überall verknüpft, bis die neue freigegeben ist
- **Versionsverlauf**: Rechts in der Seitenspalte stehen alle Fassungen mit Nummer, Status und Datum; die geltende und der laufende Arbeitsstand sind gekennzeichnet – siehe den Abschnitt Versionen und Versionsverlauf
- **Version wiederherstellen**: Eine frühere Fassung wird als neuer Arbeitsstand übernommen und durchläuft Prüfung und Freigabe regulär – überschrieben wird nichts
- **Lesebestätigung**: Für Richtlinien lässt sich eine Lesebestätigung anfordern – seit v4.00 nur noch für diesen Dokumenttyp. Wer das Dokument noch nicht bestätigt hat, sieht es als offene Aufgabe; im Personalmodul ist der Stand je Mitarbeiter nachvollziehbar. Wer ein Dokument lesen muss, legt der Master-Benutzer in der Lesepflicht-Matrix des Policy Portals fest – ohne Rollenzuordnung bleibt ein freigegebenes Dokument sichtbar, ist aber für niemanden Pflicht. Darauf weist WolfISMS bei der Freigabe hin
- **Schreibschutz**: Freigegebene Dokumente können optional schreibgeschützt werden
- **Mehrsprachigkeit**: Separate Felder für deutschen und englischen Dokumenteninhalt
- **Anhänge**: Datei-Upload pro Dokument (Nachweise, Vorlagen); zulässig sind PDF-Dateien bis 16 MB
- **Review-Datum**: Die regelmäßige Überprüfung wird geplant und als Aufgabe angezeigt
- **Export**: Dokumentenliste als .xlsx; einzelne Dokumente als Word oder PDF – Aufzählungen in Tabellenzellen werden dabei korrekt als Liste ausgegeben. Ist ein PDF-Briefpapier hinterlegt, erscheint es als Kopf- und Fußzeile
- **Word-Import**: Über dem Bearbeitungsformular lässt sich eine .docx-Datei übernehmen – Überschriften, Listen, Tabellen, Links und Bilder kommen mit. Auf Wunsch bereitet die KI den übernommenen Text gleich auf; gespeichert wird wie sonst auch erst mit „Speichern“ – siehe den Abschnitt Aus Word übernehmen
- **Charts**: Status- und Typ-Kreisdiagramme
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er erstellt Dokumente, übernimmt sie aus hochgeladenen Unterlagen, überarbeitet, prüft und führt zusammen, schlägt Verknüpfungen zu Controls, Prozessen, Dokumenten, Maßnahmen und Risiken vor, erstellt die englische Fassung, gibt ein Dokument in die Prüfung und findet Lücken – Pflichtdokumente und Controls ohne Dokument. Er ersetzt die früheren Knöpfe „KI-Bearbeitung“ und „KI-Verknüpfungen“; freigeben tut er nie. Gespeichert wird erst, was Sie bestätigen.
- **KI-Übersetzung (dok):** Ist die Oberfläche auf Englisch gestellt, steht seit v3.95 in der Detailansicht die Schaltfläche „AI translation“. Sie übersetzt den deutschen Dokumententext ins Englische und schlägt das Ergebnis für den englischen Text vor. Überschriften, Tabellen, Bilder und Layout kommen unverändert aus der deutschen Fassung – an die KI gehen nur die Textabschnitte. Der Dialog zeigt Deutsch und Englisch nebeneinander und meldet, wenn ein Abschnitt deutsch geblieben ist oder die Inline-Formatierung (fett, kursiv, Link) eines Abschnitts nicht übertragen werden konnte. Eine eigene Anweisung – etwa „amerikanisches Englisch“ – lässt sich mitgeben, der übersetzte Dokumentenname auf Wunsch mit übernehmen. „Übernehmen“ ersetzt einen vorhandenen englischen Text und legt wie jede Übernahme aus dem KI-Assistenten eine neue Version an. Voraussetzung: KI freigeschaltet, deutscher Text vorhanden, das Dokument ist weder freigegeben noch in Prüfung oder Freigabe, und Sie dürfen es ändern
- **Kommentare**: Diskussionsfaden je Dokument

© 2012–2026 WolfInfoSec GmbH

- **Verknüpfte Dokumente:** Verweist DOK0001 auf DOK0002, steht DOK0001 seit v3.94 auch bei DOK0002 unter „Dokumente“ und in dessen Verknüpfungsansicht. Lösen lässt sich die Verknüpfung von beiden Seiten; ein Verweis aus einer abgelösten Version zählt nicht mit
- **Benachrichtigung bei der Freigabe**: wird eine Richtlinie freigegeben, erhalten alle Benutzer mit Lesepflicht sofort eine E-Mail mit Nummer, Name, Version und einem Direktlink in das Policy Portal – sie müssen nicht auf die nächste Aufgaben-Erinnerung warten. Die Mail kommt in der Sprache des jeweiligen Empfängers



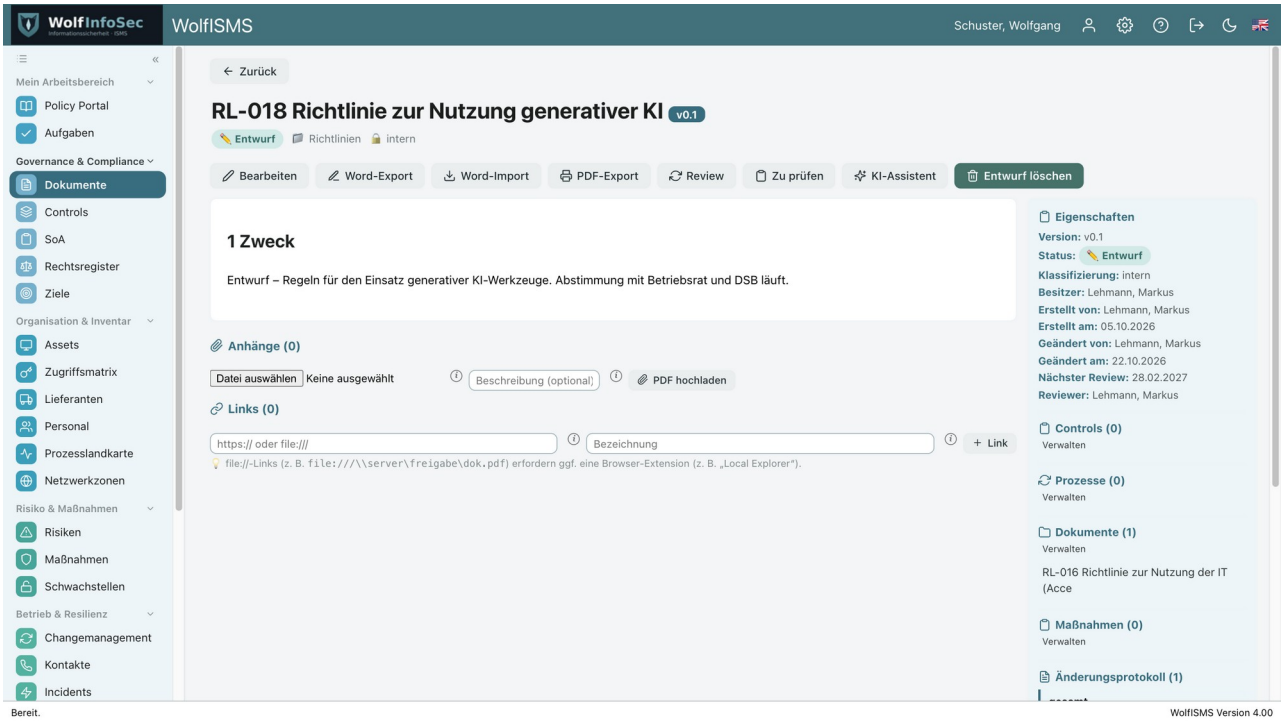
21. BPMN-Prozessmodellierung

Beschreibung

Das BPMN-Modul ermöglicht die Erstellung und Verwaltung von Prozessdiagrammen direkt im Browser, ohne externe Software. Die Diagramme können mit Dokumenten verknüpft werden.

Funktionen

- **Viewer**: Interaktive, zoombare Ansicht eines BPMN-Diagramms (schreibgeschützt)
- **Editor**: Vollständiger BPMN-Modeler auf Basis von bpmn-js (Drag & Drop, Elemente einfügen)
- **Importieren (dok)**: Upload einer .bpmn- oder .xml-Datei aus einer externen BPMN-Anwendung (z. B. Camunda, draw.io)
- **Exportieren**: Download des aktuellen Diagramms als .bpmn-Datei für die externe Bearbeitung
- **Speichern (dok)**: Diagramm mit Nummer, Titel und Status in der Datenbank ablegen
- **Titel-Vorschlag**: Beim Import wird der Dateiname automatisch als Titelvorschlag übernommen
- **Verknüpfung**: BPMN-Diagramme können in der Dokumenten-Detailansicht verknüpft werden
- **Verknüpfte Dokumente:** Unter dem Diagramm listet der Viewer seit v3.94 die Dokumente, die mit dem Prozess verknüpft sind – je Dokument eine Zeile, bevorzugt die gültige Fassung



22. Playbooks

Beschreibung

Das Playbook-Modul beschreibt, wie auf ein Szenario reagiert wird – Ransomware, Phishing, Ausfall eines Dienstleisters, meldepflichtiger Vorfall. Seit v4.00 folgt jedes Playbook einem festen Rahmen nach ISO/IEC 27035 und NIST SP 800-61 (ISO/IEC 27001 A.5.24–A.5.28): Steckbrief mit Freigabe, feste Abschnitte, Ablaufschritte, Rollen, Übungen und Tests. Hochgeladene PDF-Dateien und externe Links bleiben und lassen sich einem Playbook zuordnen.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet. Die Texte, Dateien und Links bleiben gespeichert, sind aber nicht abrufbar.

Funktionen

- **Liste:** alle Playbooks mit Ampel, Art und Freigabestand. Die Kacheln Freigegeben, In Arbeit, Überprüfung fällig und Handlungsbedarf filtern mit einem Klick, dazu ein Filter nach Art und die Suche über Nummer, Titel, Szenario und Dateinamen. Darunter stehen Dateien und Links, die noch keinem Playbook zugeordnet sind
- **Steckbrief:** Nummer (vorgeschlagen PB-001 ff.), Art (Incident Response, Notfall und Wiederanlauf, Meldung, Betrieb), Szenario, ab welchem Schweregrad es gilt, Verantwortlich und Stellvertretung, Freigabestand (Entwurf, in Prüfung, freigegeben, in Überarbeitung), Version, Freigabe und nächste Überprüfung
- **Freigabe:** setzen Sie den Freigabestand auf „freigegeben“, trägt WolfISMS Datum und Freigebende/n ein, plant die nächste Überprüfung in zwölf Monaten und setzt die Version auf 1.0, wenn noch keine eingetragen ist
- **Feste Abschnitte:** Zweck und Geltungsbereich, Auslöser und Erkennung, Erstbewertung und Eskalation, Eindämmung, Beseitigung, Wiederherstellung, Kommunikation und Meldungen, Nachbereitung – jeder mit einem Hinweis, was hineingehört, samt den Meldefristen nach NIS-2, DSGVO und CRA. Ein früher frei geschriebener Text steht als „Weitere Inhalte“ darunter
- **Ablaufschritte:** Phase (Erkennung, Erstbewertung, Eindämmung, Beseitigung, Wiederherstellung, Kommunikation, Nachbereitung), Schritt, Rolle, Frist und Nachweis
- **Rollen:** Rolle und Person – ein Benutzer oder, für Externe, ein Name – mit ihrer Aufgabe
- **Übungen und Tests:** Datum, Art (Tabletop, Walkthrough, Simulation, Live-Test), Ergebnis (geplant, erfolgreich, teilweise erfolgreich, nicht erfolgreich), Teilnehmer und Befunde
- **Ampel:** die Seitenleiste prüft, ob ein Playbook einsatzfähig ist – Verantwortliche und Stellvertretung, Art und Szenario, alle acht Abschnitte, mindestens drei Ablaufschritte mit Rolle, besetzte Rollen, Freigabe, nächste Überprüfung und ein Test in den letzten zwölf Monaten. Rot wird sie bei überfälliger Überprüfung oder einem nicht erfolgreichen letzten Test. Sie ist ein Hinweis, keine Sperre
- **Verknüpfungen (play):** Assets, Risiken, Incidents, bei denen das Playbook angewendet wurde, Dokumente und Vorgaben, Lieferanten, Behörden und Dienstleister aus den Kontakten sowie Maßnahmen
- **Dateien und Links (play):** PDF-Dateien hochladen und externe Links setzen (CERT, BSI, Herstellerdokumentation) wie bisher; beides lässt sich einem Playbook zuordnen und steht dann in seiner Detailansicht

© 2012–2026 WolfInfoSec GmbH

- **Bearbeiten und Löschen (play):** durch Verantwortliche, Stellvertretung, den Ersteller – solange niemand verantwortlich ist – oder einen Master-Benutzer. Beim Löschen bleiben zugeordnete Dateien und Links erhalten und stehen wieder in der Liste
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er legt ein Playbook an – Sie schildern das Szenario oder laden ein vorhandenes Dokument hoch –, prüft es, bereitet eine Übung (Tabletop) vor, erfasst ein Testergebnis, schärft es nach einem Incident nach, findet Lücken im Bestand und geht Ihre Playbooks mit Handlungsbedarf durch. Gespeichert wird erst, was Sie bestätigen.

© 2012–2026 WolfInfoSec GmbH

23. Lieferanten

Beschreibung

Das Lieferanten-Modul verwaltet alle externen Dienstleister und Zulieferer. Es berechnet automatisch einen Risikoscore auf Basis von Vertragsstatus, Zertifizierungen, Datenschutz und Frühwarnindikatoren.

