

*Vami*GRC

Powered by



THE AI-driven IT
Security and GRC Experts

Trusted • Holistic • Engineered



TECH
BOOST



ISO 27001

GRC ist Ihr
Wettbewerbsvorteil —
nicht Ihr
Compliance-Ballast.

NIS2

DSGVO

ISO 42001

EU KI-Gesetz

GRC

Die führende
KI-native,
agentenbasierte
GRC-Plattform
für regulierte
Unternehmen
in Europa.

DORA



95%

Reduktion manueller
Compliance-Arbeit



100%

Wirkung mit

WIZ



VamiGRC.com – DE – Bonn



VamiGRC

AGENTENBASIERT • GRC • PLATTFORM

Neue EU-Vorschriften überfordern international Unternehmen – und stellen eines der größten Geschäftsrisiken dar.

Warum integrierte GRC-Lösungen jetzt geschäftskritisch sind



Vier Risikoklassen. Ein integriertes Steuerungsmodell.

VamiGRC verbindet regulatorische, vertragliche, operative und opportunistische Risiken in einer gemeinsamen GRC-Betriebsebene.

01 Regulatorische Risiken

NI52 · DORA · CRA · EU AI Act · DSGVO

Bußgelder, Auflagen, Prüfungsfeststellungen und fehlende Compliance-Nachweise.

02 Vertragliche Risiken

Kunden-, Lieferanten- und Partnerpflichten

SLA-Verletzungen, Haftung, Audit-Klauseln und fehlende Kontrollnachweise.

03 Operative Risiken

Ausfälle · Ransomware · Prozessstörungen

Direkte Auswirkungen auf Geschäftsbetrieb, Lieferfähigkeit und Reputation.

04 Opportunistische Risiken

Marktzugang · Vertrauen · Umsatzchancen

Schwache Compliance blockiert Wachstum und macht Wettbewerbsvorteile nicht nachweisbar.

Fragmentierte Compliance wird zu messbarer Risikoreduktion und Umsatzsicherung.



#1 KI-NATIVE AGENTEN-BASIERTE GRC-PLATTFORM

Ein IMS. Alle Domänen. Ein intelligenter GRC-Ansatz.

VamiGRC vereint integrierte Managementsysteme, agentenbasierte Automatisierung und rollenbasierte Ansichten für CISOs, KI Officers und Datenschutzbeauftragte mit einer grafbasierten Risikoanalyse, inspiriert vom **WIZ** Security Graph.

01 • INTEGRIERTES IMS

Ein IMS. Fünf Domänen.

- ISMS** ISO 27001 • NIS2 • TISAX
- AIMS** EU KI Act • ISO 42001
- PIMS** DSGVO • ISO 27701
- CSMS** IEC 62443 • CRA • MDR
- BCMS** ISO 22301 • DORA

Einmal modellieren • wiederverwendbar • auditfähig durch Design

02 • AGENTENBASIERTE AUTOMATISIERUNG

Workflows im Autopilot.

- Lieferanteninformationen — OSINT, Ratings, DPA
- Risikoanalysen — Register & Aktionsplan
- Multi-Framework-Audits — weniger Redundanz
- Trust Center — mehrsprachig & konsistent

Eine Eingabe • ein Workflow • menschlich in Kontrolle

03 • GRC-GRAPH

Zusammenhänge werden sichtbar.

- Schwachstellen und ihre kritischen Risiken sichtbar durch toxische Kombinationen
- Nachweise mit Audit-bereiter Evidenz
- KPIs & Geoposition in einer weltweiten Übersicht

Silos aufbrechen • verstehen • mit Vertrauen entscheiden

Linsen & Domänen

Wählen Sie Ihre Linse
Maßgeschneidert für Ihr Dashboard —
und Einblicke, die zu Ihren Rollen passen.

**Vollständiges IMS** Aktiv

Alle Domänen

CSMS AIMS PIMS CSMS BCMS

Die vollständige Ansicht aller Domänen für integrierte GRC-Prüfungen, Zusammenhänge und übergreifende Kontrolle.

Kontrollen 2.486 Assets 1.266 Nachweise 781

**ISMS-Linse** Aktiv

Informationssicherheit

Die ISMS-fokussierte Ansicht, abgestimmt auf ISO 27001. Steuerungen, Lösungen und Nachweise — jederzeit griffbereit.

Kontrollen 1.246 Assets 573 Nachweise 329

Alle Domänen anzeigen →

VamiAI Copilot

Fragen Sie VamiAI
Ihr KI-Copilot für GRC, Risiko und Compliance.

Präzise Ausgewogen Kreativ Linse • Vollständiges IMS

VamiAI • bereit, Ihr Team zu unterstützen — unterstützt durch den WIZ Security Graph. Ich sehe Expositionen in Ihrem GRC-Graph und liefere Evidenz aus ISO 27001, NIS2, DSGVO, KI Act, DORA und mehr. Womit kann ich Ihnen helfen?

Sie können jede Frage stellen.
Probieren Sie: Richtlinien, Frameworks, Assets, Kontrollen ...

Geoposition & Graph-Ansicht

Geoposition
Risiken und Expositionen weltweit nach Regionen und Assets.

Risiken Assets Vorfälle Nachweise Compliance



Berlin, Deutschland		
Kritische Risiken	12	
Toxische Kombinationen	142	
Offene Findings	167	
Assets in Risiko	642	
Assets gesamt	947	
Compliance-Score	89%	
Risiko		Hoch • Mittel • Niedrig
Graph-Ansicht		Inventar



Für CISO, DPO, KI Officer, Risiko- & Compliance-Leads auditfähig • rollenbasiert • modular • audit-orientiert & skalierbar.

VamiGRC macht GRC operativ, intelligent und integrierbar — vamigrc.com

VamiGRC ist für **GRC** das, was **WIZ** für Cloud-Sicherheit ist.



Security Graph

Abbildet jedes Asset, jede Schwachstelle, jede Identität und jeden Netzwerkpfad – und deckt die **toxischen Kombinationen** auf, die Ihre wertvollsten Assets gefährden.



ERSETZT Dutzende von CSPM-, CWPP- und CIEM-Point-Tools.



VamiGRC

GRC Graph

Abbildet jede Kontrolle, jedes Risiko, jeden Prozess, jede Regelung, jedes Asset und jeden Nachweis – und deckt die **toxischen Kombinationen** über alle Governance-Domänen hinweg auf.



ERSETZT Dutzende von GRC-, ISMS-, PIMS-, AIMS-, BCMS- und CSMS-Point-Tools sowie Tabellenkalkulationen.

Der

WIZ

Effekt



GRC Graph – Mit toxischen Kombinationen decken wir kritische Risiken in Ihren wertvollsten Assets auf.

vamigrc.com

Risikoketten

*sofort
erkennen.*

Assets, Lieferanten, Prozesse und Risiken werden in einem Graphen verknüpft.

