



ISMS4All

Informationssicherheit & Compliance im Griff!

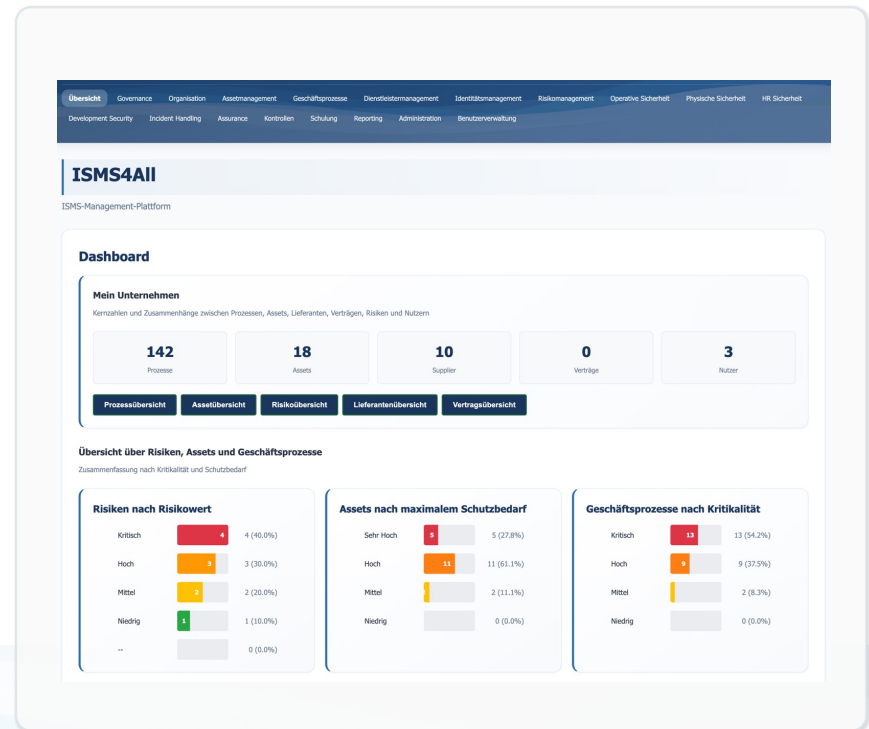
Version 1.0, 20.05.26



ISMS4All – Die moderne GRC-Plattform

Ihre Lösung für Informationssicherheitsmanagement & regulatorisches Compliancemanagement

- Klarer Fokus auf ISO 27001, DORA und NIS2
- Erfassung und Verwaltung aller relevanten Aspekte
- Strukturierung und Automatisierung von Alltagsaufgaben



Warum ISMS4All?

Mit ISMS4All haben Sie alle Informationssicherheitsanforderungen im Griff.

ISMS4All macht aus verteilten Daten ein strukturiertes, verknüpftes und zertifizierungsfähiges ISMS.

Datengrundlage statt Datenchaos

Keine verstreuten Excel-Listen, Word-Dokumente und Versionskonflikte - sondern eine gemeinsame Arbeitsgrundlage.

Zusammenhänge statt Medienbrüche

Governance, Prozesse, Assets, Risiken, Maßnahmen und Nachweise stehen in einem System in Beziehung.

Workflows statt Hand-am-Arm

Klare Workflows mit hoher Automatisierung und Erinnerungen helfen bei der kontinuierlichen Pflege des ISMS.

Transparenz und Compliance

Jederzeit das ISMS im Blick mit aktuellen Zahlen und Daten. Flexibel nutzbar für ISO27001, DORA und NIS2.

Excel & Word als Basis für ein „ISMS“

Manuelle, verteilte Pflege - geringe Transparenz - hoher Aufwand - fehlende Nachvollziehbarkeit

ISMS4All als zentrale ISMS-Plattform

Zentrale Datenhaltung - nachvollziehbare Änderungen - hohe Transparenz – starke Automatisierung – ideale Vorbereitung für Audits

Unsere Plattforminhalte im Überblick

Alle Bausteine eines wirksamen Informationssicherheitsmanagements an einem Ort.