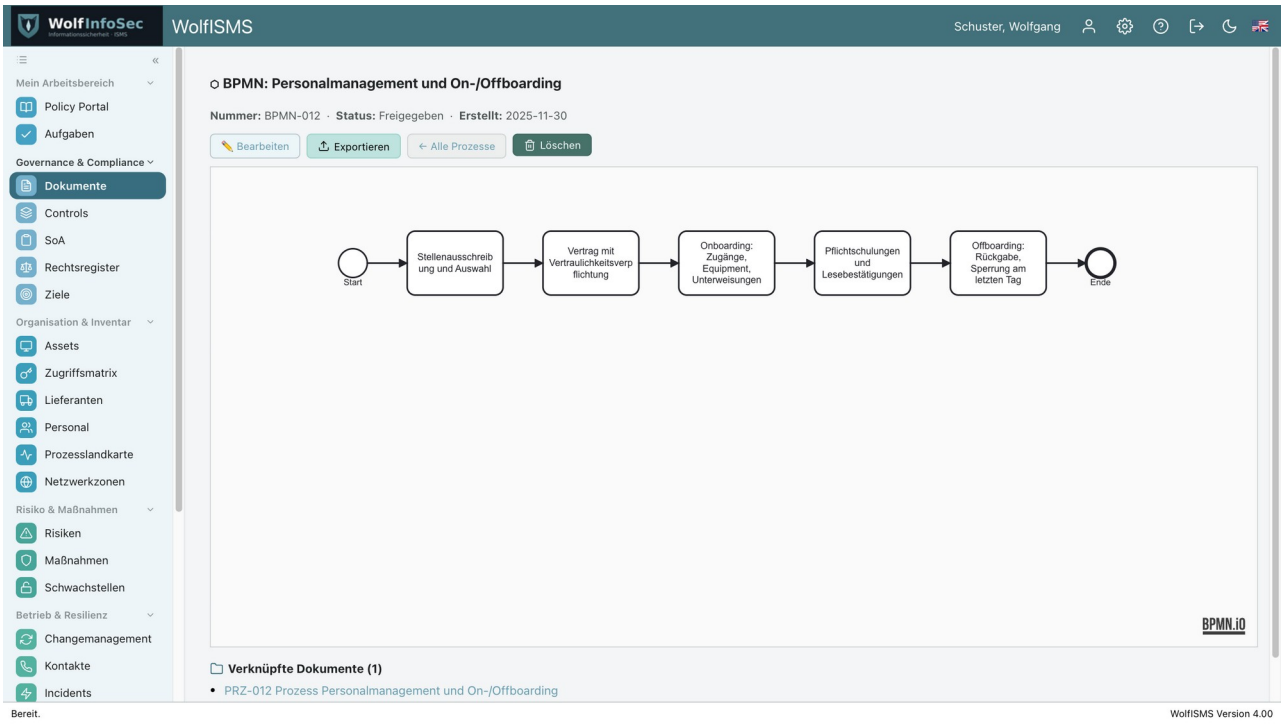
Funktionen

- **Lieferantenregister**: Liste mit Suche und Filtern nach Typ, Tier und Risikostufe; die Typkacheln erscheinen, wenn Ihr Administrator die Infokacheln eingeschaltet hat
- **Beschreibung**: Seit v4.00 ein Freitextfeld mit Editor in Bearbeiten-Maske und Detailansicht – etwa für Leistungsumfang, Standorte oder Besonderheiten. Es steht auch im Excel-Export und lässt sich über die REST-API lesen und schreiben
- **Risikobewertung**: Der Block mit den Bewertungskriterien steht seit v4.00 nur noch in der Bearbeiten-Maske; die Detailansicht bleibt dadurch übersichtlicher
- **Risikoscore**: Automatische Berechnung aus: Personendaten, Vertrag, Zertifizierungen, Sicherheitsniveau, Schadenshöhe, Eintrittswahrscheinlichkeit
- **Tier-Klassifizierung:** Tier 1 (kritisch) bis Tier 3 (unkritisch) oder unwesentlich bis missionskritisch. Seit v4.01 zählt das Tier in der Schadenshöhe doppelt und setzt eine Untergrenze: ein missionskritischer Lieferant bzw. Tier 1 hat mindestens Schadenshöhe 4, ein geschäftskritischer mindestens 3
- **Score-Historie**: Jede Neuberechnung wird mitgeschrieben, sodass sich die Entwicklung des Lieferantenrisikos über die Zeit nachvollziehen lässt
- **Fragebogen-Status**: Verfolgung des Lieferanten-Sicherheitsfragebogens
- **Verknüpfungen (vendor)**: Verlinkung mit Maßnahmen und Incidents
- **Review-Datum**: Regelmäßige Lieferantenbewertung mit Aufgabenerzeugung
- **Excel-Export**: Vollständige Lieferantenliste als .xlsx – mit E-Mail, den sieben Bewertungskriterien und der Cloud-Exit-Strategie als Klartext; die Mappe dient zugleich als Importvorlage
- **Import:** Die Schaltfläche „Import“ neben „Export“ liest eine .xlsx- oder .csv-Datei (Komma oder Semikolon, höchstens 8 MB) ein; Pflicht ist nur die Spalte „Name“. Zuerst zeigt eine Vorschau, was angelegt, geändert („alter Wert → neuer Wert“) oder übersprungen würde – geschrieben wird erst, wenn Sie dieselbe Datei mit dem Häkchen „Übernehmen“ erneut hochladen. Eine bekannte Lieferantennummer aktualisiert diesen Lieferanten, ohne Nummer der Lieferant mit genau diesem Namen; alles andere wird neu angelegt, wenn „Neuanlage“ gesetzt ist. Leere Zellen ändern nichts. Zeilen mit Werten außerhalb der Auswahllisten, unbekannten oder mehrdeutigen Verantwortlichen, ungültiger E-Mail-Adresse, doppelte Zeilen und fremde Lieferanten, die Sie nicht ändern dürfen, werden mit Grund übersprungen. Verantwortliche geben Sie als E-Mail-Adresse oder „Nachname, Vorname“ an, mehrere durch „;“ getrennt. Risiko und Score rechnet WolfISMS neu; die Spalte Cloud-Exit-Strategie wird nicht eingelesen, damit ihre Formatierung erhalten bleibt. Voraussetzung ist das Schreibrecht für Lieferanten
- **Cloud-Exit-Strategie:** Lieferanten eines Typs, den der Administrator als Cloud/SaaS markiert hat, haben in der Bearbeitungsmaske einen eigenen Abschnitt mit Editor und Ausfüllhilfe – Datenexport, Löschung nach Vertragsende, Alternativanbieter, Kündigungsfristen, Migrationsaufwand, letzter Test. Er blendet sich beim Wechsel des Typs sofort ein oder aus; ein erfasster Text bleibt dabei erhalten. Die Detailansicht zeigt die Strategie oder einen Warnhinweis mit „Jetzt erfassen“. Über der Liste steht, wie viele Cloud-/SaaS-Lieferanten noch keine Strategie haben; „Anzeigen“ filtert auf genau diese, in der Tabelle sind sie mit ☁⚠ markiert
- **AVV-Angaben (datenschutz):** Seit v4.01 zeigt die Detailansicht eines Lieferanten, der personenbezogene Daten verarbeitet („Personendaten“ Ja oder Teilweise), den Block Auftragsverarbeitung nach Art. 28 DSGVO: AV-Vertrag vorhanden, Datum, Dokument, Drittland mit

© 2012–2026 WolfInfoSec GmbH

Garantie und Transfer Impact Assessment sowie die Unterauftragsverarbeiter. Pflegen darf ihn, wer das Recht „Datenschutz“ mit Bearbeiten hat – das Lieferanten-Recht reicht dafür nicht

- **Charts**: Risikostufen- und Typ-Kreisdiagramme
- **Kommentare**: Diskussionsfaden je Lieferant
- **KI-Assistent (ab Essentials)**: Hat Ihr Administrator die KI freigeschaltet und Ihnen das Recht „KI-Nutzung“ gegeben, steht oben in der Liste und in der Detailansicht der Knopf „KI-Assistent“. Er öffnet ein Gespräch auf einer eigenen Seite, aufgebaut wie der KI-Assistent für Risiken. Er legt Lieferanten an (frei, aus einem Asset oder einer Unterlage, auch mehrere aus einer Liste), prüft einzelne, einen Typ, ein Tier oder den Gesamtbestand, wertet Nachweise aus, findet Lücken, führt zusammen und verschickt den Sicherheitsfragebogen samt passender Fragen; zurückgekommene Antworten wertet er aus – auch Fremdformate wie CAIQ oder VDA ISA/TISAX. Gespeichert wird erst, was Sie bestätigen.



Sicherheitsfragebogen

Der Fragebogen erhebt beim Lieferanten schriftlich, wie er Informationssicherheit umsetzt. Die Vorlage folgt ISO/IEC 27001:2022 und NIS2 und umfasst 49 Fragen in 12 Kategorien – von den Angaben zum Unternehmen über Zugriffssteuerung, Verschlüsselung und Notfallmanagement bis zu Meldepflichten und Subunternehmern. Welche Fragen gestellt werden, legt Ihr Administrator im Fragenkatalog fest.

- **Versenden:** In der Detailansicht des Lieferanten fasst seit v3.95 das Aufklappmenü „Fragebogen“ alle Aktionen zum Fragebogen zusammen; der erste Eintrag öffnet den Versand. Der Lieferant erhält eine E-Mail mit einem Link auf ein Formular, das er ohne Anmeldung ausfüllt. Voraussetzung sind eine E-Mail-Adresse und ein Ansprechpartner am Lieferanten; fehlt eines von beidem, sagt WolfISMS das vor dem Versand.
- **Gültigkeit:** Der Link gilt 30 Tage. Danach steht der Bogen auf „abgelaufen" und nimmt keine Antworten mehr an – ein erneuter Versand erzeugt einen neuen Link.

© 2012–2026 WolfInfoSec GmbH

- **Adresse im Link**: Ist Ihr ISMS für Lieferanten unter einer anderen Adresse erreichbar als für die eigenen Mitarbeiter, hinterlegt der Administrator diese Domain im Fragenkatalog. Der Link in der E-Mail zeigt dann dorthin
- **Ohne Mailversand:** Alternativ lässt sich der Fragebogen als PDF verschicken oder als E-Mail-Datei erzeugen und aus dem eigenen Mailprogramm senden. Die Antworten tragen Sie dann selbst ein.
- **Manuell erfassen:** Kommt die Antwort auf Papier oder als ausgefülltes PDF zurück, erfassen Sie sie von Hand. Das Original lässt sich als Anhang hinterlegen, dazu Eingangsdatum und eine Bemerkung.
- **Status:** versendet, in Erfassung, beantwortet oder abgelaufen – in der Lieferantenübersicht auf einen Blick.
- **Auswertung:** Die Antworten stehen je Lieferant unter „Fragebogen" – nach Kategorien gegliedert, mit dem Framework-Bezug jeder Frage. Ein Kurzüberblick zeigt, wie viele Fragen mit Ja, Teilweise oder Nein beantwortet wurden.
- **Wirkung auf die Bewertung:** Mit dem Eingang der Antworten steht das Feld „Fragebogen" des Lieferanten auf „Ja", und der Risikoscore wird neu gerechnet.

Der Fragebogen läuft nicht ab, wenn Sie ihn selbst erfassen.
Die Frist gilt allein für den versendeten Link – dort wird ein Token ungültig. Ein per PDF verschickter oder von Hand erfasster Bogen bleibt so lange offen, bis Sie ihn abschliessen.

© 2012–2026 WolfInfoSec GmbH

24. Personal

Beschreibung

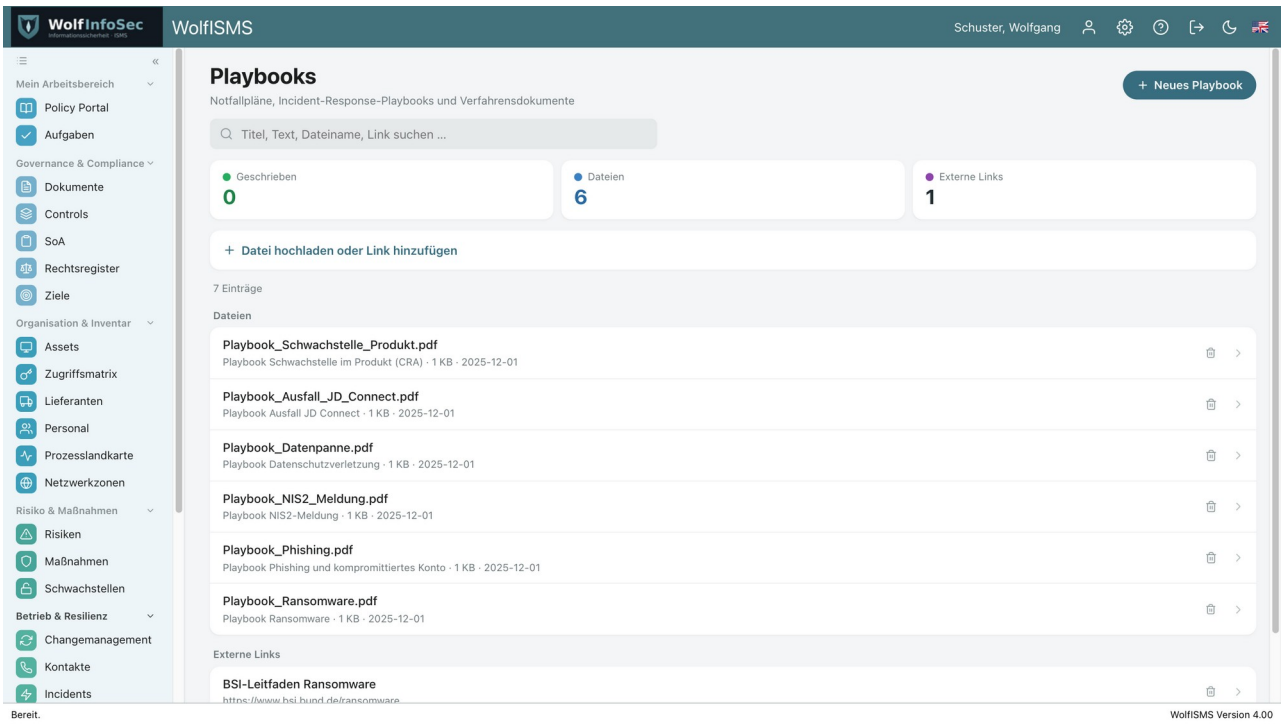
Das Personalmodul bietet einen Überblick über alle Mitarbeiter und deren Lesestatus bei Schulungsdokumenten. Es unterstützt die Nachweisführung für Sicherheitsschulungen gemäß ISO 27001 A 6.3.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet.

