FACHARTIKEL · INFORMATIONSSICHERHEIT & GRC

WolfISMS: Informationssicherheit, die im eigenen Haus bleibt

NIS-2, ISO/IEC 27001, DSGVO, TISAX – die Anforderungen an Unternehmen wachsen, die Budgets und Teams oft nicht. WolfISMS ist ein vollständiges ISMS- und GRC-Werkzeug, das Unternehmen auf eigener Infrastruktur betreiben, per REST-API in ihre IT-Landschaft einbinden und mit KI-Assistenten beschleunigen können – ohne ihre sensibelsten Daten an einen fremden SaaS-Anbieter zu geben.

WolfISMS auf einen Blick

- **Betrieb:** Docker-Container On-Premises, Kubernetes oder Cloud Service
- **Umfang:** über 20 Module von Dokumentenlenkung bis BCM, 14 Normpakete
- **Compliance:** ISO/IEC 27001, NIS-2, DSGVO, CRA, TISAX, BSI IT-Grundschutz u. a.
- **Integration:** REST-API für sieben Bereiche, SSO (Entra ID, Google), Ticketsystem-Anbindung
- **KI:** Assistenten für Risiken, Vorfälle, Schwachstellen und Audits – Anbieter frei wählbar
- **Lizenz:** lesende Nutzer immer frei, Enterprise ohne Benutzergrenze, kostenlose Free-Edition
- **Sprachen:** Deutsch und Englisch

Zwischen Excel-Tabelle und Konzernlösung

Wer ein Informationssicherheits-Managementsystem aufbaut, steht meist vor einer unbequemen Wahl. Auf der einen Seite die gewachsene Sammlung aus Excel-Listen, Word-Richtlinien und SharePoint-Ordnern: günstig, aber spätestens im Audit mühsam, weil Zusammenhänge zwischen Assets, Risiken, Maßnahmen und Nachweisen von Hand hergestellt werden müssen. Auf der anderen Seite große GRC-Plattformen, die fast ausschließlich als Cloud-Dienst angeboten werden, pro Benutzer abrechnen und mit Einführungsprojekten kommen, die für den Mittelstand schnell überdimensioniert sind.

Mit NIS-2 hat sich der Druck deutlich erhöht: Tausende Unternehmen in Deutschland sind erstmals verpflichtet, Risikomanagement, Lieferkettensicherheit und Meldewege nachweisbar zu organisieren – inklusive enger Fristen von 24 und 72 Stunden bei Sicherheitsvorfällen. Genau für diese Lücke ist WolfISMS gebaut: ein integriertes Werkzeug, das den gesamten ISMS-Kreislauf abbildet, in wenigen Minuten als Container läuft und in der Datenhoheit des Unternehmens bleibt.

Was WolfISMS ist

WolfISMS ist eine webbasierte Anwendung für Informationssicherheits-, Governance-, Risiko- und Compliance-Management. Sie wird als **Docker-Container** ausgeliefert – wahlweise im eigenen Rechenzentrum (On-Premises), in einer privaten Cloud, auf Kubernetes oder als betriebener **Cloud Service** unter einer eigenen Subdomain. Die Oberfläche ist vollständig **zweisprachig (Deutsch/Englisch)**, Dokumente und Richtlinien lassen sich in beiden Sprachen pflegen.

Im Zentrum steht ein durchgängiges Datenmodell: Ein Asset kennt seine Risiken, ein Risiko seine Maßnahmen, eine Maßnahme die Normanforderungen, die sie erfüllt, und das Audit die Nachweise dazu. Was in anderen Umgebungen über Querverweise und Copy-and-paste zusammengehalten wird, ist in WolfISMS eine Verknüpfung – und damit auswertbar.

Die Funktionen im Überblick

Governance und Dokumentenlenkung

- **Dokumentenmanagement** mit Versionierung, Prüf- und Freigabe-Workflow (Ersteller, Prüfer, Freigebender), Klassifizierung sowie Word-Import und -Export.
- **Policy Portal**: freigegebene Richtlinien werden allen Mitarbeitenden in einem eigenen Portal bereitgestellt – lesende Portalnutzer zählen nicht zur lizenzierten Benutzerzahl.
- **Ziele**, **Organigramm**, **Prozesslandkarte** und **BPMN-Prozessmodelle** für den Kontext der Organisation.
- **Rechtsregister** für gesetzliche und vertragliche Anforderungen (ISO/IEC 27001 A.5.31, NIS-2, DSGVO).

Assets, Risiken und Maßnahmen

- **Asset-Management** mit Schutzbedarf je Schutzziel, Besitzern und Review-Zyklen, CSV-Import sowie **Netzwerkzonen** und **Zugriffsmatrix**.
- **Risikomanagement** mit konfigurierbaren Bewertungsskalen, automatisch berechneter Risikobewertung, Risikohistorie und generiertem Risikobehandlungsplan.
- **Maßnahmen, Projekte und Aufgaben** mit Verantwortlichen, Fälligkeiten und Kosten; ein **Operational Plan** erzeugt wiederkehrende Aufgaben, E-Mail-Erinnerungen laufen automatisch.
- **Changemanagement** zur Nachverfolgung von Änderungen an Assets und Systemen.