Governance & Rollen

Rollen, Verantwortlichkeiten und Richtlinien pflegen, Reviews und Freigaben dokumentieren.

Asset Management

Informationswerte klassifizieren, Schutzbedarf erfassen, mit Prozessen verknüpfen.

Geschäftsprozesse & BCM

Prozesse, Kritikalität und RTO/RPO erfassen, Business Continuity Pläne und Notfallkommunikation dokumentieren.

Risikomanagement

Risiken identifizieren, bewerten, behandeln und mit Assets und Prozessen verknüpfen.

Dienstleister Management

Dienstleister, Verträge und Due Diligence erfassen, Assets & Prozesse verknüpfen.

Testmanagement & Assurance

Testplan erstellen, Ergebnisse dokumentieren, Kontrollen durchführen, Berichte und Nachweise erfassen.

Incidents Handling

Vorfälle erfassen, bearbeiten und regulatorische Aufgaben wie Meldepflichten und Lessons Learned strukturiert erfüllen.

Reporting

Berichte, Kennzahlen und Nachweise für ISO 27001, DORA oder NIS2 integriert dokumentieren.

ISMS4All – Alle Risiken im Blick

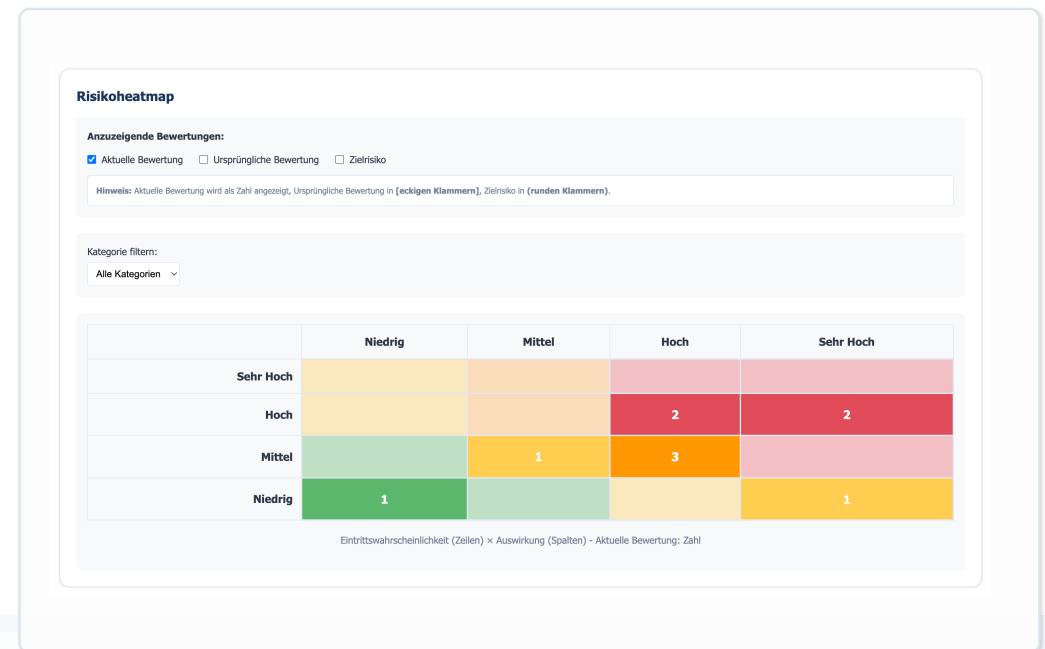
Entwickelt für kleine und mittlere Unternehmen im deutschsprachigen Raum.

ISMS4All umfasst ein vollständiges IKT-Risikomanagement für die Anforderungen aus DORA und NIS2.

- Ausrichtung an ISO/IEC 27001:2022 und ISO/IEC 27002:2022
- Praxistauglich mit Fokus auf KMUs im deutschsprachigen Raum
- Betrieb auf gehärteten Servern in Deutschland oder in eigener Umgebung

Nie wieder Excel, Word und Copy-Paste.