Funktionen

- **Avatar-Kacheln**: Mitarbeiterkacheln mit Initialen, Abteilung, Position und Lesestatus-Balken
- **Abteilungs-Filter**: Reiter je Abteilung – die Abteilungen und Teams stammen aus der zentral gepflegten Stammdatenliste – plus Alphabet-Navigationsleiste
- **Dokumentenstatus**: Pro Mitarbeiter: welche Schulungsdokumente gelesen wurden, welche noch offen sind und welche für die Rollen des Mitarbeiters gar keine Lesepflicht auslösen
- **Lesestatus-Balken**: Prozentualer Fortschritt der gelesenen Pflichtdokumente. Gezählt wird nur, was der Mitarbeiter laut Lesepflicht-Matrix lesen muss – wer nichts lesen muss, steht bei 100 %
- **Excel-Export (pers)**: Zwei Tabellenblätter: Mitarbeiterübersicht und vollständige Lesestatus-Matrix. Die Matrix kennt drei Zustände: gelesen, offen und – für Dokumente ohne Lesepflicht – ein Strich
- **Awareness-Bericht**: Schaltfläche neben „Export“, sichtbar mit Leserecht Personal. PDF mit der Lesequote gesamt, je Pflichtdokument (mit Version, Freigabe und letzter Bestätigung) und je Abteilung sowie den offenen Lesepflichten je Person. Gezählt werden nur aktive Konten – die Quote kann deshalb von den Kacheln oben abweichen, die ausgeschiedene Mitarbeitende mitzählen

© 2012–2026 WolfInfoSec GmbH



Hinweise

Das Personalmodul zeigt nur Dokumente, für die eine Lesebestätigung vorgesehen ist. Ob ein Mitarbeiter ein solches Dokument auch lesen muss, entscheidet die Lesepflicht-Matrix des Policy Portals; sie wird vom Master-Benutzer gepflegt. Das Anlegen von Benutzern erfolgt unter /admin.

On-/Offboarding

Über dem Personalverzeichnis stehen seit v3.72 zwei Reiter: „Personalverzeichnis" und „On-/Offboarding". Der zweite verfolgt Ein- und Austritte – vom Arbeitsvertrag über die Systemzugänge bis zur Rückgabe der Ausstattung.

Ein Vorgang beschreibt eine Person mit Ein- oder Austrittsdatum, Abteilung und Aufgabe. Drei Punkte sind fest vorgegeben, zwei Listen füllen Sie selbst:

- **Arbeitsvertrag / NDA**: nur beim Eintritt. Liegen Vertrag und Verpflichtungserklärung unterschrieben vor, wird der Punkt abgehakt
- **Firmen-E-Mail**: das Postfach ist eingerichtet – beim Austritt: gesperrt oder umgeleitet
- **ISMS-Benutzer**: ergibt sich aus der Verknüpfung mit einem Benutzerkonto. Beim Eintritt gilt der Punkt als erledigt, sobald ein Konto verknüpft ist; beim Austritt erst, wenn das Konto gesperrt ist. Sperren lässt es sich unmittelbar aus dem Vorgang heraus
- **Zugänge**: die Systemzugänge mit Bezeichnung, Konto und Bemerkung. Beim Anlegen des Vorgangs lässt sich die Liste zeilenweise vorbelegen
- **Equipment**: die Ausstattung mit Inventar- oder Seriennummer – Notebook, Telefon, Schlüssel, Token

Die drei festen Punkte kennen neben „offen" und „erledigt" auch „nicht erforderlich"; so gekennzeichnet zählen sie im Fortschritt nicht mit. Der Balken am Vorgang zeigt die erledigten Punkte im Verhältnis zu allen zählenden – die beiden Listen eingeschlossen.

© 2012–2026 WolfInfoSec GmbH

- **Übersicht**: Reiter für Eintritte, Austritte und abgeschlossene Vorgänge, dazu eine Suche über Name, Abteilung und E-Mail-Adresse
- **Abschließen**: ein abgeschlossener Vorgang ist gegen Änderungen gesperrt. Zum Nacharbeiten wird er wieder geöffnet
- **Austritt aus Eintritt**: aus einem Onboarding entsteht auf Knopfdruck das passende Offboarding. Stammdaten, Zugänge und Ausstattung werden als offene Punkte übernommen – zurückzugeben ist genau das, was ausgegeben wurde
- **Benutzer sperren**: setzt das verknüpfte ISMS-Konto auf inaktiv. Das eigene Konto und der jeweils letzte aktive Administrator bzw. Master-Benutzer lassen sich nicht sperren
- **Protokoll**: Anlegen, Ändern, Abschließen und Löschen eines Vorgangs stehen in den Aktivitäten

Es gilt das Recht Personal: ab Stufe 1 lesen, ab Stufe 2 bearbeiten. Benutzerkonten selbst werden weiterhin unter Administration angelegt; der Vorgang verweist nur darauf.

Schulungen

Seit v3.93 steht über dem Personalverzeichnis ein dritter Reiter, „Schulungen“. Dort planen Sie Sicherheitsschulungen und weisen nach, wer sie besucht hat – als Ergänzung zu den Lesebestätigungen, die das Personalmodul ohnehin zeigt (ISO/IEC 27001 A.6.3).

- **Schulungsliste:** Datum, Titel, Ort, Referent, Teilnehmer (besucht/zugewiesen) und der Anteil, der die Schulung abgeschlossen hat, als Prozentwert mit Balken. Darüber Kennzahlen, Filter „Alle“, „Anstehend“, „Nicht abgeschlossen“ und „Abgeschlossen“ sowie eine Suche
- **Anlegen und Bearbeiten:** Titel und Datum sind Pflicht, Ort, Referent und Beschreibung freiwillig
- **Alle Benutzer zuweisen:** eine Schaltfläche in der Detailansicht weist alle aktiven Benutzer zu, die noch nicht zugewiesen sind
- **Einzeln zuweisen:** Liste mit Kästchen und Filterfeld; „alle angezeigten markieren“ wählt etwa eine ganze Abteilung auf einmal
- **Teilnahme festhalten:** je Person „teilgenommen“ bzw. „zurücksetzen“ oder „Alle als teilgenommen markieren“. Als Teilnahmedatum gilt das Datum der Schulung. Ist es verstrichen, stehen die Offenen als „versäumt“ in der Liste
- **Bei den Mitarbeitern:** die Personalliste hat die Spalte „Offene Schulungen“ (versäumte Termine rot), die Kacheln zeigen etwa „2 Schulungen offen“, und die Detailseite einer Person listet offene und besuchte Schulungen mit Datum

Ansehen dürfen Sie die Schulungen mit Leserecht auf Personal, anlegen, zuweisen und Teilnahmen setzen mit Schreibrecht. Jede Änderung steht im Aktivitätsprotokoll.

© 2012–2026 WolfInfoSec GmbH

25. Policy Portal

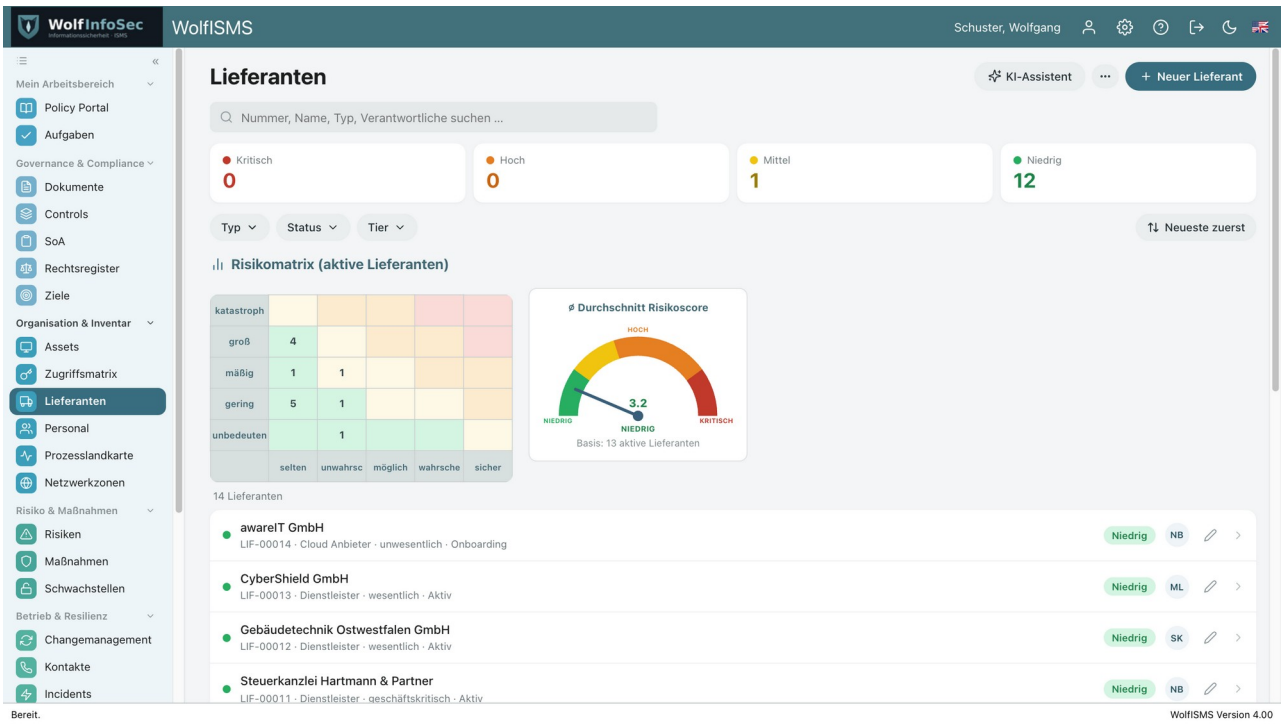
Beschreibung

Das Policy Portal ist das Mitarbeiterportal für die Richtlinien des Unternehmens. Mitarbeiter ohne ISMS-Bearbeitungsrechte können hier zugewiesene Dokumente lesen und ihre Lektüre bestätigen.

Funktionen

- **Richtlinien-Anzeige**: Seit v4.00 zeigt das Portal ausschließlich Richtlinien; die Auswahl der Dokumenttypen ist entfallen. Lesestatus und Excel-Export beschränken sich ebenso auf Richtlinien
- **Pflichtlektüre und freiwillige Dokumente**: Welche Dokumente Sie lesen müssen, hängt seit v3.71 an Ihrer Rolle. Die Pflichtlektüre steht oben und ist als „Nicht gelesen" gekennzeichnet, bis Sie bestätigt haben; alle übrigen Dokumente tragen die Kennzeichnung „Freiwillig" – Sie können sie lesen und bestätigen, müssen es aber nicht. Besteht für Ihre Rolle überhaupt keine Lesepflicht, sagt Ihnen das der Text unter der Überschrift
- **Lesebestätigung**: Ein Klick auf „Gelesen“ markiert das Dokument als bestätigt. Seit v3.90 wird dabei der Zeitpunkt festgehalten; der Awareness-Bericht zeigt ihn als letzte Bestätigung. Frühere Bestätigungen gelten weiter, nur ohne Datum. Erst danach verschwindet der Eintrag aus Ihren offenen Aufgaben
- **Lesestatus**: Übersicht, welche Dokumente bereits bestätigt wurden. Administratoren und Master-Benutzer erreichen die Auswertung über alle Mitarbeiter direkt über die Schaltfläche „Lesestatus" im Portal
- **Anhänge**: Hängen an einer Richtlinie Dateien, öffnen Sie sie direkt aus dem Portal – ohne Zugriff auf das Dokumentenmodul. Noch nicht gelesene Dokumente stehen in der Liste oben
- **Lesestatus-Reset (master)**: Master-Benutzer können den Lesestatus einzelner Dokumente zurücksetzen – etwa nach einer inhaltlichen Überarbeitung, wenn alle Mitarbeiter erneut bestätigen sollen
- **Lesepflicht-Matrix (master)**: Die Schaltfläche „Lesepflicht-Matrix" öffnet eine Kreuztabelle aus freigegebenen Dokumenten und Rollen. Ein Häkchen bedeutet: Wer diese Rolle hat, muss das Dokument lesen und bestätigen. Eine Zeile ohne Häkchen – der Zustand jedes neu freigegebenen Dokuments – bedeutet, dass es niemand lesen muss; das Dokument bleibt sichtbar und lässt sich freiwillig bestätigen. Die Rollen selbst und ihre Zuordnung zu den Benutzern pflegt der Administrator unter Administration → Rollen
- **Export**: Export des Lesestatus als .xlsx
- **Mehrsprachigkeit**: Anzeige in Deutsch oder Englisch je nach Benutzereinstellung
- **Benachrichtigung**: sobald eine Richtlinie freigegeben wird, die für Ihre Rolle Pflichtlektüre ist, kommt eine E-Mail mit einem Direktlink auf das Dokument im Portal. Ist das Dokument keiner Rolle zugeordnet, geht keine Mail hinaus. Wer keine Mails aus WolfISMS erhalten möchte, wendet sich an den Administrator