Vorfälle, Schwachstellen und Meldepflichten

- **Incident-Management** mit Verknüpfung zum externen Ticketsystem.
- **Meldeassistent** für die gesetzlichen Fristen nach **NIS-2** (24 h / 72 h / 1 Monat), **DSGVO** Art. 33/34 und **Cyber Resilience Act** Art. 14 – je Vorfall und Regelwerk mit Meldepflicht-Bewertung und Fristüberwachung.
- **Schwachstellenmanagement**, das Funde auch automatisch aus Scannern per API übernimmt.
- **Playbooks** als Handlungsanleitungen für die Vorfallbehandlung.

Lieferkette, Audit und Kontinuität

- **Lieferantenmanagement** mit Risikobewertung und einem **Online-Fragebogen** nach ISO/IEC 27001 und NIS-2: Der Lieferant erhält einen Link mit Einmal-Token und antwortet ohne eigenes Konto – die Antworten fließen direkt in die Risikobewertung ein.
- **Audit-Modul** für interne Audits und Gap-Assessments inklusive eines geführten **GAP-Assistenten**, der Anforderung für Anforderung durch die Prüfliste leitet.
- **Managementbewertung** nach ISO/IEC 27001 Kap. 9.3 mit Übernahme der Kennzahlen aus dem System.
- **Business Continuity Management (BCM)**: Business-Impact-Analyse, Notfallpläne und Übungen direkt am Asset, mit RTO, RPO und maximal tolerierbarer Ausfallzeit.
- **Berichtszentrale**, die alle Reports und Exporte entlang des ISMS-Kreislaufs bündelt.

Frameworks und Normpakete

Anforderungskataloge werden als Normpakete eingespielt und lassen sich mit Maßnahmen und Nachweisen verknüpfen; aus ISO/IEC 27001 entsteht auf Knopfdruck die **Erklärung zur Anwendbarkeit (SoA)** als gelenktes Dokument. Aktuell verfügbar sind 14 Pakete:

Bereich	Normpakete
Informationssicherheit	ISO/IEC 27001:2022 · BSI IT-Grundschutz 2023 · BSI Grundschutz++ · VdS 10000 · CISIS12
Regulierung (EU)	NIS-2 · NIS-2-Durchführungsverordnung · Cyber Resilience Act · DSGVO
Branche & Lieferkette	TISAX · VDA ISA · SOC 2 (AICPA TSC) · Cyber Essentials
Qualität	ISO 9001:2015

KI-Assistenten mit Kontrolle

Ab der Standard-Edition unterstützen KI-Assistenten bei den zeitintensivsten Aufgaben: der Analyse von Risiken, Vorfällen und Schwachstellen, der Zuordnung passender Maßnahmen sowie bei Audits und Gap-Assessments. Zwei Prinzipien unterscheiden sie von einem „Chatbot im ISMS“:

- **Der Mensch entscheidet.** Die KI macht Vorschläge, übernommen wird nur, was der Anwender bestätigt. Jeder Vorschlag wird gegen den echten Maßnahmen- und Normkatalog geprüft – erfundene Einträge werden verworfen, bevor sie jemand sieht.
- **Freie Anbieterwahl.** WolfISMS arbeitet mit Anthropic Claude, OpenAI, Azure OpenAI und dem europäischen Anbieter Mistral. Unternehmen mit strengen Datenschutzvorgaben wählen so ein Modell mit Verarbeitung in der EU oder im eigenen Azure-Tenant. Die KI ist abschaltbar; ohne sie bleibt jede Funktion voll nutzbar.

Was WolfISMS von anderen GRC-Lösungen unterscheidet

1. On-Premises statt Zwangs-Cloud

Ein ISMS enthält die Landkarte der eigenen Verwundbarkeit: Schwachstellen, offene Risiken, Netzwerkzonen, Notfallpläne, Sicherheitsvorfälle. Viele GRC-Anbieter bieten ausschließlich SaaS an – diese Informationen liegen dann zwangsläufig bei einem Dritten, oft außerhalb der EU. WolfISMS läuft dort, wo das Unternehmen es will: im eigenen Rechenzentrum, sogar in abgeschotteten Netzen, auf Kubernetes oder – wer den Betrieb abgeben möchte – als Cloud Service. Die Entscheidung liegt beim Kunden, nicht beim Hersteller.

2. Offene REST-API für die bestehende IT-Landschaft

Ein ISMS, das nur über manuelle Eingaben gefüttert wird, veraltet. WolfISMS bietet eine dokumentierte **REST-API** für Incidents, Maßnahmen, Assets, Risiken, Lieferanten, Schwachstellen und Benutzer. Typische Szenarien:

- Ein **SIEM** legt Sicherheitsvorfälle automatisch an.
- Ein **Schwachstellenscanner** liefert seine Funde direkt ins Schwachstellenmanagement.

- Eine **CMDB** gleicht den Asset-Bestand ab.
- Ein **Ticketsystem** holt offene Maßnahmen ab und meldet die Ticketnummer zurück.
- Ein **Reporting-Werkzeug** liest Risiken und Kennzahlen für den Managementbericht.