01 VERNETZEN

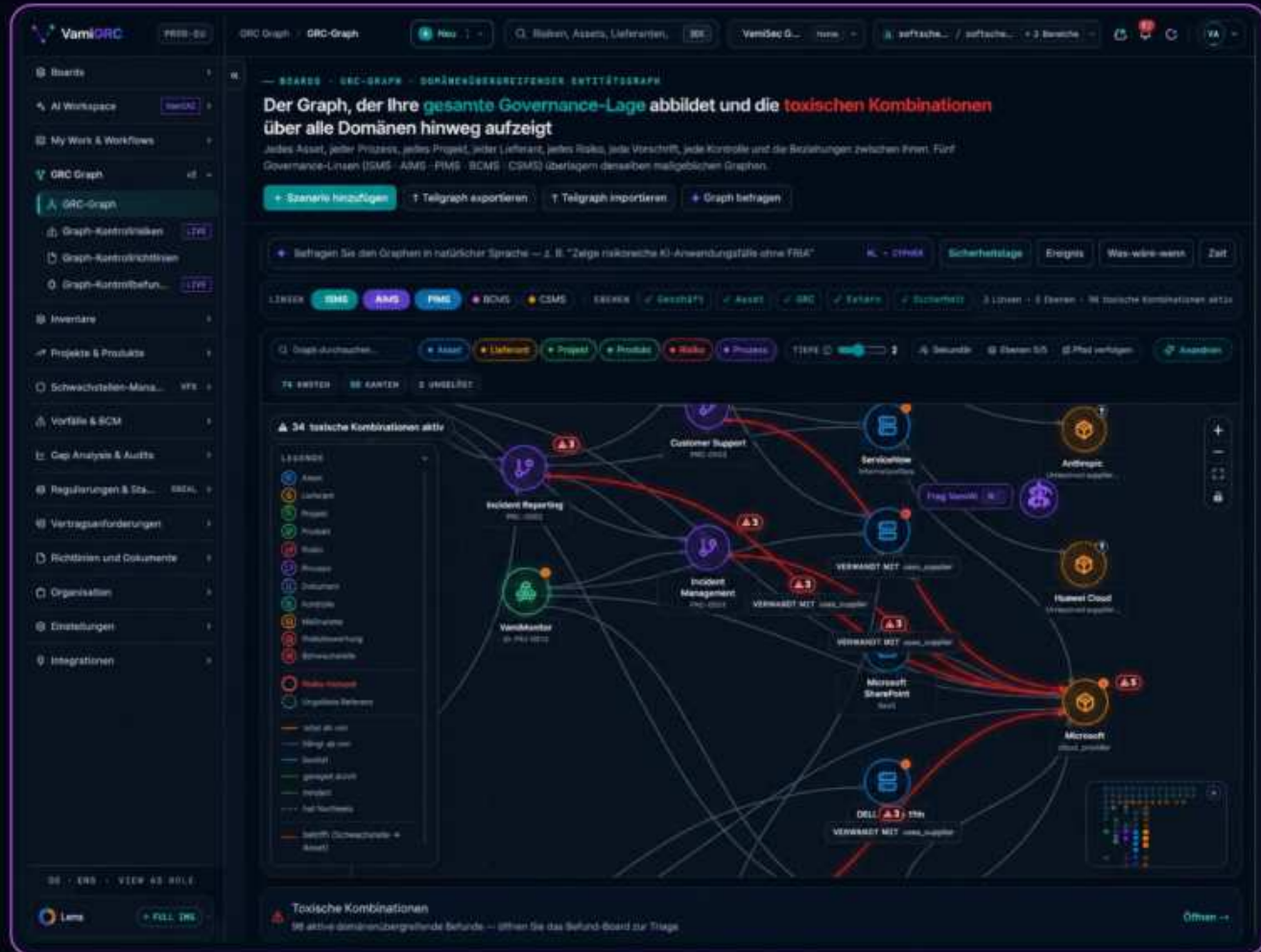
Alle GRC-Domänen verbinden

02 ERKENNEN

Toxische Kombinationen
priorisieren

03 VAMIAI

Den Graphen natürlich befragen



Risiken quantifizieren.

Exposition, Heatmap und
90-Tage-Trend schaffen eine
belastbare
Entscheidungsgrundlage.

01 EXPOSITION

Risikoauswirkung in Euro
bewerten

02 PRIORISIERUNG

Wirkung x Wahrscheinlichkeit

03 RISIKO-VELOCITY

Dynamik über 90 Tage verfolgen

Wo das Risiko der Organisation tatsächlich liegt.

SCHÄTZEN-ANSICHT **ALLR** ISMS AIMS FINS CEMS NEMS

QUELLE Alle Quellen

RESULTIERENDE EXPOSITION

RESULTIEREND ANFANG

€175K / Jahr

ggü. €175K anfänglich — Kontrollen senken die Exposition um 0%

(Risk-eligible (spunt) nettowert) 300.33800

Monetary figures are estimates derived from qualitative scores and breach-entry criticality, calibrated via the master and per-nature factors (70)

% ERKENNTNISSE

Estimated annualised residual risk exposure is €175K.

Opportunistic risk is the sole driver at €175K, accounting for 100% of the total.

ANFANGSRISIKO

RESULTIEREND

Anfängerisiken

0 Risiken

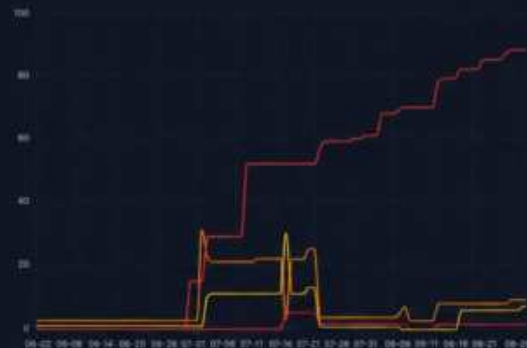


AUSWIRKUNG: Trag / Verlust



Niedrig 0 Mittel 0 Hoch 0 Kritisch 0

Risiko-Trend: 90T



RISIKO-VELOCITY

+101 86-62 + 86-28

Risiken gesamt

5 + 186

Kritisch

0 + 2 +2

Hoch

3 + 9 +6

Mittel

1 + 66 +87

Niedrig

1 + 7 +6

Nettoänderung der Risikozahl in diesem Zeitraum

GRC-Prozesse automatisieren.

Risiken, Audits und
Lieferantenprüfungen – kontrolliert
und nachvollziehbar.

01 RISIKEN & MASSNAHMEN

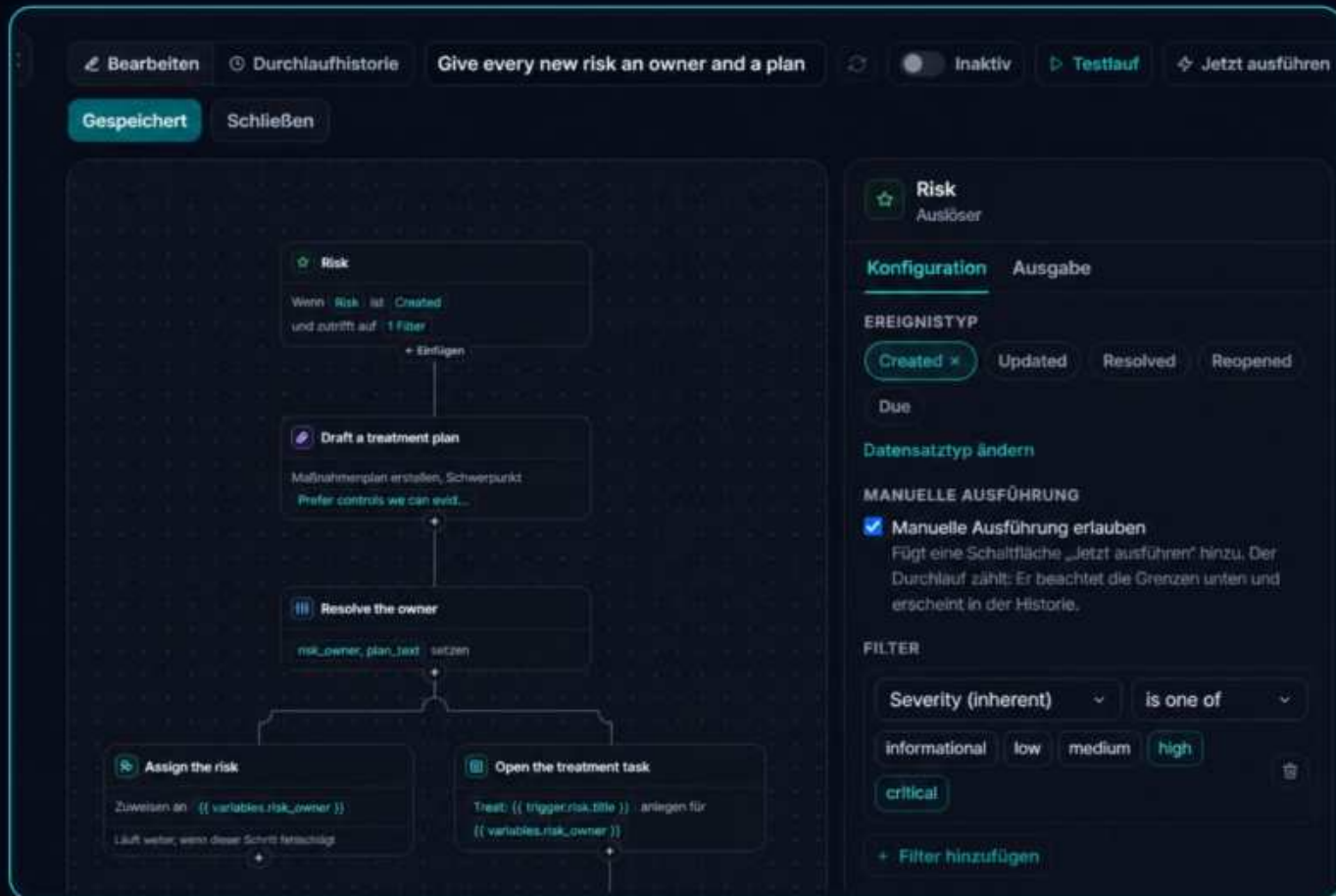
Analysieren · planen · zuweisen

02 INTERNE AUDITS

Planen · prüfen · dokumentieren

03 LIEFERANTENPRÜFUNGEN

Bewerten · nachverfolgen ·
steuern





VamiAI • 10:24 • gedacht für 8 Sekunden

Ich habe die bereitgestellten Daten im IMS, dem GRC-Graph und eurer aktiven Frameworks (z. B. NIS2, DORA, GDPR) analysiert und Ausführungsentwürfe zusammengestellt, die auf eure Autonomie-Einstellungen abgestimmt sind.