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
Mein Arbeitsbereich
Policy Portal
Aufgaben
Governance & Compliance
Dokumente
Controls
SoA
Rechtsregister
Ziele
Organisation & Inventar
Assets
Zugriffsmatrix
Lieferanten
Personal
Prozesslandkarte
Netzwerkzonen
Risiko & Maßnahmen
Risiken
Maßnahmen
Schwachstellen
Betrieb & Resilienz
Changemanagement
Kontakte
Incidents
Lieferanten
KI-Assistent
+ Neuer Lieferant
Nummer, Name, Typ, Verantwortliche suchen …
Kritisch 0
Hoch 0
Mittel 1
Niedrig 12
Typ
Status
Tier
Neueste zuerst
Risikomatrix (aktive Lieferanten)
katastroph
groß 4
mäßig 1 1
gering 5 1
unbedeuten 1
selten
unwahrsc
möglich
wahrsche
sicher
ø Durchschnitt Risikoscore
HOCH
3.2
NIEDRIG
KRITISCH
Basis: 13 aktive Lieferanten
14 Lieferanten
awarelT GmbH
LIF-00014 · Cloud Anbieter · unwesentlich · Onboarding
Niedrig NB
CyberShield GmbH
LIF-00013 · Dienstleister · wesentlich · Aktiv
Niedrig ML
Gebäudetechnik Ostwestfalen GmbH
LIF-00012 · Dienstleister · wesentlich · Aktiv
Niedrig SK
Steuerkanzlei Hartmann & Partner
LIF-00011 · Dienstleister · geschäftskritisch · Aktiv
Niedrig NB
Bereit.
WolfISMS Version 4.00

26. Kontakte

Beschreibung

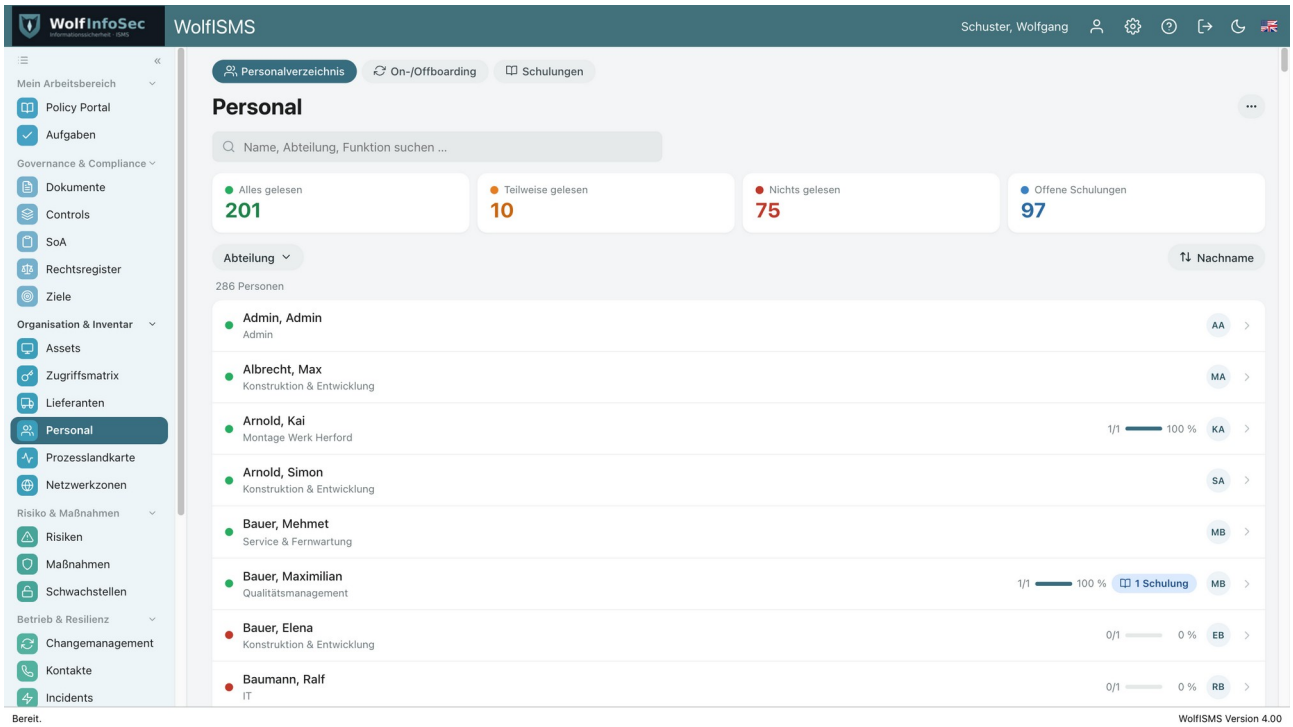
Das Kontaktmodul ist das zentrale Adressbuch des ISMS. Es verwaltet vier Kategorien von Kontakten in separaten Reitern: interne Mitarbeiter, externe Dienstleister, Behörden sowie Interessensgruppen (z. B. Verbände, NGOs, Partnerorganisationen). Das Modul unterstützt die Dokumentation relevanter Ansprechpartner gemäß ISO 27001 und NIS-2.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet.

Funktionen

- **Vier Reiter**: Mitarbeiter, Dienstleister, Behörden und Interessensgruppen – jede Kategorie in einer eigenen Übersichtstabelle mit Suche und Filterung
- **Kontaktdaten**: Telefon, Mobil, E-Mail (anklickbar als mailto-Link), Website, Abteilung, Position, Standort und Bemerkung
- **Statistik-Kacheln**: Anzahl der Einträge je Kategorie auf einen Blick
- **Detailansicht**: Vollständige Kontaktinformationen auf einer eigenen Seite
- **Anlegen / Bearbeiten / Löschen**: Vollständige Funktionen für Benutzer mit Bearbeitungsrecht (kontakte ≥ 2)
- **Interessensgruppen**: Zusätzliche Felder für Typ (z. B. Verband, NGO) und Relevanz (hoch/mittel/niedrig)

Benutzerrecht: kontakte (0 = kein Zugriff, 1 = Lesen, 2 = Bearbeiten) – URL: /kontakte



© 2012–2026 WolfInfoSec GmbH

27. BCM – Business Continuity Management

Beschreibung

Das BCM-Modul unterstützt die Planung und Überwachung der Geschäftskontinuität gemäß ISO 22301 und ISO/IEC 27001 (A.5.29, A.5.30). Ausgangspunkt sind die Assets: Für ein Asset – in der Regel einen Geschäftsprozess oder eine Information – bewertet die Business Impact Analyse, wie schwer ein Ausfall über die Zeit wiegt. Notfallpläne und BCM-Übungen werden ebenfalls einem Asset zugeordnet.

Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet.

Die Wiederanlaufziele RTO, RPO und MAZ stehen am Asset selbst und werden im Assetmodul gepflegt; die BIA zeigt sie an.

Geändert mit v3.84: keine eigenen „Kritischen Prozesse“ mehr.
Bis v3.83 führte das BCM eine eigene Prozessliste. Sie ist entfallen – Prozesse werden als primäre Assets geführt. Eine ältere BIA, die noch auf einen früheren Prozess verweist, zeigt „früher Prozess: …“; ordnen Sie ihr über ✏ ein Asset zu und tragen Sie RTO, RPO und MAZ am Asset ein.

Funktionen

- **Business Impact Analyse (BIA)**: die Startseite des Moduls. Je Asset werden die Auswirkungen eines Ausfalls in vier Dimensionen – finanziell, operativ, regulatorisch, Reputation – über die Zeitschritte 1 h, 4 h, 24 h, 72 h und 1 Woche bewertet (1 = unbedeutend bis 4 = kritisch). Daraus ergibt sich ein Gesamtscore mit Einstufung niedrig, mittel, hoch oder kritisch. Jede BIA trägt eine Nummer im Format BIA-00001.
- **Übersicht**: Liste aller BIAs mit Asset, Asset-Besitzer, Gesamtscore, dem Höchstwert je Dimension und RTO/RPO/MAZ. Die Kacheln zählen die erfassten BIAs, die kritischen und die primären Assets ohne BIA.
- **Wiederanlaufziele**: RTO (Wiederanlaufzeit), RPO (tolerierter Datenverlust) und MAZ (maximal tolerierbare Ausfallzeit) werden farblich hervorgehoben – je kürzer, desto kritischer. Gepflegt werden sie am Asset.
- **Notfallpläne**: Notfallplan, Wiederanlaufplan, Kommunikationsplan, Krisenstabsplan, IT-Notfallplan und Sonstiges – mit Version, Gültigkeit, Statusworkflow (Entwurf → In Review → Freigegeben, Zurückgezogen) und dem Asset, für das der Plan gilt.
- **BCM-Übungen**: Tabletop, Funktionsübung, Vollübung und Technischer Test mit Datum, Teilnehmern, Ergebnis (bestanden, teilweise, nicht bestanden) und Erkenntnissen, zugeordnet zum geübten Asset.
- **Maßnahmen aus Übungen:** Seit v3.95 lassen sich einer Übung Maßnahmen zuordnen – vorhandene über „Verwalten“ im Abschnitt Maßnahmen der Seitenleiste, neue mit „Neue Maßnahme anlegen & verknüpfen“, die sofort verknüpft sind. Die Maßnahme zeigt die Übung als Rückverweis „BCM-Übungen“. Dafür brauchen Sie das Bearbeitungsrecht für BCM, zum Anlegen zusätzlich das für Maßnahmen.
- **Mehrsprachigkeit**: Titel und Texte lassen sich zusätzlich auf Englisch pflegen.
- **Excel-Export**: „Excel-Export“ rechts in der Reiterleiste. Das Blatt „Abdeckung“ zeigt je Asset BIA-Score, freigegebene Pläne und die letzte Übung und benennt die Lücken – keine BIA, kein

© 2012–2026 WolfInfoSec GmbH

freigegebener Plan, nie geübt, Übung älter als zwölf Monate, letzte Übung nicht bestanden. Dazu je ein Blatt für die BIA (höchster Wert je Dimension und ab welcher Zeitstufe der Schaden erheblich wird), die Notfallpläne (abgelaufene rot) und die Übungen

- **Übungsbericht (PDF)**: in der Detailansicht einer Übung. Kopfdaten und Ergebnis, die Wiederanlaufziele des geübten Assets, die zugehörigen Notfallpläne – ein am Übungstag abgelaufener Plan steht rot –, Teilnehmer, Erkenntnisse, frühere Übungen desselben Assets und ein Freigabeblock

Benutzerrecht: bcm (0 = kein Zugriff, 1 = Lesen, 2 = Bearbeiten) – URL: /bcm

© 2012–2026 WolfInfoSec GmbH

28. REST-API und API-Key-Verwaltung

Beschreibung

WolfISMS stellt eine REST-API bereit, über die externe Systeme Datensätze automatisiert anlegen und abfragen können – ein SIEM meldet Vorfälle, ein Ticketsystem holt offene Maßnahmen ab, eine CMDB gleicht den Assetbestand ab, ein Einkaufssystem meldet Lieferanten, ein Schwachstellenscanner liefert seine Funde ein, ein Reporting-Werkzeug liest Risiken. Der Zugang ist über API-Keys abgesichert, die ausschließlich Administratoren verwalten. Jeder Key wird als SHA-256-Hash gespeichert und ist im Klartext nur einmalig bei der Erstellung sichtbar.

Verfügbarkeit: Die REST-API gehört zum Zusatzpaket „+“ – Essentials Plus und Advanced Plus, erkennbar am „+“ im Kürzel der Lizenz – und zu Enterprise (ENT). In den übrigen Editionen fehlt die Verwaltung der API-Keys, und jeder Aufruf der API endet mit dem Status 403. Vergebene Schlüssel bleiben gespeichert und gelten wieder, sobald eine passende Lizenz eingespielt ist.

Dieses Kapitel gibt den Überblick. Wer eine Anbindung baut, findet die vollständige Beschreibung mit allen Feldern, Filtern und Beispielen im eigenen Dokument „WolfISMS REST-API".

API-Key-Verwaltung (/admin/api_keys)

- **Key anlegen:** Der Administrator gibt eine Beschreibung ein; das System erzeugt einen kryptografisch sicheren 64-stelligen Hex-Key. Dieser wird nur einmalig im Klartext angezeigt und muss sofort kopiert werden
- **Aktivieren / Deaktivieren:** Keys können jederzeit gesperrt und wieder aktiviert werden, ohne sie löschen zu müssen
- **Löschen:** Endgültiges Entfernen eines Keys; danach werden alle Anfragen mit diesem Key abgewiesen
- **Übersicht:** Alle Keys werden mit Beschreibung, Erstellungsdatum und Status tabellarisch dargestellt

Bereiche und Endpunkte

Alle Anfragen müssen den Header X-API-Key mit einem gültigen, aktiven API-Key mitführen. Die sechs Bereiche sind gleich geschnitten; <bereich> steht für incidents, massnahmen, assets, risiken, lieferanten oder schwachstellen.

Endpunkt	Funktion
POST /api/v1/<bereich>	Datensatz anlegen. Die Nummer vergibt das aufrufende System und muss eindeutig sein – nur bei Schwachstellen vergibt WolfISMS sie auf Wunsch selbst
GET /api/v1/<bereich>	Liste abfragen: Filter, Freitextsuche, frei wählbares Datumsfeld, Sortierung und Paginierung über limit und offset. Die Antwort enthält total, count und items
GET /api/v1/<bereich>/<nummer>	Einzelnen Datensatz als JSON abrufen
PATCH /api/v1/<bereich>/<nummer>	Synchronisationsstand quittieren. Fachliche Inhalte lassen sich über die API bewusst nicht ändern – dafür ist die Oberfläche da. Ausgenommen sind die weiteren Besitzer, die sich außer bei Incidents überall pflegen lassen, und die Schwachstellen: dort dürfen zusätzlich Status, Score und Besitzer zurückgeschrieben werden

© 2012–2026 WolfInfoSec GmbH

Endpunkt	Funktion
GET /api/v1/<bereich>/werte	Zulässige Werte laut Stammdaten – für Assets, Risiken, Lieferanten und Schwachstellen. Ein Client sollte sie abfragen, statt sie fest zu hinterlegen

Die API unterliegt keiner Drosselung: ein Sync-Client darf im Sekundentakt lesen und quittieren. Geschützt ist sie allein über den API-Key – deshalb für jedes anbindende System einen eigenen Schlüssel anlegen und nicht mehr benötigte löschen.