API-Keys werden nur als SHA-256-Hash gespeichert, sind einzeln deaktivierbar und durch ein Rate-Limit geschützt; eine integrierte REST-Konsole erleichtert Test und Anbindung.

3. Faires Lizenzmodell: Lesen kostet nichts

Die meisten Anbieter rechnen jeden Benutzer ab – auch die Mitarbeitenden, die nur Richtlinien lesen. In WolfISMS zählen ausschließlich Benutzer mit Schreibrechten. **Lesende und Portalnutzer sind in jeder Edition unbegrenzt.** Die ganze Belegschaft kann Richtlinien im Portal lesen, ohne dass die Kosten mitwachsen. Die Enterprise-Edition hat zudem keine Benutzergrenze.

4. Integriert statt Insellösung

Risiko, Asset, Lieferant, Vorfall, BCM, Audit und Dokumentenlenkung teilen sich ein Datenmodell. Eine Schwachstelle wird zum Risiko, das Risiko bekommt Maßnahmen, die Maßnahme erfüllt Anforderungen aus mehreren Normen zugleich – ISO 27001, NIS-2 und TISAX müssen nicht dreimal gepflegt werden.

5. Sicherheit und Identitäten „by Design“

- **Zwei-Faktor-Authentifizierung (TOTP)** für alle Konten.
- **Single Sign-on** über Microsoft Entra ID und Google Workspace (OIDC).
- Feingranulare **Modulrechte**, Rollen und abschaltbare Module – jede Organisation sieht nur, was sie braucht.
- Durchgehender CSRF-Schutz, Eingabeprüfung an jedem Schreibpfad, Historie und Kommentarfunktion für die Nachvollziehbarkeit im Audit.

6. Schnell startklar

Ein **Einrichtungsassistent** führt durch die ersten Schritte – Unternehmensdaten, Organisation, Normpakete. Die Installation besteht im Kern aus einem „docker compose up“; Updates werden über die Anwendung eingespielt, Backups sind integriert. Eine kostenlose Free-Edition erlaubt den Einstieg ohne Beschaffungsprozess.

Im Vergleich

Kriterium	Excel / SharePoint	Typische SaaS-GRC-Plattform	WolfISMS
Betrieb	Eigene Ablage	Nur Cloud des Anbieters	**On-Premises, Kubernetes oder Cloud Service**
Datenhoheit	Ja, aber unstrukturiert	Beim Anbieter	**Beim Kunden**
Verknüpfung Asset–Risiko–Maßnahme–Norm	Manuell	Ja	**Ja, durchgängig**

Kriterium	Excel / SharePoint	Typische SaaS-GRC-Plattform	WolfISMS
NIS-2-Meldefristen	Nicht vorhanden	Teilweise	**Meldeassistent NIS-2, DSGVO, CRA**
Schnittstellen	Keine	Oft nur in hohen Paketen	**REST-API** (Plus-Editionen, Enterprise)
Lesende Benutzer	–	Meist kostenpflichtig	**Unbegrenzt, ohne Aufpreis**
KI-Unterstützung	Keine	Proprietär, ein Anbieter	**Wählbar, inkl. EU-Anbieter**
Einstieg	Sofort	Einführungsprojekt	**Container + Assistent, Free-Edition**

Editionen

WolfISMS wächst mit der Organisation. Alle Editionen enthalten die Kernmodule – Dokumente, Policy Portal, Assets, Risiken, Maßnahmen, Aufgaben, Incidents, Lieferanten, Personal, Frameworks und Berichte.

Edition	Schreibende Benutzer	Enthalten zusätzlich
Free	1	Einstieg und Erprobung (je 10 Assets, Risiken, Dokumente, Lieferanten)
Standard	5	Unbegrenzte Datenmengen, KI-Assistenten
Standard Plus	5	wie Standard, plus REST-API, SSO und Zugriffsmatrix
Professional	20	Projekte, Operational Plan, Audit, Managementbewertung, Schwachstellen, Rechtsregister, Playbooks, BCM
Professional Plus	20	wie Professional, plus REST-API, SSO und Zugriffsmatrix
Enterprise	unbegrenzt	Vollausbau mit allen Modulen und Schnittstellen

Lesende und Portalnutzer sind in allen Editionen unbegrenzt. Optional übernimmt der **Cloud Service** den Betrieb unter einer eigenen Subdomain.

Fazit

WolfISMS verbindet den Funktionsumfang einer GRC-Plattform mit der Kontrolle einer selbst betriebenen Anwendung. Unternehmen, die NIS-2 umsetzen, eine ISO/IEC-27001-Zertifizierung anstreben oder TISAX-Anforderungen erfüllen müssen, erhalten ein Werkzeug, das die Zusammenhänge im ISMS abbildet, Meldefristen im Blick behält und sich über die REST-API nahtlos in SIEM, CMDB und Ticketsystem einfügt – und dabei die sensibelsten Informationen des Unternehmens dort lässt, wo sie hingehören: im eigenen Haus.