Standardaufgaben werden durch Struktur, Verknüpfung und Automatisierung deutlich effizienter.



Flexibel im Betrieb, modern in der Nutzung

ISMS4All kombiniert Wahlfreiheit beim Hosting mit optionaler KI-Unterstützung.

Vom unkomplizierten Einstieg bis zum Self-Hosting:
Wie und wo Ihre Daten liegen entscheiden Sie!

Das Diagramm zeigt drei Hosting-Modelle in separaten Kästen:

- Geteiltes Hosting:** Ein Server, mehrere Kunden. Gezeigt werden mehrere Server-Schrank-Symbole, die durch eine Klammer verbunden sind, die auf einen zentralen Server-Schrank zeigt.
- Dediziertes Hosting:** Ein Server, ein Kunde. Gezeigt wird ein einzelner Server-Schrank, der mit einem Kunden-Symbol verbunden ist.
- Individuelles Hosting:** Ihr Server, Ihre Entscheidung. Gezeigt wird ein einzelner Server-Schrank, der mit einem Kunden-Symbol verbunden ist, das an einem Laptop sitzt.

Unten steht der Text: Betriebsmodelle: Basic, Pro oder individuell

Über unseren Partner, die siaris GmbH kann auf Wunsch eine datenschutzkonforme KI-Integration ergänzt werden.

Das Screenshot zeigt ein KI-Chat-Fenster mit dem Titel 'Welche Quellen werden im ISMS für aktuelle externe Bedrohungen berücksichtigt?'. Die Antwort lautet: 'Externe Quellen für Bedrohungen im ISMS: Anzahl: 35 Quellen. Quellen-Typen: CERTs, Hersteller-Updates, Threat-Intelligence-Plattformen, Leak-Datenbanken, Schwachstellen-Datenbanken, Brancheninitiativen, Behörden.' Darunter ist eine Tabelle mit den 'Top 10 Quellen (Auswahl)' zu sehen:

Quelle	URL	Beschreibung / Typ	ID
CERT-Bund	BSI CERT-Bund	Nationale CERT für Deutschland - Warnungen zu IT-Sicherheitsvorfällen.	00001
CISA KEV	CISA Known Exploited Vulnerabilities	Katalog aktiv ausgenutzter Schwachstellen (US-Behörde).	00031
NVD	National Vulnerability Database	US-Datenbank für CVE-Details und Schwachstellen.	00032
AlertVault OTC	AlertVault Open Threat Exchange	Kollaborative Plattform für Threat Intelligence (i.e.S. Malware, Angriffswerkzeuge).	00010
MSRP	MSRP Report	Plattform zum Austausch von Threat Intelligence und Malware-Informationen.	00044
Hive IT Been Pwned	HSP	Datenbank für kompromittierte Accounts/Passwörter (Leak-Überprüfung).	00003
BSI IT-Grundschutz	BSI IT-Grundschutz	Standard für IT-Sicherheitsmaßnahmen in Deutschland.	00026
ENISA Threat Landscape	ENISA Reports	EU-weite Bedrohungsanalysen und Trends.	00005
Cisco Talon	Cisco Talon Intelligence	Threat Intelligence und Malware-Analysen von Cisco.	00034
Dehived	Dehived	Datenbank für geleakte Zugangsdaten (z. B. Mail/Passwort-Kombinationen).	00035

Unter der Tabelle steht: Kategorien-Übersicht

- CERTs/Behörden (10 Quellen)**
 - Beispiele: CERT-Bund (00001), CERT-EU (00018), DFN-CERT (00006), Europol EC3 (00015).
 - Zweck: Offizielle Warnungen, nationale/EU-weite Bedrohungslagen.
- Hersteller-Updates (5 Quellen)**
 - Beispiele: Microsoft Security Updates (00007), SAP Security Notes (00008), Cisco (00002).
 - Zweck: Produkt-spezifische Schwachstellen und Patches.

Am unteren Rand des Chat-Fensters steht: 'Warte, bis die aktuelle Anfrage vollständig bearbeitet worden ist' und 'Workflow Agent'.