- Welche Risiken haben den höchsten MISP*
- Führe eine Analyse des CAIQ durch
- Zeige mir die zu GDPR gehörenden Kontrollen
- Finde toxische Kombinationen zwischen MS-AIMS*



Du • 10:25

Ich benötige einen Risiko-Inventarbericht, der Kataloge und das NIS2 (lokal, profil) mit Expositionspfad Art. 19(3) aufteilt, nach Schweregrad.

Kritisch	maximaler Schweregrad
Hoch	hoher Schweregrad
Mittel	mittlerer Schweregrad



VamiAI • 10:26 • gedacht für 12 Sekunden

Was ist die Schwelle für einen Bericht im Risikoregister und wer soll benachrichtigt werden?

- Im Risikoregister speichern
- Für das Security-Team freigeben
- Öffne in einem Audit

Die Schwelle für den Bericht im Risikoregister ist erreicht. Teile ihn mit dem Security-Team.



VamiAI • 10:27 • Analyse abgeschlossen

AKTIONSKARTEN • ERGEBNIS

4 Kritisch • 12 Hoch • 18 Mittel • NIS2: Kontrolllücken-19
Eingeräumt • IMS-AI • Bewertungs-ID: exc-R-6471

Bewertungssprache



vami-ai: risiko-analyse

Letzter Bericht: nach Analyse • gespeichert



vami-ai: regulatorische-zuordnung

GDPR/DORA/NIS2 • Bewertung • Lücken

Stelle eine Frage zu deinem IMS, Kontrollen, Reglement...



• /02 • VAMI-AI • AGENTISCHER ASSISTENT

Sprich mit deinem *IMS*. Es kennt bereits die Antwort.

VamiAI ist in deinem IMS, deinem GRC-Graphen und deinen aktiven Frameworks verankert. Es kann abfragen, analysieren, entwerfen und ausführen – bei jedem Schreiben läuft alles durch deine Autonomie-Richtlinie (L0-L3 Mensch-im-Loop).

- "Welche Lücken gefährden NIS2? – 14 Lücken • nach Schweregrad aufgeteilt • ein Klick in das Risikoregister
- "Pre-Antwort" des CAIQ – toxische Kombinationen über PMS-AIMS* • zitiert • audit-protokolliert
- Aktionskarten benötigen explizite Genehmigung auf L3 • gestreckter Fortschritt • pausieren / zurücksetzen jederzeit

Triff VamiAI



Projektkontext wird Risikobild.

VamiAI strukturiert Nachweise,
erkennt Risiken und erstellt eine
Management-Zusammenfassung.

01 EVIDENCE

Nachweise direkt analysieren

02 RISK REGISTER

Registrieren · bewerten · zuweisen

03 REPORTING

Excel und Management-PDF exportieren

KI-Arbeitsbereich · Risikoanalyse

Risikoanalyse KI-865T0727

Erstellen Sie eine strukturierte Risikoanalyse anhand von Projektkontext und Nachweisen.

Berichte ansehen + Neue Bewertung

Dashboard + Neue Bewertung Fortschritt **Ergebnisse** Empfehlungen 18 Berichte Verlauf

2025-07-02 Document-based assessment using provided tenant evidence.

Bearbeiten Bericht exportieren

SAP Migration

Migration from on-premises SAP to SAP RISE managed cloud service.

Zentrale Risikothemen

- Cloud shared responsibility and RACI gaps
- Identity and access management weaknesses for SAP
- Data protection and regulatory compliance uncertainty
- Monitoring and incident response coverage in cloud
- Business continuity and disaster recovery validation
- Third-party and supply chain dependencies
- Network connectivity and interface security
- Change and cutover governance for migration

Gesamtrisiko 12 risks

Hoch

- Erniedl. 0
- Hoch 10
- Mittel 2
- Niedrig 0

Projektprofil

BESCHREIBUNG
Migration from on-premises SAP to SAP RISE managed cloud service.

ERKENNTE PROJEKTTYPEN

- SAP migration
- Cloud transformation

DATENTYPEN

- unknown

UMGEBUNG
unknown

EXPOSITION
unknown

COMPLIANCE-STANDARDS

- ISO 27001
- AI Act
- NIS2

Flag VamiAI 0.2

+ Management-Zusammenfassung

The SAP Migration project involves transitioning from an on-premises SAP system to the SAP RISE managed cloud service. The overall risk is assessed as medium-high, with key concerns around cloud shared responsibility, identity management, data protection, and incident response. High-priority recommendations focus on establishing a RACI model, enhancing access governance, and ensuring data compliance.

Bereitstellungsvarianten 1 Varianten

VAR-1

SAP RISE Migration - Overall

- Mittel

Risikoregister 10 Risiken - Zeile umklappen zum Aufklappen Expand all

ID	RISIKONAME	VARIANTE	L	S	RESTRISIKO	RESTRISIKO	KATEGORISIRISIKO	STATUS
PER-1	Cloud shared responsibility and RACI gaps with SAP RISE	VAR-1						
	Ambiguity over who (tenant vs. SAP RISE provider/partner) is responsible for key security and operational controls leads to gaps in coverage, delayed incident handling, or non-compliance.		2	3	3	3	3	3

Ein Control Set.

Viele Regelwerke.

Gleichartige Anforderungen werden zusammengeführt – Redundanz und Auditaufwand sinken.

01 COMPOSE

ISO 27001 · NIS2 · CRA

02 AI GOVERNANCE

AI Act · ISO 42001 kombinieren

03 ASSURANCE

Eine Basis für alle Audits

The screenshot displays the VamiGRC Framework Composer interface. On the left is a sidebar with navigation options: Dashboards, AI Workspace, Meine Arbeit & Workflows, GRC Graph, Inventar, Projekte & Produkte, Vulnerability Management, Incidents & BCM, Gap Analysis & Audits, Regelwerke & Standards (selected), Anwendbarkeitsklärung, BYO Frameworks, Framework Katalog, and Control Browser. Below this is a 'Menu reduzieren' button and a status bar showing 'EU-Region' and 'Online'.

The main area is titled 'Regelwerke & Standards · Framework Composer'. It is divided into three sections: 'FINALISIERTE (0)', 'ENTWÜRFE (4)', and 'NEUE KOMPOSITION'. The 'FINALISIERTE' section shows completed compositions like 'DSA – auto-composed' and 'ISO 27001 – auto-composed'. The 'ENTWÜRFE' section shows drafts like 'DORA ISO 27001 CRA Vantiback' and 'Grundschutz++ • DORA 2024'. The 'NEUE KOMPOSITION' section is active, showing a grid of standards to be added to a new composition. These include:

- REGELWERKE AUSWÄHLEN (2-6)**: A list of standards with checkboxes and tags (T1, T2, T3).
 - BSI Grundschutz++ (German IT baseline protection catalogue - comprehensive ISMS implementation guide, BSI 544 550p) [T1]
 - ISO/IEC 27001 (Anforderungen an ein Informationssicherheitsmanagementsystem) [T1]
 - NIS2 Directive (EU Network and Information Security Directive) [T1]
 - CIS Controls (Praktische bereitstellungsfähige Kontrollen) [T2]
 - NIST SP 800-53 (Security and privacy controls for federal information systems) [T3]
 - DORA (Digital Operational Resilience Act) [T1]
 - ISO/IEC 27701 (Privacy Information Management framework for ISO 27001) [T1]
 - AI Act (Artificial Intelligence Act) [T1]
 - Zero Trust for AI Agents (Security controls catalog for AI agent systems) [T2]
 - CSMS (Cybersecurity & Product Security Management) [T3]
 - DORA (Digital Operational Resilience Act) [T1]
 - ISO/IEC 27002 (Informationssicherheitskontrollen und Leitlinien) [T1]
 - CER Directive (Regulation of electronic communications in 11 sectors, EU 2022/9257) [T2]
 - ISO/IEC 27017 (Cloud spezifische Informationssicherheitsanforderungen) [T2]
 - WDAS 2.0 (Kampfschiffe digitale Identitäts- Rollen- und Trust Services, EU 2024/1188) [T3]
 - ISO/IEC 43001 (AI-Managementsystem-Standard) [T1]

 A 'Neue Komposition' button is in the top right. At the bottom of the main area are buttons for 'Komposition erstellen' and 'Abbrechen'.