Was die Synchronisationsfelder bedeuten.
Jeder Datensatz führt die Felder sync und synctime. sync = 0 heisst „noch nicht übertragen", sync = 1 „übertragen", und leer heisst „nicht für die Übertragung vorgesehen". So merkt sich WolfISMS den Stand, nicht das angebundene System – ein neu aufgesetzter Client verschickt deshalb keine Altlasten erneut.

© 2012–2026 WolfInfoSec GmbH

29. Ziele

Beschreibung

Das Ziele-Modul dokumentiert die Unternehmensziele und die daraus abgeleiteten Informationssicherheitsziele (ISO 27001 Kapitel 5.2 / 6.2) und verfolgt deren Zielerreichung anhand frei definierbarer Kennzahlen (KPIs) mit lückenlosem Verlauf.

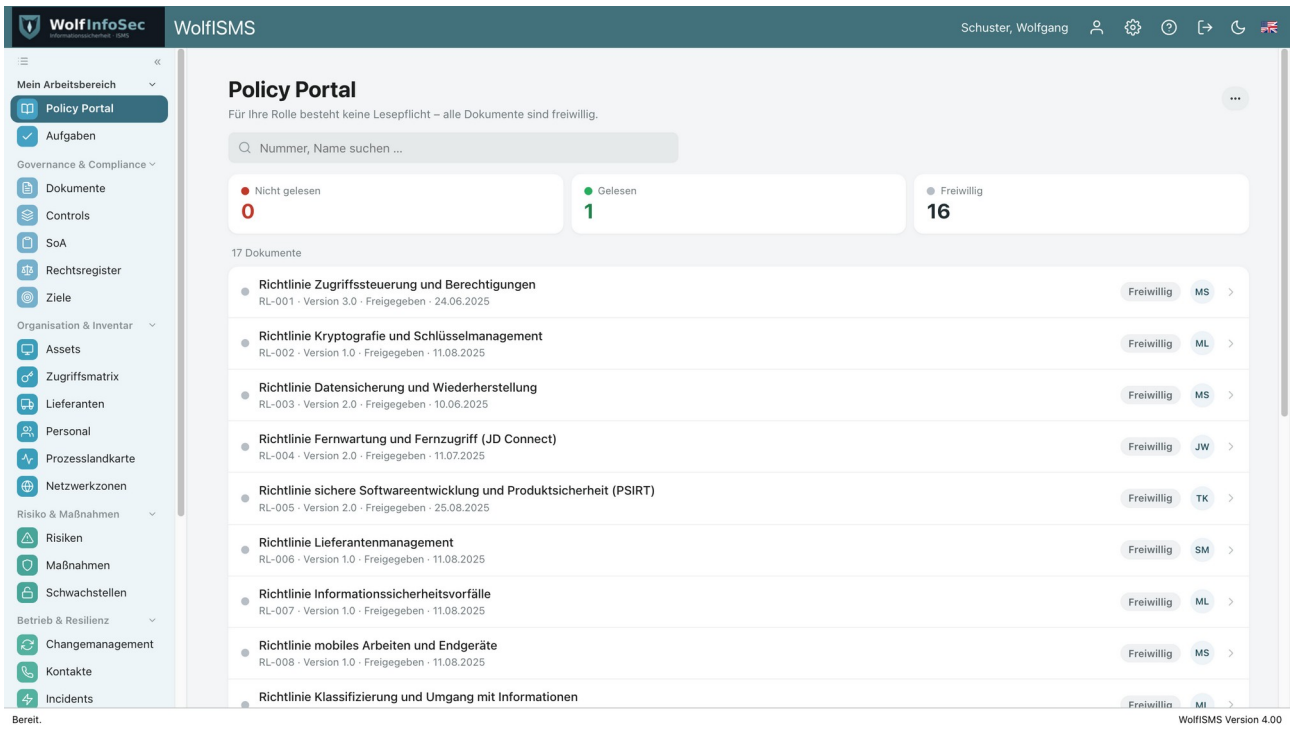
Verfügbarkeit: Das Modul gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt, und der direkte Aufruf endet auf einer Hinweisseite; die erfassten Daten bleiben erhalten und sind nach dem Einspielen einer passenden Lizenz unverändert da. Fehlt das Modul trotz passender Lizenz, hat der Administrator es unter Administration → Module abgeschaltet.

Funktionen

- **Unternehmensziele**: Aufklappbares Freitextfeld für die übergeordneten Unternehmensziele (z. B. Wachstum, Kundenzufriedenheit, Marktposition)
- **Informationssicherheitsziele**: Aufklappbares Freitextfeld für die daraus abgeleiteten Sicherheitsziele (z. B. Verfügbarkeit, Vertraulichkeit, Integrität kritischer Systeme)
- **KPIs anlegen**: Frei definierbare Kennzahlen mit Name, Beschreibung, Einheit, Zielwert und Richtung (höher ist besser / niedriger ist besser)
- **Wert erfassen**: Jeder gemessene Wert wird als neuer Historieneintrag gespeichert und nie überschrieben – der aktuelle Wert ist immer der jüngste Eintrag (lückenloser Audit-Trail)
- **Verlauf**: Liniendiagramm je KPI mit eingezeichneter Zielwert-Linie sowie tabellarischer Werthistorie inkl. Kommentar, Ersteller und Zeitstempel
- **Trendanzeige**: Pfeile zeigen die Entwicklung zum vorherigen Messwert (gestiegen / gesunken / unverändert)
- **Farbcodierung**: Der aktuelle Wert wird grün (Ziel erreicht) oder rot (Ziel verfehlt) hervorgehoben, je nach gewählter Richtung
- **Mehrsprachigkeit**: Separate Felder für die deutsche und englische Anzeige von Zieltexten sowie KPI-Name, -Beschreibung und -Einheit
- **Verwendung in der Managementbewertung**: Die hier gepflegten KPIs erscheinen automatisch im Abschnitt „Erreichung der Informationssicherheitsziele“ der Managementbewertung
- **Kennzahlenbericht**: Zeitraum wählen – vorbelegt sind die letzten zwölf Monate –, dann „Kennzahlenbericht (PDF)“ oder „Excel“. Das PDF enthält die Informationssicherheitsziele, eine Übersicht mit Zielwert, letztem Wert, Anteil der Messungen im Ziel und Trend sowie je KPI das Verlaufsdiagramm und die Werte mit Kommentar; die Excel-Mappe alle Werte des Zeitraums. Phishing-Klickraten oder Schulungsquoten legen Sie als KPI an, dann erscheinen sie im Bericht

Benutzerrecht: ziele (0 = kein Zugriff, 1 = Lesen, 2 = Bearbeiten), das auch Administratoren und Masteruser brauchen – Menü: Governance & Compliance, URL: /ziele

© 2012–2026 WolfInfoSec GmbH



© 2012–2026 WolfInfoSec GmbH

30. Externe Links

Beschreibung

Das Modul Externe Links bietet eine zentrale Sammlung von Verweisen auf externe Systeme, die im Arbeitsalltag häufig benötigt werden, z. B. Ticketsystem, KPI-System oder SharePoint.

Funktionen

- **Linkliste**: Übersicht aller hinterlegten externen Links mit Bezeichnung und Ziel-URL, anklickbar in einem neuen Tab
- **Hinzufügen**: Erfassung neuer Links mit Bezeichnung und URL
- **Löschen**: Entfernen nicht mehr benötigter Links

Benutzerrecht: custom (0 = kein Zugriff, 1 = Zugriff) – URL: /custom

© 2012–2026 WolfInfoSec GmbH

31. Berichte

Beschreibung

Seit v3.90 führt der Menüpunkt „Berichte“ alle Berichte und Exporte des ISMS an einer Stelle zusammen. Die Karten sind nach ihrer Rolle in der ISO/IEC 27001 gegliedert – Managementsystem, Risiken und Maßnahmen, Betrieb und Sicherheitsmaßnahmen, Personal und Awareness – und nennen jeweils den Normbezug. Die Seite erzeugt selbst nichts: Jeder Knopf führt auf den Bericht im zuständigen Modul, wo er auch weiterhin zu finden ist.

Verfügbarkeit: Die Berichtsübersicht gehört zur Edition Advanced (ADV) und zu Enterprise (ENT). In Free und Essentials fehlt der Menüpunkt; die einzelnen Berichte bleiben in ihren Modulen erreichbar.

Übersicht der Berichte

Bericht	Format	Im Modul	Normbezug
Managementbewertung	PDF, PowerPoint	Managementbewertung → Bewertung öffnen	9.3
Auditbericht	PDF	Audit → Audit öffnen	9.2
Kennzahlenbericht	PDF, Excel	Governance & Compliance → Ziele	6.2, 9.1
Umsetzungsstand ISO/IEC 27001, SoA, NIS-2	Seite	Controls	4–10, 6.1.3 d
Risikobericht	PDF, Excel	Risiken	8.2, 8.3
Maßnahmen, Projekte	Excel	Maßnahmen bzw. Projekte	6.1.3, 8.3
Meldefristen	Seite	Incidents	A.5.24–5.26, NIS-2
Sicherheitsvorfälle	Excel	Incidents	A.5.24–5.28
Schwachstellen und Patchstand	Excel	Schwachstellen	A.8.8
Changemanagement	Excel	Changemanagement	A.8.32
BCM, Übungsbericht	Excel, PDF	BCM	A.5.29–5.30
Assets, Zugriffsmatrix, Lieferanten, Rechtsregister, Dokumente	Excel	jeweiliges Modul	A.5.9, A.5.15–5.22, A.5.31, 7.5
Awareness-Bericht	PDF	Personal	7.3, A.6.3
Personal und Lesestatus	Excel	Personal	7.2

Funktionen

- **Nur, was Sie dürfen**: Eine Karte erscheint nur, wenn das Modul eingeschaltet ist, Ihre Lizenz es enthält und Sie das Modulrecht haben – dieselben Regeln wie im Hauptmenü. Gruppen ohne sichtbare Karte entfallen

© 2012–2026 WolfInfoSec GmbH

- **Einzelne Objekte**: Die Karten Auditbericht, Managementbewertung und BCM bieten die jüngsten Audits (PDF und Kurzbericht), Bewertungen (PDF und PowerPoint) und Übungen (Übungsbericht) direkt zur Auswahl an
- **Zeitraum**: Den Zeitraum des Kennzahlenberichts wählen Sie direkt auf der Karte; vorbelegt sind die letzten zwölf Monate
- **Meldefristen**: Die Karte zeigt, wie viele Meldefristen offen und wie viele überfällig sind
- **Filter**: Aus der Berichtsübersicht aufgerufen, sind die Excel-Exporte ungefiltert. Aus der Liste eines Moduls heraus übernehmen sie die dort gesetzten Filter

Hinweise

Ein Bericht zeigt die Daten zum Zeitpunkt, an dem er erzeugt wird; das Erstellungsdatum steht im Kopf. Hat Ihr Administrator ein PDF-Briefpapier hinterlegt, liegt es unter jeder Seite der PDF-Berichte.

© 2012–2026 WolfInfoSec GmbH

32. Administration

Beschreibung

Der Administrationsbereich ermöglicht die vollständige Benutzerverwaltung, Rechtevergabe und Systemüberwachung. Er ist ausschließlich für Benutzer mit admin-Berechtigung zugänglich. Eine ausführliche Beschreibung aller Funktionen enthält die Administrationsdokumentation.