Unten steht der Text: KI-Chat für Wissenszugriff, Auswertung und Routineaufgaben

Zusammen mit ai.go wird Informationssicherheit lebendig

Über die datenschutzkonforme KI-Integration ai.go unseres Partners Siaris GmbH wird ISMS4All im Alltag erlebbar.

The screenshot shows the 'API-Konfiguration' section of the ISMS4All platform. It includes a navigation menu at the top with categories like 'Übersicht', 'Governance', 'Organisation', 'Assetmanagement', 'Identitätsmanagement', 'Risikomanagement', 'Dienstleistermanagement', 'Operative Sicherheit', and 'Physische Sicherheit'. The main content area is titled 'API-Konfiguration' and contains a sub-section 'API Access'. Below this, there is a table listing API keys for 'ai.go'. The table has columns for Name, Berechtigungen, Erstellt, Zuletzt genutzt, Aufrufe (7 T.), Aufrufe (30 T.), and API-Schlüssel. The 'ai.go' entry shows 20 read and 20 write permissions, created on 2026-04-20 at 09:53:01, with 0 calls in both 7 and 30-day periods. The API key is displayed as a long alphanumeric string with 'Kopieren' and 'Löschen' buttons.

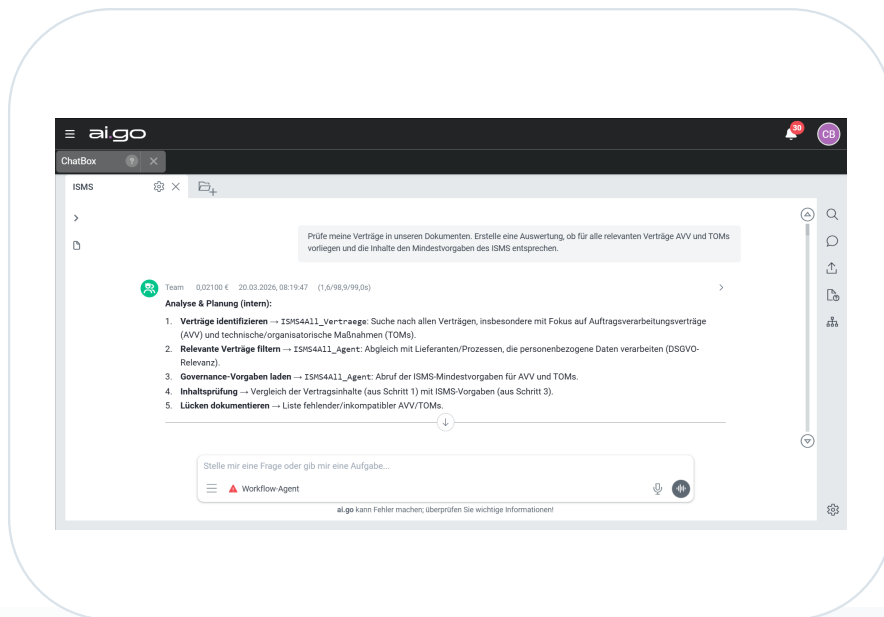
Name	Berechtigungen	Erstellt	Zuletzt genutzt	Aufrufe (7 T.)	Aufrufe (30 T.)	API-Schlüssel
ai.go	20 Lesen, 20 Schreiben	2026-04-20 09:53:01	–	0	0	59a9708818563066b5887761260c4 0ec235be140b798874b791c881ef 7c5988 Kopieren Löschen

The screenshot shows the ai.go chat interface. The chat window is titled 'ai.go' and contains a message from the system: 'Welche Quellen werden im ISMS aktuell für externe Bedrohungen im Risikomanagement berücksichtigt?'. The response is titled 'Externe Quellen für Bedrohungsinformationen im ISMS-Risikomanagement' and lists several sources: 'Allgemeine Threat-Intelligence-Feeds', 'CERT-Bund (BSI) Nationale CERT-Warnungen und Empfehlungen', 'MISP (Malware Information Sharing Platform) Kollaborative Plattform für Bedrohungsdaten', 'AlienVault OTX (Open Threat Exchange) Kollaborative Bedrohungsdaten', 'ENISA Threat Landscape Reports EU-Berichte zu Cyber-Bedrohungen', and 'CISA Known Exploited Vulnerabilities (KEV) Katalog aktiv ausgenutzter Schwachstellen (US-Behörde)'. The chat interface includes a search bar, a 'Workflow-Agent' indicator, and a footer note: 'ai.go kann Fehler machen, überprüfen Sie wichtige Informationen!'.