Compliance-Lücken schneller schließen.

VamiAI bewertet Controls vor; Menschen prüfen,
entscheiden und dokumentieren.

Gap-Analyse mit Human in the Loop

Interne und externe Audits

CAPA - Programme - Reviews

The screenshot displays the VamiAI audit management interface. At the top right, a user profile for 'audit.lead@vami.grc' is shown. The main header indicates the current view is 'Internal Audits'. The selected audit is 'ISO 27001 2026', which is in an 'UNDER REVIEW' state (indicated by a red box) and has the ID 'INT-2826-B25'. A 'Close Audit' button is visible. Below this, the audit details show 'ISO_IEC_27001' as the standard, 'Lead: Audit Lead', 'Started: 26 Aug 2026', and '3/124 assessed'. The 'Overview' tab is active, showing a progress bar with four stages: 'Planned' (green checkmark), 'In Progress' (green checkmark), 'Under Review' (red circle), and 'Closed' (grey circle). An 'Audit Plan' download button is next to the 'Closed' stage. Below the progress bar, the 'ASSESSMENT PROGRESS' section shows '3 / 124 controls assessed' (2%) and '121 controls still pending assessment'. At the bottom, a summary bar shows '- / 4' and '67%'.

audit.lead@vami.grc
Global Admin

< Internal Audits

ISO 27001 2026 **UNDER REVIEW** INT-2826-B25

ISO_IEC_27001 Lead: Audit Lead Started: 26 Aug 2026 3/124 assessed

Close Audit

Overview Controls 124 Notes Report

Planned In Progress Under Review Closed

Download Audit Plan

ASSESSMENT PROGRESS

3 / 124 controls assessed 2%

121 controls still pending assessment

- / 4 67%

Supplier Risk *automatisieren*

BIA, OSINT, Fragebögen und
Verträge fließen in ein konsistentes
Risikobild.

01 BIA

Kritikalität risikobasiert bewerten

02 INTELLIGENCE

OSINT und Trust Center prüfen

03 CONTRACTS

DPA · NDA · InfoSec Agreements

The screenshot displays the VamiGRAC interface for managing supplier risk. The left sidebar contains navigation menus for Boards, AI Workspace, My Work & Workflows, GRC Graph, Inventories, Business Processes, Processing Activities, AI Use Cases, Information & Data, Assets, Suppliers, People & Accounts, Domains & ASM, Risks & Register, Controls, Evidence, Projects & Products, Vulnerability Management, Incidents & BCM, Gap Analysis & Audits, Regulations & Standards, Contractual Requirements, Policies and Documents, Organization, Settings, and Integrations.

The main content area shows the 'Suppliers' section for 'Microsoft'. Key details include:

- Supplier ID:** SUP-8884
- Company Name:** Microsoft
- Website:** microsoft.com
- Country:** United States
- Address:** This company
- Type:** Cloud Provider
- Devices:** -
- Criticality:** High
- Tier / SLA:** Tier 1 - High
- Updated:** 20. Jul 2026

The dashboard is divided into several sections:

- Overview:** Includes tabs for Overview, Documents, Assessment, BIA & Risks, and Questionnaire.
- Basics:** Provides a summary of the supplier's role and description.
- Ownership & RACI:** Details ownership and roles.
- BIA & criticality:** Displays criticality levels for Confidentiality (High), Integrity (High), and Availability (High).
- Risk summary:** Shows a risk score of 50/100, categorized as 'ELEVATED'.
- Questionnaire classification:** Shows a 'Tier 1 - High' classification based on data sensitivity.
- Compliance & governance:** Includes links to Operations, privacy, AI & notes.

01 GOVERN

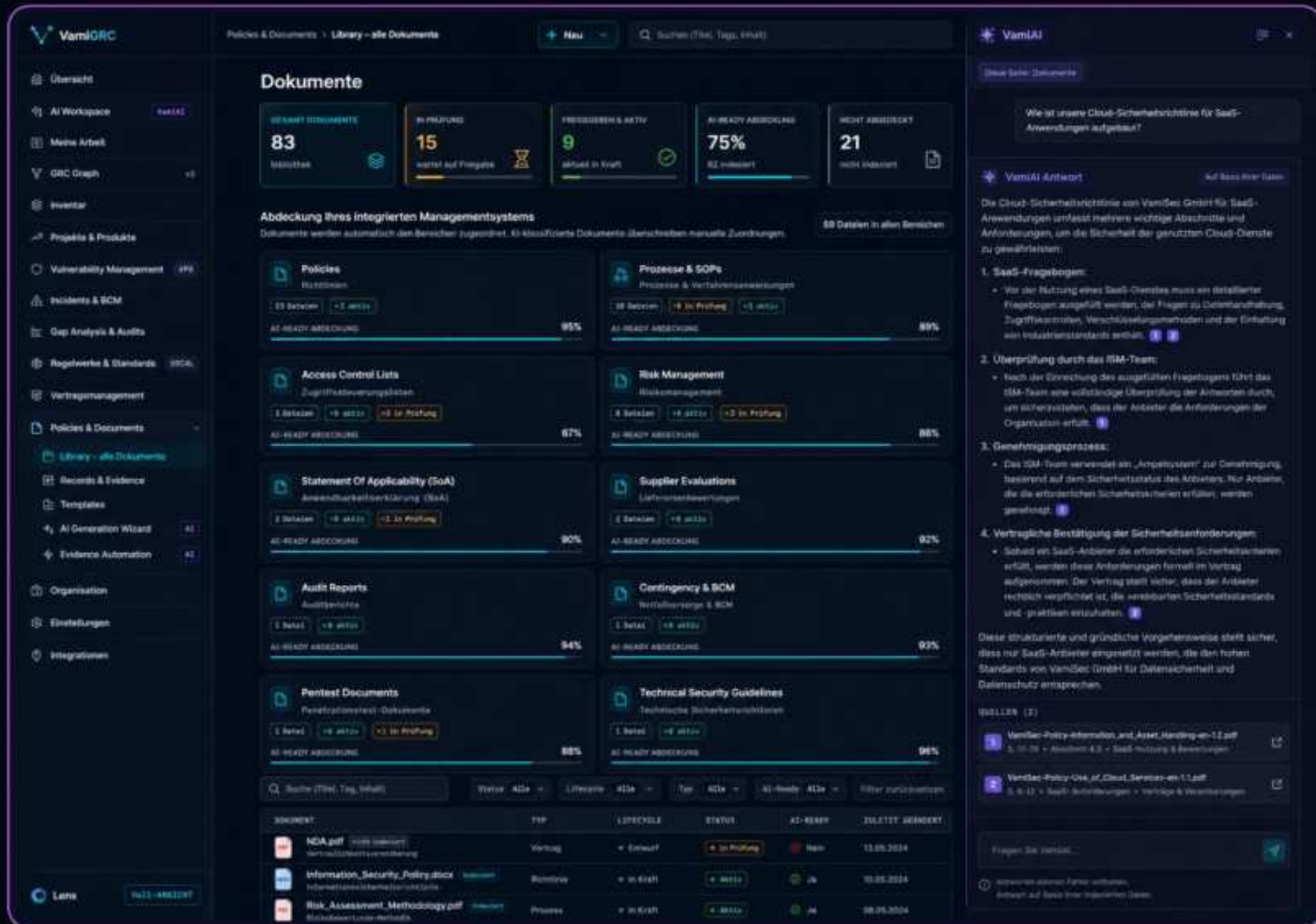
**Freigeben · versionieren ·
inventarisieren**

02 ASK

VamiAI antwortet mit Quellen

03 REFUSE

Wissen auditfähig wiederverwenden



Nachweise *sicher teilen.*

Trust Center und Pakete liefern Kunden, Auditoren und Partnern geprüfte Evidenz.