Benutzer und Organisation

- **Admin-Übersicht**: Statistik-Kacheln (Benutzer, Aktivitäten) und Schnelllinks zu allen Unterbereichen
- **Unternehmen**: Unter /admin/unternehmen stehen die Stammdaten der eigenen Organisation – Name, Adresse, Rechtsform, Mitarbeiterzahl, Umsatzklasse, Standorte, Branche und NACE-Code. Sie beschreiben den Kontext der Organisation (ISO/IEC 27001, Kapitel 4); Mitarbeiterzahl und Umsatzklasse bestimmen zusätzlich die Größenklasse nach NIS2. Als einzige Systemeinstellung dürfen diese Angaben auch Masteruser pflegen
- **Alle Benutzer**: Vollständige Benutzerliste mit Suche, Rollen-Reitern, Alphabet-Filter und Berechtigungs-Badges
- **Benutzer anlegen / bearbeiten**: Benutzerrechte, Stammdaten, Sprache und Rollen festlegen. Die Rollen sind eine Mehrfachauswahl – ein Benutzer kann zugleich z. B. Informationssicherheits- und Datenschutzbeauftragter sein
- **Konto aktivieren / deaktivieren**: Ein Konto lässt sich sperren, ohne es zu löschen – gesperrte Benutzer können sich weder per Passwort noch per SSO anmelden
- **Abwesenheit**: Die Abwesenheit mit Vertreter lässt sich auch für einen anderen Benutzer eintragen – über die Benutzerliste
- **Benutzer importieren**: Benutzerstammdaten aus einer Datei übernehmen
- **Passwort-Reset**: Passwort eines Benutzers durch einen Administrator zurücksetzen
- **Abteilungen und Teams**: Unter /admin/abteilungen werden Abteilungen und Teams zentral gepflegt – mit Leitung und Über-/Unterordnung. Alle Module wählen die Abteilung anschließend aus dieser Liste aus, statt sie frei einzutippen
- **Organigramm**: Die Schaltfläche „Grafische Ansicht" in der Abteilungsverwaltung öffnet das Organigramm – dieselben Daten als Baum. Kästen lassen sich per Ziehen umhängen, ein Klick öffnet Name, Leitung, übergeordnete Abteilung, Beschreibung und Farbe. Die Wurzel ist der Unternehmensname aus den Unternehmensangaben. Ausgeben lässt sich die Grafik als PNG oder SVG oder direkt drucken
- **Abteilungen als Excel**: Die Abteilungsliste lässt sich als Mappe herunterladen und wieder einlesen – mit übergeordneter Abteilung und Leitung im Klartext, damit sich die Mappe auch von Hand erweitern lässt. Der Import löscht nie, rät nie und schreibt erst nach der Vorschau mit gesetztem Häkchen
- **Prozesslandkarte und Netzwerkzonen**: Zwei weitere grafische Sichten, seit v4.00 als Menüpunkte in der Gruppe Organisation & Inventar. Den Zugriff regeln die Rechte prozesslandkarte und netzwerkzonen (1 = Lesen, 2 = Bearbeiten), die auch Administratoren und Masteruser brauchen. Die Prozesslandkarte ordnet die Prozesse in Führungs-, Kern- und Unterstützungsprozesse, die Netzwerkzonen zeigen die Netzsegmentierung von den externen Netzen über DMZ, interne Netze und OT bis zur Hochsicherheitszone; die Bänder beider Karten passt der Administrator unter Administration → Kategorien an. Beide arbeiten wie das Organigramm: ziehen, klicken, als PNG oder SVG ausgeben. Verantwortliche, Abteilung und ein verknüpftes Dokument (Prozessbeschreibung bzw. Netzkonzept) stehen im Seitenpanel
- **Pläne & Register**: Ablage für Netzwerkpläne und Prozessdarstellungen (PNG, PDF, draw.io) sowie das Assetregister als Tabelle – für Administratoren und Master-Benutzer, erreichbar über die Kachel im Adminbereich

© 2012–2026 WolfInfoSec GmbH

- **Aktivitätsprotokoll**: Vollständiges Protokoll aller Systemaktivitäten; Filter nach Bereich und Benutzer
- **Excel-Exporte**: Benutzerliste mit Berechtigungen sowie das Aktivitätsprotokoll als .xlsx

Kataloge und Stammdaten

- **Stammdaten**: Verwaltung von Dropdown-Werten (Status, Typen, Kategorien)
- **Kategorien:** Unter Administration → Kategorien pflegt der Administrator auf einer Seite die Kategorien von Incidents, Changemanagement, Rechtsregister und Kontakten (Dienstleister) sowie die Bänder von Prozesslandkarte und Netzwerkzonen: anlegen, umbenennen (deutsch und englisch, bei den Bändern und im Rechtsregister auch die Farbe), sortieren und löschen. Eine Kategorie, die noch verwendet wird, lässt sich nicht löschen; eine umbenannte Kategorie ändert sich in allen Einträgen mit. Asset-, Risiko-, Bedrohungs- und Schwachstellenkategorien erreichen Sie über Reiter derselben Seite, gepflegt werden sie weiter in ihren eigenen Masken
- **Bedrohungen & Schwachstellen**: Pflege der Kataloge, aus denen im Risikomodul bei der Verknüpfung eines Risikos ausgewählt wird
- **Auswirkung / Risikoskala**: Konfiguration der Bezeichnungen und Beschreibungen der 5-stufigen Auswirkungsskala
- **Asset-Kategorien**: Pflege der OBASHI-Kategorien des Assetmanagements
- **Risiko-Kategorien**: Pflege der Kategorienliste des Risikomoduls
- **Lieferantentypen**: Pflege der Typenliste des Lieferantenmoduls; ein Häkchen kennzeichnet Cloud-/SaaS-Typen, deren Lieferanten eine Cloud-Exit-Strategie brauchen
- **Risikoparameter**: Konfiguration der Scoring-Gewichte und Schwellenwerte für die automatische Lieferantenrisikobewertung
- **Rollen**: Unter /admin/rollen werden die unternehmensweiten Rollen angelegt, umbenannt und den Benutzern zugewiesen; die Liste zeigt zu jeder Rolle auch, wer sie innehat. Es ist dieselbe Rollenliste wie im Rollenkatalog der Zugriffsmatrix (/zugriffsmatrix/rollen) – dort stehen zusätzlich Kürzel, Aktiv-Kennzeichen und die übrigen Katalogfelder. Eine Rolle, die noch verwendet wird, lässt sich nicht löschen. Die Kachel steht auch Master-Benutzern offen
- **Lesepflicht-Matrix**: Welche Rolle welches freigegebene Dokument lesen muss, legt der Master-Benutzer im Policy Portal unter „Lesepflicht-Matrix" fest. Ein neu freigegebenes Dokument hat zunächst keine Lesepflicht – sie wird einmal bewusst gesetzt. Ohne Zuordnung bleibt das Dokument im Portal sichtbar, löst aber weder Aufgaben noch Erinnerungsmails aus

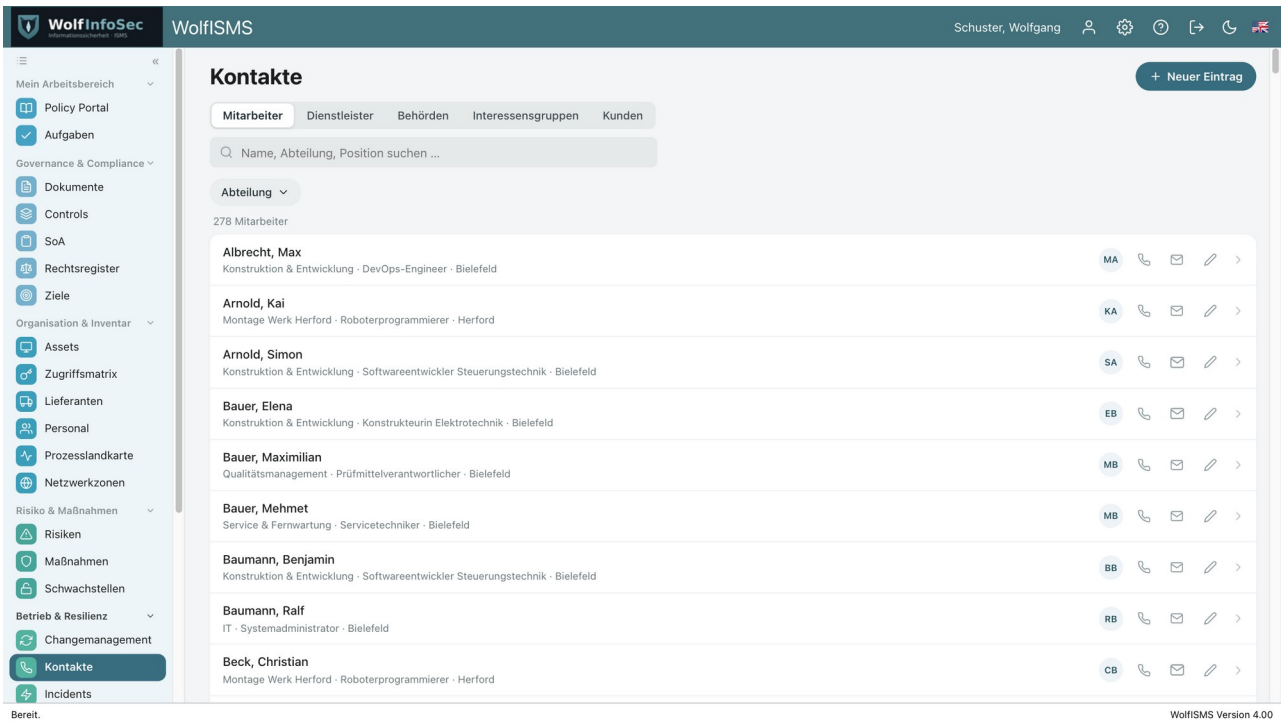
System und Betrieb

- **E-Mail / SMTP**: Konfiguration des ausgehenden Mailservers für Aufgaben-E-Mails und Benachrichtigungen; Test-Mail-Funktion
- **Single Sign-On**: Unter /admin/sso lassen sich die Anmeldung über Microsoft Entra ID und über Google einrichten – Zugangsdaten, zugelassene E-Mail-Domains und die Frage, ob unbekannte Benutzer automatisch als Nur-Lese-Konto angelegt werden. Ein Schalter am Kopf der Maske entscheidet, ob diese Werte gelten oder die aus der Serverkonfiguration. „Speichern & Discovery prüfen" testet die Verbindung zum Anbieter; ein Neustart ist nicht nötig
- **Cron-Zeiten**: Festlegung von Uhrzeit und Rhythmus der Hintergrund-Jobs (Aufgaben-Erinnerung, Risikoscore-Snapshot). Jeder Job lässt sich auch sofort manuell anstoßen
- **Backup & Restore**: Download eines kombinierten Backups (.tar.gz) aus Datenbank-Dump und hochgeladenen Dateien; Wiederherstellung per Upload. Vor einer Dateien-Wiederherstellung wird der bisherige Uploads-Ordner automatisch als Zeitstempel-Kopie gesichert

© 2012–2026 WolfInfoSec GmbH

- **Updates**: Prüft die eingebundenen JavaScript-Bibliotheken – Editor und BPMN-Modeler – und aktualisiert sie. Neue WolfISMS-Versionen spielt seit v4.00 der Betreiber der Installation ein, nicht mehr die Anwendung selbst. In containerisierten Installationen nicht verfügbar
- **Framework-Import**: Import von Framework-Kapiteln aus CSV/JSON sowie Direktinstallation aus einem Online-Framework-Katalog; bereits vorhandene Frameworks werden automatisch erkannt
- **Daten SQL-Export/Import**: Export und Import der Stammdaten von Dokumenten, Risiken und Maßnahmen zwischen WolfISMS-Instanzen – einzeln oder als Komplettpaket. Importierte Datensätze werden auf einen frischen Bearbeitungsstand zurückgesetzt; Anhänge, Historien und Verknüpfungen werden nicht übertragen
- **Module**: Unter /admin/module lässt sich jedes Fachmodul einzeln ein- und ausschalten und die Reihenfolge innerhalb seiner Menügruppe per Ziehen oder über die Pfeiltasten festlegen; die Gruppe steht in jeder Zeile. Ein ausgeschaltetes Modul verschwindet aus dem Menü, seine Seiten und sein REST-Bereich sind gesperrt; die erfassten Daten bleiben erhalten und sind nach dem Wiedereinschalten unverändert da. Das Policy Portal lässt sich nicht abschalten, weil readonly-Benutzer sonst kein Ziel mehr hätten
- **2FA / TOTP**: Systemweite Zwei-Faktor-Authentifizierung aktivieren oder deaktivieren
- **KI-Einstellungen**: Konfiguration der KI-Unterstützung für die KI-Assistenten aller Fachmodule, die KI-Übersetzung und den Word-Import: Anbieter (Anthropic, OpenAI, Mistral, Google Gemini, nele.ai, Azure OpenAI, Microsoft Copilot oder ein OpenAI-kompatibler Dienst), Modell, API-Key – bei Azure OpenAI und Copilot wahlweise die Anmeldung über Microsoft Entra ID –, Basis-URL und optionaler Prompt-Zusatz. KI-Funktionen stehen in jeder bezahlten Edition zur Verfügung; in der freien Version ist der Bereich gesperrt
- **Design & Farben**: Farbschema der Oberfläche unter /admin/design – Petrol (Standard), Klassisch mit den Originalfarben oder seit v4.00 Schwarz / Grau / Weiß. Dazu kommen der Dunkelmodus als Vorgabe (jeder Benutzer kann selbst umschalten), die Farbe der Kopfleiste und der Schalter für die Infokacheln über den Modullisten, Vorgabe ausgeblendet. Die Einstellung gilt für alle Benutzer; Excel-, Word- und PDF-Exporte bleiben davon unberührt, ebenso Risikomatrix, Kacheln der Risikostufen und Score-Tachos, die immer grün bis rot zeigen
- **Branding**: Hochladen des eigenen Firmenlogos (PNG), einer Word-Vorlage für Exporte sowie eines PDF-Briefpapiers für den Dokumenten-Export
- **Ticketsystem**: URL-Vorlage, über die die Nummer eines Vorfalls in das Ticketsystem verlinkt
- **Lizenz**: Hochladen einer Lizenzdatei (*.lic)
- **Adminhandbuch**: Download der Administrationsdokumentation als PDF direkt aus der Anwendung
- **About**: Version, Lizenz und Lizenzbestimmungen der Installation – seit v4.00 eine Kachel unter System und Betrieb statt des Logos oben rechts
- **Zurück zur Übersicht**: Über jeder Seite der Administration führt „‹ Administration“ zur Übersicht zurück

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
Mein Arbeitsbereich
Policy Portal
Aufgaben
Governance & Compliance
Dokumente
Controls
SoA
Rechtsregister
Ziele
Organisation & Inventar
Assets
Zugriffsmatrix
Lieferanten
Personal
Prozesslandkarte
Netzwerkzonen
Risiko & Maßnahmen
Risiken
Maßnahmen
Schwachstellen
Betrieb & Resilienz
Changemanagement
Kontakte
Incidents
Kontakte
+ Neuer Eintrag
Mitarbeiter
Dienstleister
Behörden
Interessensgruppen
Kunden
Name, Abteilung, Position suchen ...
Abteilung
278 Mitarbeiter
Albrecht, Max
Konstruktion & Entwicklung · DevOps-Engineer · Bielefeld
MA
Arnold, Kai
Montage Werk Herford · Roboterprogrammierer · Herford
KA
Arnold, Simon
Konstruktion & Entwicklung · Softwareentwickler Steuerungstechnik · Bielefeld
SA
Bauer, Elena
Konstruktion & Entwicklung · Konstrukteurin Elektrotechnik · Bielefeld
EB
Bauer, Maximilian
Qualitätsmanagement · Prüfmittelverantwortlicher · Bielefeld
MB
Bauer, Mehmet
Service & Fernwartung · Servicetechniker · Bielefeld
MB
Baumann, Benjamin
Konstruktion & Entwicklung · Softwareentwickler Steuerungstechnik · Bielefeld
BB
Baumann, Ralf
IT · Systemadministrator · Bielefeld
RB
Beck, Christian
Montage Werk Herford · Roboterprogrammierer · Herford
CB
Bereit.
WolfISMS Version 4.00

33. Häufige Fragen (FAQ)

Ich sehe ein Modul nicht – was ist zu tun?