ISMS4All + ai.go: moderne ISMS-Plattform, KI-Integration und europäisch ausgerichtete Datensouveränität aus einer Hand.

Alle Aufgaben an einer Stelle erledigen

Dank ai.go lassen sich alle gängigen Aufgaben aus unserem ISMS4All direkt per Chat im Workspace erledigen.



Vom starren ISMS zum Sicherheits-Arbeitsplatz

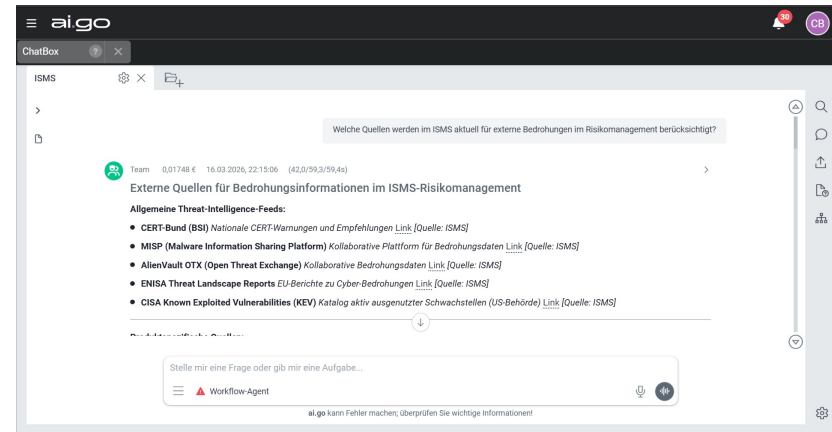
- **Interaktive Nutzung** statt starrer Dokumentenablage: Informationen, Aufgaben und Nachweise sind direkt im Chat verfügbar.
- **Kontextbezogene Unterstützung** für unterschiedliche Rollen - vom Application-Manager bis hin zur Geschäftsführung und Entwicklung.
- **Automatisierung typischer Routineaufgaben** wie Zusammenfassungen, Berichtsentwürfe und graphische Informationsaufbereitung.
- **Chat-basierte Erledigung von Alltagsaufgaben:** Bedrohungen erfassen, Prozesse aktualisieren und Risiken bearbeiten direkt aus ai.go.

Minuten statt Tage für Alltagsaufgaben dank ai.go-Integration

Weniger Komplexität, mehr Tempo – die KI-Integration beschleunigt die definierten Prozesse und Aufgaben.

Alle Alltagsaufgaben in Rekordzeit erledigen:

- Neue Bedrohungsquellen erfassen
- Verträge, AVVs und weitere Dokumente auf Compliance prüfen
- Lücken bei den dokumentierten Dienstleistern finden
- Maßnahmen für die Risikobehandlung evaluieren
- Richtlinien und Regelungen auf Konformität prüfen



pebes GmbH – der Anbieter dahinter

Beratung und Umsetzung für Informationssicherheit, Compliance und Cloud-Security.

pebes unterstützt Unternehmen beim Aufbau wirksamer Informationssicherheit – strategisch, operativ, praxisnah.

10+

Jahre Erfahrung

IT- und Informationssicherheit in Strategie, Projekten und Betrieb.

300+

Projekte

Vorhaben in Informationssicherheit und Governance.



- ISMS & Compliance
- ISO 27001, DORA, NIS2
- Beratung – Schulung – Überprüfungen



UNSER KONTAKT



isms@pebes.de



+49 7134 53 439 62



www.isms4all.de