01 PUBLISH

Policies und Zertifikate veröffentlichen

02 DISTRIBUTE

Compliance-Pakete gezielt verteilen

03 REPORT

Versionen und Nutzung nachvollziehen

The screenshot displays the VamiGRC Trust Center interface. The left sidebar contains navigation options: Projekte & Produkte, Vulnerability Management, Incidents & BCM, Gap Analysis & Audits, Regulatorische Anforderungen, Vertragsanforderungen, Richtlinien & Dokumente, Organisation, Trust Center (selected), Compliance Pakete, Compliance Profile, Zertifikatsregister, Einstellungen, and Integrationen. The main content area is titled 'Trust Center' and shows the 'Website-Einstellungen' (Website Settings) for 'softScheck GmbH'. It includes a 'Trust Center ist live' status, a 'Website mit KI aus Ihrer Seite erstellen' section, and a 'Branding' section with fields for organization name, tagline, primary color, and secondary color. The 'Branding' section also shows a 'Logo' and a 'Domain' field. The 'Trust Center' section includes a 'Trust Center ist live' status, a 'Website mit KI aus Ihrer Seite erstellen' section, and a 'Branding' section. The 'Trust Center' section also includes a 'Trust Center ist live' status, a 'Website mit KI aus Ihrer Seite erstellen' section, and a 'Branding' section. The 'Trust Center' section also includes a 'Trust Center ist live' status, a 'Website mit KI aus Ihrer Seite erstellen' section, and a 'Branding' section.

Trust Center
Erstellen Sie Ihr öffentliches Security- & Compliance-Portal mit Branding, Inhaltsbereichen, Richtlinien und Zertifikaten. Alles, was Sie veröffentlichen, wird rechts unter der öffentlichen URL geändert.

[Seite bearbeiten](#) [Öffentliche Seite ansehen](#) [Live](#)

Portfolio: Website-Einstellungen Dokumente Zertifikate Vulnerability Reports Verteilung Analytics API-Schlüssel Agents

Trust Center ist live
Öffentliche URL: trust.softscheck.com [Statische Seite herunterladen](#) [Veröffentlichung verwalten](#) [Offline behalten](#)

Letzte Veröffentlichung: Heute, 09:42 [Veröffentlicht von System](#) Version: v2.2.1 [Versionsverlauf anzeigen](#)

Website mit KI aus Ihrer Seite erstellen
Geben Sie Ihre Domain ein. KI analysiert Ihre Website, kopiert Ihr Branding (Farben, Logo, Text) und erstellt einen vollständigen Trust Center-Entwurf, der zu Ihrem Design passt - als Grundlage zur Prüfung und Veröffentlichung.

[als Entwurf generieren](#)

Branding

ORGANISATIONSNAMEN
Wie im Trust Center dargestellt:

TAGLINE (OPTIONAL)

PRIMÄRFARBE

LOGO
 [Ändern](#)

☒ Eigenes Domain-Branding aktivieren

Komplettierte Veröffentlichung
Alle Inhalte werden öffentlich verteilt

Sichere Verteilung
Sicherheitszertifikat, Audit und Warten werden

Veränderungen & Historie
Unabhängige Versionshistorie und Wiederherstellung

Nutzungsanalysen
Verfolgen Sie Zugriff und Downloads

Compliance Pakete
Kuratieren evidenzbasierte Pakete für kontrollierte Weitergabe an Kunden und Prüfer.

[+ Neues Paket](#) [Alle Pakete anzeigen](#)

Entwürfe: 2 [Veröffentlichte](#): 5 [Archiviert](#): 1

ISO/IEC 27001:2022 - Kundenpaket [Entwurf](#)

Framework	ISO/IEC 27001:2022
Erstellt	Heute, 10:15
Evidenz	24 Nachweise
Letzte Aktualisierung	Heute, 10:15

[Fortsetzen](#) [...](#)

SOC 2 Type II - Q2 2024 [Entwurf](#)

Framework	SOC 2 Type II
Erstellt	Gestern, 16:45
Evidenz	10 Nachweise
Letzte Aktualisierung	Gestern, 16:45

[Fortsetzen](#) [...](#)

Kürzlich veröffentlicht [Alle anzeigen](#)

NAME	VERSION	VERÖFFENTLICHT	STATUS
ISO/IEC 27001:2022	v2.0.0	22. Mai 2024	Live
SOC 2 Type II - Q1 2024	v1.0.0	10. Apr. 2024	Live
DSGVO - Verarbeitung & Schutz	v1.0.0	22. März 2024	Live

[Verteilungspunkt verwalten](#)
Bezeichnung von Zugriff, Audit und Wiederherstellen

Daten fließen direkt ins GRC.

Konnektoren synchronisieren
Cloud, Identity, Endpoints, Code
und OSINT.

01 DISCOVER

Inventare automatisch aktuell
halten

02 ENRICH

Risiken mit Fakten anreichern

03 ORCHESTRATE

Workflows aus Events starten

The screenshot displays the VamiGRC Integrations Hub interface. The top navigation bar includes the VamiGRC logo, a 'PROD - EU' environment selector, a search bar with the text 'Suche nach Risiken, Assets, Lieferanten ...', and user settings for 'VA'.

The left sidebar contains a 'Projekte & Produkte' section with a list of categories: Vulnerability Management (99%), Incidents & BCM, Gap Analysis & Audits, Regulations & Standards (95%), Contractual Requirements, Policies & Documents, Organisation, and Einstellungen. Below this is an 'INTEGRATIONEN' section with a list of connectors: Integrations Hub (selected), Cloud Provider, Identity Plattformen, Endpoint & Awareness, Verioin Control, OSINT Tools, VamiAI Chatbot (AI), and Task Management & Benachrichtigungen. At the bottom of the sidebar is a 'Lens' section with a 'Voll aktiv' status.

The main content area is divided into three columns. The first column, 'Integrationskatalog', lists various integration categories with their respective counts: Endpoint & Awareness (3/3), Cloud Provider (3/3), Identity Plattformen (2/2), Version Control (2/2), OSINT Tools (1/1), VamiAI Chatbot (1/1), and Task Management & Benachrichtigungen (2/2). The second column, 'Microsoft Intune', shows the connection status as 'Verbindung hergestellt' (Connection established) and 'Jetzt synchronisieren' (Sync now). It also displays the 'Verbindungskonfiguration' (Connection configuration) with fields for 'Verbindungsstatus' (99%), 'Verzeichnis (Mandant) ID', 'Anwendungs-ID (Client)', and 'Client-Geheimnis'. The third column, 'Erkannte Geräte' (Discovered Devices), shows a summary of device status: 1,248 devices (92% with latest type), 1,102 compliant (98%), 98 non-compliant (8%), and 48 unknown (4%). Below this is a table of discovered devices.

GERÄTENAME	PLATTFORM	KONFORMITÄT	LETZTE SEEN
LAPTOP-76263H	Windows 11	Konform	Heute, 09:41
DESKTOP-34URPQ	Windows 10	Nicht konform	Heute, 09:38
MACBOOK-1A367C	macOS 14	Konform	Heute, 09:38
IPAD-BFBE2D	iOS 17	Unbekannt	Heute, 09:33

Security Champions

aktivieren.

Gamification macht Engagement,
Fortschritt und GRC-Reife messbar.