Wenn ein Modul im Navigationsmenü fehlt oder Sie eine „Keine Berechtigung“-Meldung erhalten, fehlt Ihnen das entsprechende Recht. Wenden Sie sich an Ihren Systemadministrator, der Ihnen das Recht unter /admin/change_user zuweisen kann. Ein Administrator kann ein Modul außerdem unter Administration → Module ganz abschalten; dann fehlt es im Menü aller Benutzer, die erfassten Daten bleiben aber erhalten. Möglich ist außerdem, dass die Edition der Lizenz das Modul nicht enthält: Ziele, Personal, Kontakte, Berichte, Projekte, Operational Plan, Audit, Managementbewertung, Schwachstellen, Rechtsregister, Playbooks, BCM und die Zugriffsmatrix gehören zur Edition Advanced, die REST-API zum Zusatzpaket „+“, und die KI-Funktionen setzen eine bezahlte Edition voraus. In diesem Fall zeigt der direkte Aufruf der Seite einen Hinweis auf die nötige Edition.

Zugeklappte Gruppe: Bevor Sie Ihren Administrator fragen, prüfen Sie, ob die Gruppe des Moduls im Menü zugeklappt ist – dann steht nur ihre Überschrift da. Ein Klick darauf öffnet sie wieder.

Ich kann plötzlich nichts mehr speichern – woran liegt das?

Das hat in der Regel eine von zwei Ursachen: Entweder wurde Ihrem Konto das Recht readonly zugewiesen, oder die Systemlizenz ist abgelaufen. Im zweiten Fall bleiben alle Module lesbar, aber sämtliche Schaltflächen zum Speichern sind gesperrt, bis der Administrator eine gültige Lizenz einspielt. Betrifft die Sperre dagegen nur das Anlegen neuer Assets, Risiken, Dokumente oder Lieferanten, ist die Mengengrenze der freien Version erreicht – siehe die folgende Frage.

Kann ein Eintrag mehrere Besitzer haben?

Ja. In Risiken, Assets, Dokumenten, Maßnahmen, Projekten, Controls, Lieferanten, Incidents, Schwachstellen und Changes kreuzen Sie im Feld „Besitzer“ (bzw. „Verantwortlich“) mehrere Personen an. Jede davon darf den Eintrag bearbeiten und wird an fällige Aufgaben erinnert.

Warum kann ich keinen weiteren Eintrag mehr anlegen?

Läuft WolfISMS ohne Lizenzdatei, also in der freien Version, sind Assets, Risiken, Dokumente und Lieferanten auf je zehn Einträge begrenzt. Ist die Grenze erreicht, lässt sich die Maske für einen neuen Eintrag nicht mehr öffnen und die Anwendung meldet: Die freie Version ist auf 10 Assets begrenzt. Alles bereits Erfasste bleibt sichtbar, änderbar und exportierbar – gesperrt ist nur das Anlegen.

Sie haben zwei Möglichkeiten: einen nicht mehr benötigten Eintrag löschen, dann ist der Platz sofort wieder frei, oder Ihren Administrator um eine bezahlte Lizenz bitten – damit entfällt die Grenze. Bei Dokumenten zählen übrigens die Dokumentennummern: eine neue Version eines vorhandenen Dokuments dürfen Sie auch dann noch anlegen, wenn die zehn erreicht sind.

Wie ändere ich mein Passwort?

Klicken Sie oben rechts auf Ihren Namen und wählen Sie „Passwort ändern“. Das neue Passwort muss mindestens 10 Zeichen haben und Groß- und Kleinbuchstaben sowie eine Ziffer enthalten. Melden Sie sich über Microsoft oder Google an, verwalten Sie Ihr Passwort dort und nicht in WolfISMS.

© 2012–2026 WolfInfoSec GmbH

Was bedeutet „Read Only“?

Benutzer mit readonly-Berechtigung können die für sie sichtbaren Inhalte über das Policy Portal lesen, aber keine Daten erstellen, bearbeiten oder löschen. Alle Speichern- und Bearbeiten-Schaltflächen sind ausgeblendet.

Wie exportiere ich Daten nach Excel?

Jede Modulliste hat oben rechts ein Drei-Punkte-Menü mit dem Eintrag Export. Der Export enthält die aktuell gefilterte Ansicht als .xlsx-Datei, die direkt in Microsoft Excel geöffnet werden kann.

Wie funktioniert der Dokumenten-Workflow?

Dokumente durchlaufen drei Stufen: (1) In Arbeit – wird vom Besitzer bearbeitet. (2) Zu prüfen – ein Prüfer bestätigt den Inhalt. (3) Freigegeben – der Freigebende erteilt die formale Freigabe. Eine neue Version setzt den Prozess wieder auf „In Arbeit“ zurück. Jedes Speichern hält dabei eine eigene Fassung fest; die freigegebene Version bleibt daneben stehen, bis die neue freigegeben ist.

Wie komme ich an eine frühere Fassung eines Dokuments?

Öffnen Sie das Dokument und sehen Sie rechts unter „Versionen" nach: Dort steht jede Fassung mit Nummer, Status und Datum, ein Klick öffnet sie. Wollen Sie mit einer alten Fassung weiterarbeiten, wählen Sie „Wiederherstellen" – ihr Inhalt wird dann als neuer Arbeitsstand übernommen und durchläuft Prüfung und Freigabe wie gewohnt. Gelöscht oder überschrieben wird dabei nichts.

Wie übernehme ich ein Word-Dokument?

Legen Sie ein neues Dokument an oder öffnen Sie ein vorhandenes zum Bearbeiten. Über dem Formular steht der Kasten „Aus Word übernehmen“: Datei hineinziehen oder auswählen, „Übernehmen“ – der Inhalt steht danach im Editor, samt Überschriften, Listen, Tabellen und Bildern. Prüfen Sie ihn und speichern Sie dann; vorher steht nichts in der Datenbank. Ist die KI eingeschaltet, bereitet sie den Text auf Wunsch gleich auf. Gelesen werden .docx-Dateien bis 16 MB – ältere .doc-Dateien bitte in Word zuerst umwandeln.

Was ist eine Lesebestätigung und wo bestätige ich sie?

Für Richtlinien kann eine Lesebestätigung verlangt werden. Die betreffenden Dokumente erscheinen in Ihren offenen Aufgaben und im Policy Portal. Öffnen Sie das Dokument im Portal und klicken Sie auf „Gelesen“ – Datum und Bestätigung werden gespeichert und im Personalmodul als Nachweis geführt. Wird ein Dokument inhaltlich überarbeitet, kann ein Master-Benutzer den Lesestatus zurücksetzen; dann ist eine erneute Bestätigung erforderlich. Seit v3.71 hängt die Lesepflicht an Ihrer Rolle: Pflicht sind nur die Dokumente, die Ihrer Rolle zugeordnet sind – alle übrigen tragen im Portal die Kennzeichnung „Freiwillig" und zählen weder in den Fortschritt noch in Ihre Aufgaben oder die Erinnerungsmails. Welche Rollen Sie haben, pflegt der Administrator; welche Rolle was lesen muss, der Master-Benutzer in der Lesepflicht-Matrix.

Wozu dient die Zugriffsmatrix und wie oft muss ich sie prüfen?

Die Zugriffsmatrix hält fest, welche Rolle auf welches Asset zugreifen darf, wer das genehmigt hat und wann die Berechtigung zuletzt überprüft wurde. Die Prüffrequenz legen Sie je Berechtigung selbst fest (vierteljährlich, halbjährlich oder jährlich). Fällige und überfällige Prüfungen werden farblich gekennzeichnet; die Listenansicht mit dem Filter „privilegiert“ zeigt zuerst die kritischen Fälle.

© 2012–2026 WolfInfoSec GmbH

Warum ist meine Zugriffsmatrix leer?

Die Matrix wird aus zwei Quellen gebildet: den nicht archivierten sekundären Assets (primäre erst über „Primäre Assets einblenden“) und den aktiven Rollen. Fehlt eine der beiden Seiten, bleibt die Ansicht leer. Prüfen Sie, ob im Assetmanagement Assets der gewählten Kategorie vorhanden sind und ob im Rollenkatalog Rollen als „aktiv“ markiert sind.

Kann ich BPMN-Diagramme aus anderen Tools importieren?

Ja. Im BPMN-Editor finden Sie den Button „Importieren“. Unterstützt werden .bpmn- und .xml-Dateien aus gängigen BPMN-Tools wie Camunda Modeler, draw.io oder Signavio. Der Import erfolgt direkt im Browser.

Wie werden Lieferantenrisiken berechnet?

Der Risikoscore wird automatisch aus mehreren Faktoren berechnet: Verarbeitung personenbezogener Daten, Vertragsstand, Zertifizierungen, Sicherheitsniveau, Schadenspotenzial, Eintrittswahrscheinlichkeit und Tier-Kritikalität. Seit v4.01 zählt das Tier in der Schadenshöhe doppelt und setzt eine Untergrenze – ein missionskritischer Lieferant landet damit nicht mehr auf „niedrig“, nur weil er keine Personendaten verarbeitet. Der Score fließt in die Lieferanten-Risikomatrix auf dem Dashboard ein; jede Neuberechnung wird in der Score-Historie festgehalten.

Wie richte ich die Zwei-Faktor-Authentifizierung (2FA) ein?

Wenn der Administrator 2FA systemweit aktiviert hat, werden Sie beim nächsten Login automatisch zum Einrichten aufgefordert. Sie können 2FA auch manuell starten: Klicken Sie oben rechts auf Ihren Namen und wählen Sie „2FA einrichten“. Scannen Sie den angezeigten QR-Code mit einer TOTP-App und bestätigen Sie mit dem generierten 6-stelligen Code. Um 2FA zu deaktivieren, wählen Sie „2FA deaktivieren“ im selben Menü.

Wie arbeite ich mit dem KI-Assistenten für Dokumente?

Die KI muss Ihr Administrator freischalten und Ihnen das Recht „KI-Nutzung“ geben; sie setzt eine bezahlte Edition voraus, also mindestens Essentials. Dann steht in der Dokumentenliste und in der Detailansicht der Knopf „KI-Assistent“. Sagen Sie im Gespräch, was Sie vorhaben – ein neues Dokument erstellen, eine Vorlage hochladen und übernehmen, ein Dokument überarbeiten oder prüfen. Den Entwurf rechts können Sie jederzeit selbst ändern; gespeichert wird er erst mit „Übernehmen“, als neue Fassung im Entwurf. Freigegebene Dokumente bleiben unberührt, bis Sie eine neue Version anlegen.

Warum kann ich einen Anhang nicht hochladen?

Anhänge müssen echte PDF-Dateien sein und dürfen 16 MB nicht überschreiten. Eine Datei, die nur die Endung .pdf trägt, aber intern ein anderes Format hat, wird abgelehnt. Speichern Sie das Dokument in diesem Fall erneut als PDF.

Welche KI-Assistenten gibt es?

Seit v4.00 hat jedes Fachmodul einen: Risiken, Assets, Lieferanten, Dokumente, Maßnahmen, Schwachstellen, Changes, Incidents, Projekte, Controls, Rechtsregister, Datenschutz, Audits und Playbooks. Alle sind gleich aufgebaut – ein Gespräch auf einer eigenen Seite, links der Chat, rechts der Entwurf – und erreichbar über den Knopf „KI-Assistent“ in der Liste und in der Detailansicht. Was der jeweilige Assistent kann, steht im Kapitel des Moduls. Er braucht dasselbe Recht wie das Bearbeiten im Modul und dazu das Recht „KI-Nutzung“, und nichts wird ohne Ihre Bestätigung gespeichert.

© 2012–2026 WolfInfoSec GmbH

Welche Daten verlassen dabei das System?

Die Angaben, um die es gerade geht – etwa das Risiko, das Dokument oder der Vorfall –, dazu Auszüge aus den Katalogen, die für den jeweiligen Schritt gebraucht werden, und der bisherige Gesprächsverlauf. Kataloge werden gekürzt und nach Thema vorsortiert. Ob und mit welchem Anbieter die KI überhaupt arbeitet, entscheidet Ihr Administrator.

Was macht die KI bei Assets und Gap-Assessments?

Der KI-Assistent für Assets legt mit Ihnen neue Assets an, schlägt Schutzbedarf und Wiederanlaufziele mit Begründung vor und findet Verknüpfungen bis hin zu den Risiken; er prüft auch einzelne Assets, eine OBASHI-Ebene oder den Gesamtbestand. Im Audit formuliert der KI-Assistent zu jeder Anforderung Prüffragen. Jeder KI-Dialog weist darauf hin, dass KI-generierte Angaben vor der Verwendung zu prüfen sind – für ihre Richtigkeit und Vollständigkeit wird keine Gewähr übernommen.

Warum sehen die Farben der Oberfläche anders aus als früher?