01. GAMIFICATION

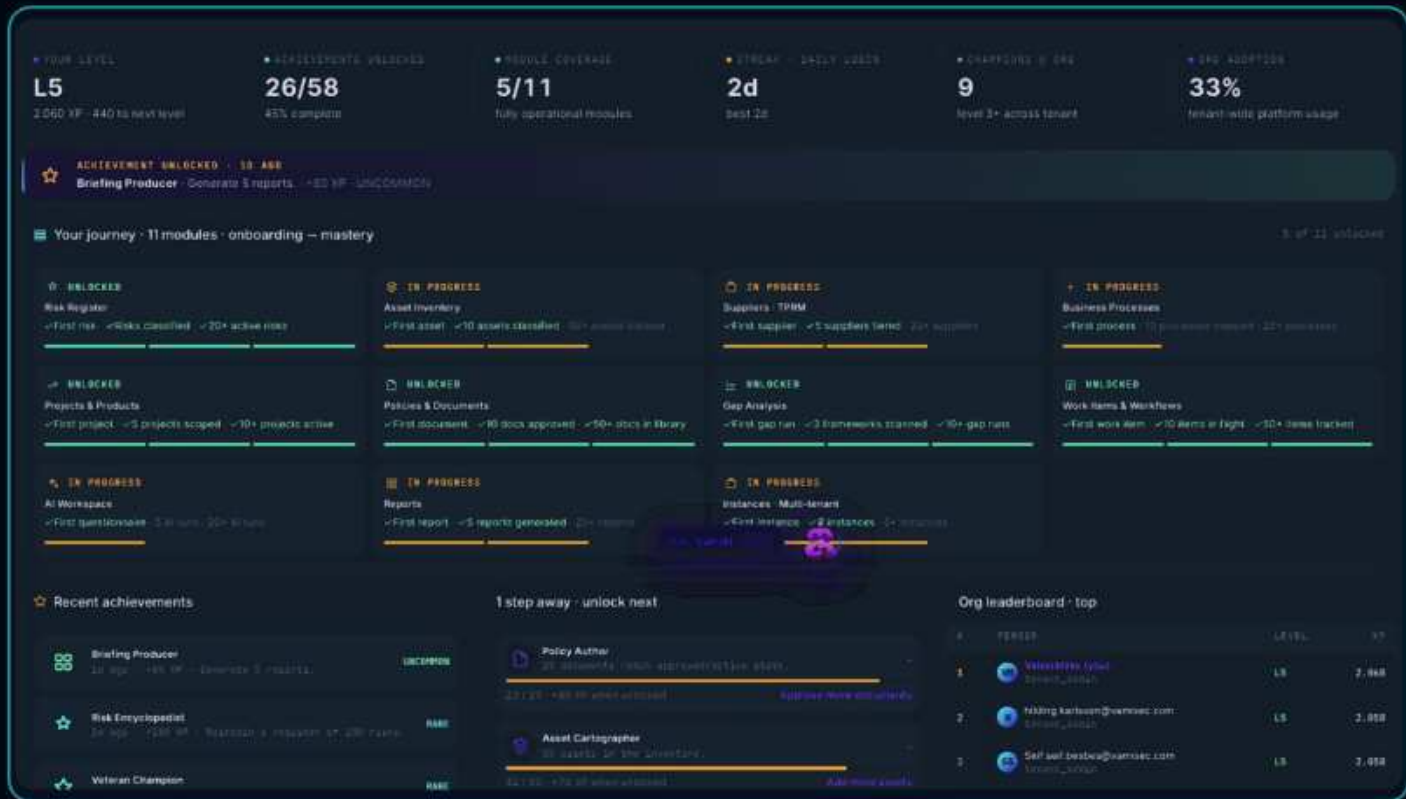
XP · Level · Erfolge

02. CHAMPION-NETZWEK

Engagement im Team verankern

03. GRC-REIFE

Module freischalten · Reifegrad steigern



Live-KPIs steuern GRC.

19 KPIs verbinden Live-Daten,
Zielwerte, Owner und
Berichtsweg.

01 LIVE-DATEN

Abweichungen sofort erkennen

02 VERANTWORTUNG

Owner · Zielwert · Berichtsweg

03 VAMIAI BUILDER

KPIs in natürlicher Sprache
erstellen

KPIs, die dein Team verfolgt.

Operative Kennzahlen über die fünf IMS-Domänen, aus deinen Live-Daten berechnet, je mit Zielwert, Schwellenwert und Verantwortlichem.

REINGEBUNGSEINGABE: 100 bis 4 aus der Tabelle erstellen



KPIs nach Name suchen...

Filter

Domänenübergreifendes KPI-Raster · 19 erfasst

KPI	Domäne	VERANTWORTLICHER	AKTUELL	ZIELWERT	BERICHTSWEG
AI use-case completeness	AI	AI Officer	100%	100%	Quarterly
DPA coverage	DPO	DPO	100%	100%	Quarterly
DPIA coverage on AI use cases	DPO	DPO	100%	100%	Quarterly
Gap findings closure rate	ISMS Manager	ISMS Manager	100%	100%	Quarterly
Internal audit completion	Internal Audit	Internal Audit	100%	100%	Quarterly
Management review approval	Top Management	Top Management	100%	100%	Annually
MTTR - all incidents	CSO	CSO	224.0h	SLA & 72h	Annually
Risk control coverage	ISMS	ISMS	100%	100%	Quarterly

Statusübersicht



ABWICHUNG NACH DOMÄNE



Eigener KPI-BUILDER

Definiere eine Kennzahl in einfacher Sprache, VamiAI übersetzt sie in eine Graph-Abfrage, liefert die Daten und hängt die Quelle an.

Anteil der Schwachstellen nach innerer SLA

Frage nur solche Kennzahlen, denen du

VamiAI fragen

Maßnahmen bleiben bis zur Freigabe sichtbar.

Flexible Boards führen Aufgaben mit Ownern und Fristen durch jeden Bearbeitungsstatus.

Drag-and-drop Statuswechsel

Vorlagen für GRC-Prozesse

Nachrichten und Aufgaben

The screenshot displays a Kanban board interface for 'General Remediation'. The board is organized into five columns representing different stages of a task:

- Open (OFFEN):** Contains a placeholder card 'Karte hierher ziehen' and a '+ Aufgabe hinzufügen' button.
- In Progress (IN ARBEIT):** Contains a card titled 'remediation1' with sub-tasks 'KITTEL', 'Plan', and 'Sicherheitstests'. The card is assigned to 'aziz merhben' with a due date of '01. Okt. 2026'. It also has a '+ Aufgabe hinzufügen' button.
- In Review (IN PRÜFUNG):** Contains a placeholder card 'Karte hierher ziehen' and a '+ Aufgabe hinzufügen' button.
- Approved (FREIGEgeben):** Contains a placeholder card 'Karte hierher ziehen' and a '+ Aufgabe hinzufügen' button.

On the left, a sidebar lists various boards under the heading 'BOARDS'. The 'General Remediation' board is selected and shows a count of 1 task. Other boards listed include 'Awareness and...', 'Change Management...', 'Document Control', 'HR Employee...', and 'Improvement and...'. The top right of the board area includes buttons for '+ Aufgaben hinzufügen' and 'Board bearbeiten'.

Governance ab Projektstart.

Security, Datenschutz und
KI-Compliance begleiten Projekte
von Beginn an.

01 APPROVALS

InfoSec · Privacy · AI freigeben

02 INTEGRATION

Assets · Supplier · Daten
verknüpfen

03 ASSURANCE

RACI und BIA revisionsfähig

The screenshot displays the VamiGRC software interface, which is used for project governance, security, and compliance. The interface is divided into several sections:

- Header:** Includes the VamiGRC logo, a navigation bar with 'Projekte & Produkte' and 'Projekte', and a search bar.
- Left Sidebar:** Contains a navigation menu with options like 'Bereits', 'AI Workspace', 'My Work & Workflows', 'GRC Graph', 'Inventory', 'Projekte & Produkte', 'Schwachstellen-Manager', 'Vorfälle & BCM', 'Gap Analysis & Audits', 'Regulierungen & Standards', 'Vertragsanforderungen', 'Richtlinien und Dokumente', 'Organisation', 'Einstellungen', and 'Integrationen'.
- Main Content Area:**
 - Project Overview:** Displays 'Projekte > PRJ-0001' with a title 'Migration ServiceNow' and a status 'No summary provided'. It includes a 'Design' tab and a 'Kritisch: 30' indicator.
 - Business Owner:** A table showing 'Hybrid' as the business owner, 'INT - EXT' as the system, and '18.5.2027' as the next review date.
 - Overview Tab:**
 - Grunddaten:** Includes fields for 'Projekt-ID', 'Status', 'Business-Owner', and 'Verknüpfte Inventare'.
 - Compliance & Governance:** Includes fields for 'Daten & Datenschutz', 'Verfahrensklassifizierung', 'Personenbezogene Daten verarbeitet', 'DSFA erforderlich', 'KI-Risikodaten', 'KI-Risikoklasse', and 'Automatisierte InfoSec-Bewertung'.
 - Verantwortung & RACI:** A table showing roles and responsibilities for 'Projekt-Owner', 'Security Assessor', 'KI-Governance-Verantwortlich', 'Interne Nutzer', 'Nutzer (Besitz)', 'RPO (Stunden)', 'Nächstes Review', 'Solution Architect', 'Datenschutzverantwortlich', 'Weitere Verantwortliche', 'Externe Nutzer', 'RTO (Stunden)', 'Review-Rhythmus (Tage)', and '365d'.
 - BIA & Kritikalität:** A table showing 'C: High', 'I: Medium', and 'A: Medium' for 'Kritikalität'.

Security begleitet den Produktlebenszyklus.

Acht Phasen verbinden Anforderungen, Nachweise, Threat Modeling und Release-Gates.

CRA · MDR · RED · IEC 62443

TARA & Threat Modeling

SBOM & Gate-Modell

Product Security Lifecycle (PSL)

Manage the security lifecycle, compliance overlays and release gates for this product.

PSL ACTIVE

Overview

Phase

Controls

Threat modeling

Verification & release

Disclosure

Regulator docs

Lifecycle phase (concept 52)

8-phase machine anchored on IEC 62443-4-1 with cross-walks to SSDF, MS-SDL and IEC 81001-5-1.

Step back

Advance >

01_GOVERN

Govern

SR (Security Management)

02_REQUIREMENTS

Requirements

SR

03_SECURE_DESIGN

Secure Design

SD

04_IMPLEMENTATION

Implementation

SI

CURRENT

05_VERIFICATION

Verification

SVV

06_RELEASE

Release

(artifact)

GATE: RELEASE_GATE

07_OPERATE

Operate & PMS

OR + SUN

08_EOS

End-of-Support

SE

→ History · 3 event(s)

→ Show framework mappings

Catalogue v2026.05.A

Alle acht Lifecycle-Phasen bleiben als Steuerungs- und Nachweisstruktur vollständig sichtbar.

DURCHGÄNGIGER PRODUCT SECURITY LIFECYCLE

01	02	03	04	05	06	07	08
Govern	Requirements	Secure Design	Implementation	Verification	Release	Operate & PMS	End-of-Support

8 Phasen · klare Gates · lückenlose Evidenz

Schwachstellen werden nachweisbar behoben.

Pentests, Findings und Remediation laufen in einem kontrollierten End-to-End-Prozess.

Pentests zentral planen

Owner · Fristen · Retests

VamiAI schlägt Maßnahmen vor

The screenshot displays the VamiGRC interface for managing pentests. The left sidebar contains a navigation menu with options like Boards, AI Workspace, My Work & Workflows, GRC Graph, Inventories, Projects & Products, Vulnerability Management, Pentests, Vulnerabilities, Remediation Plans, Threat Intel, Incidents & BCM, Gap Analysis & Audits, Regulations & Standards, Contractual Requirements, and Policies and Documents. The main content area shows the details for a specific pentest engagement, 'PEN-2026-0001', titled 'Pentest Red Team 2026'. It includes tabs for Draft, Not Requested, and Web Application, and buttons for Edit, Preview LoA, Change State, and Cancel Engagement. Below this is a table with columns for Engagement Type, Test Depth, Planned, Actual, and Retest Due. The engagement type is 'External Provider' and the test depth is 'Grey Box'. The table also has tabs for Overview, Scope, Authorisation, Documents, Findings, and History. The Overview tab is active, showing details such as Description, Rules of Engagement, Test Window, Team, Methodology & Frameworks, and Budget & Effort.

VamiGRC PROD-EU Vulnerability Management / Pentests

Home / Pentesting Management > PEN-2026-0001

PEN-2026-0001 Draft Not Requested Web Application Edit Preview LoA Change State Cancel Engagement

Pentest Red Team 2026

ENGAGEMENT TYPE	TEST DEPTH	PLANNED	ACTUAL	RETEST DUE
External Provider	Grey Box	—	—	—

Overview Scope Authorisation Documents Findings History

DESCRIPTION
Not specified.

RULES OF ENGAGEMENT
Not specified.

TEST WINDOW
Not specified.

TEAM
Provider
Lead Tester

METHODOLOGY & FRAMEWORKS
Not specified.

BUDGET & EFFORT
Effort
Amount
Retest Window

Angriffsflächen erkennen. Risiken validieren.

ASM, VamiRedTeam und Dark-Web-Intelligence führen direkt zur Remediation.

[Externe Exposition überwachen](#)[Agentisches Red Teaming](#)[Leaks · Credentials · API-Keys](#)

>

<<

Domains > vamisec.com

 **vamisec.com**

www.vamiredteam.com

Pending Verification

Risk 19 • Low

Owned

Export evidence

Export PDF

Scan settings

Verify ownership

Scan now

Overview

Hosts

Findings

AI Detection

GDPR

History

SEVERITY	CATEGORY	TITLE	CONTROL	STATUS	ACTIONS
Low	Dns Security	Mail (MX) present without an MTA-STS policy	ISO 27001 A.5.14	Open	Resolve Accept False+
Low	Dns Security	No CAA record published	ISO 27001 A.8.24	Open	Resolve Accept False+
Medium	Security Header	Mis	ISO 27001 A.8.26	Open	Resolve Accept False+
Medium	Dns Security	DNSSEC not enabled (no DNSKEY record)	NIS2 Art.21(2)(h)	Open	Resolve Accept False+

Bedrohungssignale werden konkrete Prioritäten.

CISA KEV, NVD und EPSS werden mit Assets, Produkten und SBOM verknüpft.

Relevante CVEs statt Datenflut

EPSS und KEV priorisieren

Betroffenheit automatisch erkennen

The screenshot displays the 'Threat Intelligence KEV / EPSS' dashboard. It features a sidebar on the left with navigation icons. The main content area is titled 'Threat Intelligence KEV / EPSS' and includes a 'FEED FRESHNESS' section with three cards: 'CISA KEV' (Updated 4 h ago, 1.686 entries), 'NVD CVE' (Updated 3 h ago, 383.278 entries, Newest CVE modified: 28. Aug. 2026), and 'EPSS' (Updated 12 h ago, 365.805 entries). Below this is a filter bar with buttons for 'All CVEs', 'KEV Catalog', 'Top EPSS', 'Recent CVEs', and 'CVE Lookup'. A search bar is labeled 'Search CVE id...'. There are also filters for 'All severities', 'Modified since' (with a date picker), and a count of '25 CVEs'. At the bottom, there are radio buttons for 'KEV only', 'Affects you only' (selected), and 'Include suppressed'. A slider for 'Min EPSS percentile' is set to '0ff'. The bottom of the interface shows a table header with columns: 'CVE', 'SEVERITY / CVSS', 'EPSS', 'KEV', 'AFFECTS YOU', and 'MODIFIED'.

Threat Intelligence KEV / EPSS

FEED FRESHNESS

CISA KEV
Updated 4 h ago
1.686 entries

NVD CVE
Updated 3 h ago
383.278 entries
Newest CVE modified: 28. Aug. 2026

EPSS
Updated 12 h ago
365.805 entries

All CVEs ○ KEV Catalog ☆ Top EPSS ⌚ Recent CVEs 🔍 CVE Lookup

🔍 Search CVE id... All severities Modified since tt.mm.jjjj 25 CVEs

☐ KEV only ☒ Affects you only ☐ Include suppressed

Min EPSS percentile 0ff

CVE	SEVERITY / CVSS	EPSS	KEV	AFFECTS YOU	MODIFIED
-----	-----------------	------	-----	-------------	----------

Vorfälle steuern. Meldepflichten erfüllen.

Incidents, Eskalationen und Fristen bleiben in einem gemeinsamen Lagebild.

NIS2 · CRA · DORA

Playbooks direkt starten

Crisis War Room integrieren

The screenshot displays the VamiGRC Incident Management dashboard. The left sidebar contains navigation links for Boards, AI Workspace, My Work & Workflows, GRC Graph, Inventories, Projects & Products, Vulnerability Management, Incidents & BCM (highlighted), Crisis War Room, Playbooks, Reporting Obligations, BCMS, BCP / DR Plans, Tabletop Exercises, Gap Analysis & Audits, and Regulations & Standards. The main content area is titled 'Active Incidents' and features a summary of incident counts: 5 Total, 4 Active, 0 Critical, and 1 Escalated. Below this is a table of incidents with columns for Incident ID, Title, Severity, Status, Level, Assignee, Created, and Actions. The table lists five incidents, including 'Internet-Exposed PostgreSQL Service Detected', 'Phishing attempt in contact@vamisec.com inbox', 'testttt', 'Zero Day Wordpress', and 'Spear Phishing angriff mit KI Deepfake'. The bottom right corner shows 'Per page 50' and a pagination control for page 1.