Seit v4.00 hat WolfISMS ein neues Erscheinungsbild – ruhigere Listen, schlichte graue Knöpfe und Symbole statt bunter Bilder (siehe „Die Oberfläche seit v4.00“). Außerdem kann Ihr Administrator unter „Design & Farben“ ein Farbschema für die ganze Installation festlegen: Petrol, Klassisch oder Schwarz / Grau / Weiß. Hell oder dunkel wählen Sie selbst über den Knopf neben der Sprachflagge. Risikomatrix, die Kacheln der Risikostufen und die Score-Tachos behalten immer ihre Farben von grün bis rot, Excel-, Word- und PDF-Exporte ebenso.

Wer bekommt meine Aufgaben, wenn ich abwesend bin?

Der Vertreter, den Sie unter „Abwesenheit pflegen“ auf Ihrer Kontoseite für den Zeitraum eintragen. Er sieht Ihre Aufgaben unter „Meine Aufgaben“ und bekommt Ihre Erinnerungsmails; nach dem Ende fällt alles von allein zurück. Ohne eingetragene Abwesenheit bleiben die Aufgaben bei Ihnen.

Wo trage ich RTO, RPO und MAZ ein?

Am Asset: im Bearbeitungsformular unter „Wiederanlaufziele“. Die Werte werden aus festen Stufen gewählt, und die RTO darf die MAZ nicht übersteigen. Die BIA im BCM-Modul zeigt sie für das bewertete Asset an. Eine eigene Prozessliste im BCM gibt es seit v3.84 nicht mehr.

Wo finde ich die Berichte für das Audit?

Im Menüpunkt „Berichte“. Er zeigt alle Berichte und Exporte, auf die Sie Zugriff haben, mit ihrem Bezug zur ISO/IEC 27001 – vom Auditbericht über die Managementbewertung bis zum Awareness-Bericht.

Warum passiert nichts, wenn ich eine Aktion im neuen Tab öffne?

Seit v3.93 führt WolfISMS Links, die Daten ändern – Verknüpfen und Lösen, Kontakte löschen, die Lesebestätigung im Policy Portal, Lieferantenaktionen, den Behandlungsplan –, nur noch als abgesicherte Formularanfrage aus. So kann kein Link auf einer fremden Webseite eine Änderung in Ihrem Namen auslösen. Ein gewöhnlicher Klick funktioniert wie bisher. Öffnen Sie eine solche Aktion dagegen mit der mittleren Maustaste oder Strg-Klick in einem neuen Tab, erscheint nur ein Hinweis – klicken Sie den Link dann im ursprünglichen Tab an.

Warum zeigt die Seitenleiste nur fünf Einträge?

Damit lange Listen die übrigen Abschnitte nicht nach unten schieben. Seit v3.94 zeigt jeder Abschnitt mit „Verwalten“ höchstens fünf Einträge, darunter „mehr … (+N)“. Der Link öffnet die

© 2012–2026 WolfInfoSec GmbH

Verknüpfungsansicht mit allen Einträgen. Dürfen Sie die Verknüpfungen nicht ändern, sehen Sie die Liste vollständig.

Warum steht eine Verknüpfung auch beim anderen Eintrag?

Gespeichert wird eine Verknüpfung bei dem Eintrag, an dem sie angelegt wurde. Seit v3.94 zeigt auch die Gegenseite sie an – etwa den Change am Asset oder DOK0001 bei DOK0002, wenn DOK0001 auf DOK0002 verweist. Ändern lässt sie sich beim anlegenden Eintrag; nur zwischen zwei Dokumenten können Sie sie von beiden Seiten lösen.

Wie lasse ich ein Dokument ins Englische übersetzen?

Stellen Sie die Oberfläche auf Englisch und öffnen Sie das Dokument. In der Detailansicht steht dann die Schaltfläche „AI translation“. Die KI übersetzt den deutschen Text Abschnitt für Abschnitt; Überschriften, Tabellen und Bilder bleiben, wie sie sind. Sie sehen Deutsch und Englisch nebeneinander und übernehmen das Ergebnis mit einem Klick – dabei entsteht eine neue Version. Die Schaltfläche fehlt, solange das Dokument keinen deutschen Text hat, freigegeben oder in Prüfung ist.

Wo sind die Schaltflächen zum Verknüpfen geblieben?

Seit v3.95 verknüpfen Sie über die Seitenleiste: Jeder Abschnitt dort – Controls, Risiken, Maßnahmen und so weiter – hat den Link „Verwalten“, wenn Sie die Verknüpfungen ändern dürfen. Die gleichlautenden Schaltflächen in der Leiste über dem Inhalt führten auf dieselben Seiten und sind deshalb entfallen.

Warum hat nicht jedes Feld ein ⓘ?

Erklärt werden Felder, deren Bedeutung nicht schon aus der Beschriftung hervorgeht. Such- und Filterfelder haben grundsätzlich keines.

Mein Konto ist gesperrt – was nun?

Nach zehn falschen Passwörtern sperrt WolfISMS die Anmeldung für dieses Konto 15 Minuten lang; die Meldung nennt die Restzeit. Danach geht es ohne Zutun weiter. Wer sein Passwort nicht mehr weiß, nutzt in der Zwischenzeit „Passwort vergessen“ auf der Anmeldeseite. Die Anmeldung über Microsoft oder Google ist von der Sperre nicht betroffen.

Wie schalte ich den Dunkelmodus ein?

Mit dem Knopf oben rechts neben der Sprachflagge: der Mond schaltet auf dunkel, die Sonne zurück auf hell. Die Wahl wird an Ihrem Konto gespeichert und gilt auf jedem Gerät. Haben Sie nie umgeschaltet, gilt die Vorgabe Ihres Administrators.

Wo sind die Kacheln über den Listen geblieben?

Die Statistik- und Kategoriekacheln über den Modullisten sind seit v4.00 zunächst ausgeblendet, damit die Liste selbst im Vordergrund steht. Ihr Administrator kann sie unter Design & Farben für alle wieder einschalten. Gefiltert wird weiter über die Kacheln mit Zahlen und die Filter direkt über der Liste.

Warum kann ich in den Listen nicht mehr blättern?

Seit v4.00 zeigt jede Liste alle Einträge auf einer Seite. Tippen Sie ins Suchfeld: die Liste filtert sofort, und jedes eingegebene Wort muss im Eintrag vorkommen.

© 2012–2026 WolfInfoSec GmbH

Wie schreibe ich ein Playbook?

Öffnen Sie Playbooks und klicken Sie oben rechts auf „Neues Playbook“. Titel, Beschreibung und Text tragen Sie im selben Editor ein wie bei Dokumenten; mit „Speichern“ steht das Playbook in der Liste unter „Geschriebene Playbooks“. Dafür brauchen Sie das Recht Playbooks. PDF-Dateien hochladen und Links setzen geht weiter wie bisher.

Warum sehe ich das Modul Datenschutz nicht?

Das Recht „Datenschutz“ ist für jeden Benutzer zunächst aus, auch nach dem Update. Ihr Administrator gibt Ihnen Lesen oder Bearbeiten; danach steht „Datenschutz“ im Menü unter Governance & Compliance.

Wer pflegt den AVV eines Lieferanten?

Wer das Recht „Datenschutz“ mit Bearbeiten hat – das Lieferanten-Recht reicht dafür nicht und ist dafür auch nicht nötig. So kann der Datenschutzbeauftragte die AVV-Angaben pflegen, ohne die übrigen Lieferantendaten zu ändern. Der Block erscheint, sobald beim Lieferanten „Personendaten“ auf Ja oder Teilweise steht.

© 2012–2026 WolfInfoSec GmbH

34. Glossar

Begriff	Bedeutung
API-Key	Kryptografischer Zugriffsschlüssel für die REST-API; wird als SHA-256-Hash gespeichert und nur einmalig im Klartext angezeigt
Asset	Informationsverarbeitendes System, Anwendung oder Information mit Wert für das Unternehmen
Audit	Systematische Überprüfung der Umsetzung von ISMS-Anforderungen
AVV	Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO zwischen Verantwortlichem und Auftragsverarbeiter (Lieferant)
Backup	Kombiniertes Sicherungsarchiv (.tar.gz) aus Datenbank-Dump und hochgeladenen Dateien
BCM	Business Continuity Management – systematisches Management zur Aufrechterhaltung geschäftskritischer Prozesse im Krisenfall (ISO 22301 / ISO 27001)
BIA	Business Impact Analyse – Bewertung der Auswirkungen eines Ausfalls eines Assets auf Finanzen, Betrieb, Reputation und Compliance über verschiedene Zeitschritte
BPMN	Business Process Model and Notation – standardisierte Prozessmodellierungssprache
Break-Glass	Notfallzugriff über ein versiegeltes Konto, das nur nach einem dokumentierten Notfallverfahren aktiviert wird (Stufe N der Zugriffsmatrix)
Change	Änderungsantrag (auch RfC) für eine Änderung an Systemen oder Konfigurationen; wird im Gremium freigegeben und nach der Umsetzung nachbetrachtet (ISO 27001 A.8.32)
CIA	Confidentiality, Integrity, Availability – Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit)
CRA	Cyber Resilience Act – EU-Verordnung für Cybersicherheit vernetzter Produkte
Deny-by-default	Grundprinzip der Zugriffsmatrix: Ohne ausdrückliche Festlegung besteht kein Zugriff; jede Abweichung ist zu begründen und zu genehmigen
DSFA	Datenschutz-Folgenabschätzung nach Art. 35 DSGVO – Bewertung der Risiken einer Verarbeitung für die Betroffenen, wenn die Schwellwertanalyse sie verlangt
DSGVO	Datenschutz-Grundverordnung – EU-Verordnung zum Schutz personenbezogener Daten
Incident	Sicherheitsvorfall – tatsächliche oder potenzielle Verletzung der Informationssicherheit
ISMS	Informations-Sicherheits-Management-System – systematisches Rahmenwerk zur Steuerung der Informationssicherheit
ISO 27001	Internationaler Standard für ISMS (Ausgabe 2022)
KI-Bearbeitung	früherer Knopf im Dokumentenmodul; seit v4.00 übernimmt das der KI-Assistent für Dokumente. Die KI-Assistenten der Fachmodule brauchen einen vom Administrator aktivierten KI-Anbieter
Kommentare	Diskussionsfunktion je Eintrag in Assets, Lieferanten, Risiken, Dokumenten, Maßnahmen, Incidents und Controls; Bearbeiten und Löschen nur durch Ersteller oder Admin
KPI	Key Performance Indicator – frei definierbare Kennzahl mit Zielwert und Verlaufshistorie zur Messung der Zielerreichung (Modul Ziele)
Lesebestätigung	Bestätigung eines Mitarbeiters, eine Richtlinie oder Schulungsunterlage gelesen zu haben; dient als Nachweis für Sicherheitsschulungen
Managementbewertung	Bewertung des ISMS durch die oberste Leitung nach ISO 27001 Kapitel 9.3

© 2012–2026 WolfInfoSec GmbH

Begriff	Bedeutung
Maßnahme	Konkrete Aktivität zur Risikobehandlung oder Framework-Erfüllung
master	Benutzerrecht für erweiterte Systemfunktionen (Freigaben, Gesamtaufgaben, Rollenpflege)
MAZ	Maximale Ausfalldauer – längster akzeptabler Zeitraum, in dem ein Prozess unterbrochen sein darf, bevor untragbare Geschäftsschäden entstehen
NIS-2	Network and Information Systems Directive 2 – EU-Richtlinie zur Cybersicherheit
	kritischer Infrastrukturen
norm	Benutzerrecht für die Bearbeitung von Controls und Rechtsregister
OBASHI	Ordnungsschema für Assets: Ownership, Business Process, Application, System, Hardware, Infrastructure – bestimmt die Reihenfolge der Asset-Kategorien
Operational Plan	Modul für wiederkehrende Pflichtaufgaben (Fristenkalender); bei Erledigung wird automatisch eine neue Instanz erzeugt, die vorherige bleibt unveränderlich als Nachweis erhalten
PIR	Post-Implementation-Review – Nachbetrachtung eines umgesetzten Changes; Voraussetzung für seinen Abschluss
Playbook	Vordefinierter Reaktionsplan für Sicherheitsvorfälle
privilegiert	Kennzeichnung besonders weitreichender Berechtigungen (Stufen A und N der Zugriffsmatrix), die bei der Rezertifizierung gesondert betrachtet werden
readonly	Benutzerrecht für ausschließlich lesenden Zugriff über das Policy Portal
Review	Geplante regelmäßige Überprüfung eines Eintrags (Asset, Dokument, Risiko etc.)
Rezertifizierung	Wiederkehrende Überprüfung, ob eine erteilte Berechtigung noch erforderlich ist (ISO 27001 A.5.18)
Risikoscore	Numerischer Wert aus Eintrittswahrscheinlichkeit × Schadenshöhe
RPO	Recovery Point Objective – maximal tolerierter Datenverlust bei einem Ausfall
RTO	Recovery Time Objective – maximal tolerierte Wiederherstellungszeit nach einem Ausfall
Schwellwertanalyse	Prüfung, ob eine Verarbeitung eine DSFA braucht – anhand der Muss-Liste der Aufsicht und der neun Kriterien aus WP 248
SoA	Statement of Applicability – Erklärung zur Anwendbarkeit der Controls
SSO	Single Sign-On – Anmeldung mit dem vorhandenen Firmenkonto über Microsoft oder Google
Tier	Kritikalitätsstufe eines Lieferanten (Tier 1 = kritisch, Tier 3 = unkritisch)
TOTP	Time-based One-Time Password (RFC 6238) – zeitbasiertes Einmalpasswort als zweiter Authentifizierungsfaktor; wird von Authenticator-Apps erzeugt und ist 30 Sekunden gültig
VVT	Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO
Zugriffsmatrix	Soll-Übersicht, welche Rolle auf welches Asset in welchem Umfang zugreifen darf (ISO 27001 A.5.15 / A.5.18)

WolfISMS – Wolf's Informations-Sicherheits-Management-System
© 2012–2026 WolfInfoSec GmbH
Version: 4.01 | Stand: November 2026