Active Incidents

TOTAL: 5, ACTIVE: 4, CRITICAL: 0, ESCALATED: 1

Search by number or title...

INCIDENT	TITLE	SEVERITY	STATUS	LEVEL	ASSIGNEE	CREATED	ACTIONS
INC-2026-0005	Internet-Exposed PostgreSQL Service Detected (TCP/5432)...	HIGH	Open	L1	secops@vamisec.com	3 weeks ago	
INC-2026-0004	Phishing attempt in contact@vamisec.com inbox	LOW	Open	L1	secops@vamisec.com	3 weeks ago	
INC-2026-0003	testttt	MEDIUM	Closed	L1	secops@vamisec.com	3 weeks ago	
INC-2026-0002	Zero Day Wordpress	LOW	Escalated	L3	Jean-Pierre C.	last month	
INC-2026-0001	Spear Phishing angriff mit KI Deepfake	MEDIUM	Open	L1	Aziz M.	last month	

Per page 50, Page 1

Playbooks geben Sicherheit.

Vordefinierte und eigene
Checklisten führen Teams sicher
durch jede Incident-Phase.

01 BEST PRACTICES

23 Playbooks sofort nutzen

02 CUSTOM

Eigene Abläufe flexibel erstellen

03 VAMIAI

Strukturierte Reaktionspläne generieren

The screenshot displays the VamSec Incident Response Platform interface. On the left is a sidebar with navigation options: Boards, All Workspace, My Work & Workflows, GRC Dash, Inventories, Projects & Products, Vulnerability Manage..., Incidents & BCM, Incidents, Crisis War Room, **Playbooks + 15+**, Reporting Obligations, BCM / Contin..., UCP / DR Plans, Checklist Exercises, Gap Analysis & Audits, Regulations & Stand..., Contractual Requirements, Policies and Documents, Organization, Settings, and Integrations. The main area is titled 'Incidents & BCM / Playbooks + 15+'. It features a 'Playbooks' section with a grid of 23 pre-defined playbooks. Each playbook card includes its ID, version, title, category, status (Approved/Custom), and a brief description of the incident type and response steps. The playbooks are organized into three columns and seven rows. At the bottom right, there is a 'Generate with AI' button and a user profile icon for 'VamSec'.

PLAYBOOKS	APPROVED	PENDING REVIEW	AI-GENERATED
23	23	0	0

Search by name... Category All Status All

PLAYBOOK ID	VERSION	TITLE	CATEGORY	STATUS	DESCRIPTION
PS-001	v1.1	Phishing Teams	Phishing	Approved	23 phases / 2 steps
PS-002	v1.1	Third-Party Breach	Data breach	Approved	1 phases / 7 steps
PS-003	v1.1	Active Directory Compromise	AD Compromise	Approved	1 phases / 10 steps
PS-004	v1.1	Account Takeover (AD Account)	Account Takeover	Approved	1 phases / 13 steps
PS-005	v1.1	Brute-Force / Credential Stuffing / Password Spraying	Brute Force	Approved	1 phases / 13 steps
PS-006	v1.1	CEO Fraud	CEO Fraud	Approved	1 phases / 10 steps
PS-007	v1.1	Client Malware Detection (KDR)	Client Malware	Approved	1 phases / 18 steps
PS-008	v1.1	Data Breach (Customer Data)	Data breach	Approved	1 phases / 13 steps
PS-009	v1.1	DDoS Attack (Website (AWS))	DDoS (AWS / AWS)	Approved	1 phases / 8 steps
PS-010	v1.1	DDoS Attack (Customer Data)	DDoS (Customer Data)	Approved	1 phases / 9 steps
PS-011	v1.1	Hardware / System Failure	Hardware System Failure	Approved	1 phases / 13 steps
PS-012	v1.1	Lost or Stolen Device	Lost / Stolen Device	Approved	1 phases / 5 steps
PS-013	v1.1	Phishing Mail	Phishing Mail	Approved	1 phases / 23 steps
PS-014	v1.1	Policy Violation	Policy Violation	Approved	1 phases / 8 steps
PS-015	v1.1	Local Admin Privilege Request Handling	Privilege Request	Approved	1 phases / 5 steps

Aut: VamSec 15/2

BCP / DR

vernetzt planen.

BCP- und DR-Pläne verbinden
Prozesse, Assets, Supplier,
Playbooks und Tests.

01 DEPENDENCIES

Abhängigkeiten vollständig
abbilden

02 TARGETS

RTO · RPO · MTPD steuern

03 TESTING

Tests planen · Aktualität belegen

The screenshot displays the 'BCP softScheck' interface. At the top, the breadcrumb 'DR / BCP Plans > BCP softScheck' is visible. The main title 'BCP softScheck' is followed by a 'Draft' status indicator. Below this, a table provides key details: 'OWNER (USER)' is 'Unassigned', 'OWNER (TEAM)' is empty, 'LAST TESTED' is 'Never', and 'NEXT TEST DUE' is '2 months ago'. A navigation bar includes 'Overview', 'Documents', 'Team', 'Playbooks', 'Inventory scope', and 'Testing'. The 'Sections' list on the right includes 'Generate with AI' and 'Edit' buttons. The main content area lists eight sections: 1. Purpose & Scope, 2. Objectives & Recovery Targets, 3. Activation & Invocation, 4. Crisis / Disaster-Recovery Team, 5. Critical Business Processes, 6. Continuity Strategy, 7. Dependencies & Resources, and 8. Communication & Stakeholders. Each section has a brief description of its content.

DR / BCP Plans > BCP softScheck

BCP softScheck

Draft

OWNER (USER)	OWNER (TEAM)	LAST TESTED	NEXT TEST DUE
Unassigned		Never	2 months ago

Overview Documents Team Playbooks Inventory scope Testing

Sections

- 1. Purpose & Scope
Purpose of this Business Continuity Plan, the organisational units / sites / services it covers, and what is explicitly out of scope.
- 2. Objectives & Recovery Targets
Continuity objectives and target metrics — RTO (recovery time), RPO (data loss tolerance) and MTPD (max tolerable period of disruption) for the in-scope services/processes.
- 3. Activation & Invocation
When this plan is invoked, who can declare an incident/disaster, and the immediate first steps after activation.
- 4. Crisis / Disaster-Recovery Team
The team that manages the disruption — roles, named members and deputies, and how they are reached. (Maintained in the Team builder block below.)
- 5. Critical Business Processes
The business processes that must keep running during a disruption, their criticality and max tolerable outage, and — for each — the **alternative (fallback) process** used when the primary is unavailable. (Maintained in the Critical Processes builder block below.)
- 6. Continuity Strategy
How each critical process is kept running — alternative workflows, manual fallbacks, alternate sites/tools, and the resources the fallback requires.
- 7. Dependencies & Resources
People, tools, suppliers and systems the critical processes depend on (inferred from the inventory in the Scope block).
- 8. Communication & Stakeholders

Krisenübungen

realistisch proben.

Tabletop-Übungen verbinden
Szenario, Run Log, Bewertung und
Verbesserungsmaßnahmen.

01 SCENARIO

KI-gestützt entwickeln

02 RUN LOG

Übung und Zeitverlauf koordinieren

03 IMPROVEMENT

Findings in Maßnahmen überführen

cc

Tabletop Exercises · AD Recovery Test

Loading exercise...

AD Recovery Test

Running

PLANNED: 20. 10. 2024

STARTED: 20. 10. 2024

Tests plan: BCP softcheck

Scenario

Run log

Evaluation

Findings

Guided builder

% From a prompt

Scenario

Edit

Attacker type: Opportunistic attacker

Mitre matrix: ENTERPRISE

Pre-opener: 2025 research showed that re-registered abandoned cloud buckets and expired domains still receive millions of update and telemetry requests from fielded devices and software. Your estate includes IoT/edge devices that poll a vendor endpoints for firmware, and that vendor relationship has lapsed.

Opener: Security discovers that the domain/cloud bucket a fleet of devices fetches firmware from has expired and been re-registered by an unknown party — which is now serving unsigned "updates" to your devices that have begun applying them.

Objectives:

- Assess the organization's ability to detect and respond to unauthorized infrastructure changes.
- Evaluate the effectiveness of supply chain security measures.
- Test incident response procedures for handling compromised devices.

1 Abandoned infrastructure identified

The attacker scans for expired domains, dangling DNS, and abandoned cloud buckets that fielded devices still trust and poll. Your devices have no idea their update source changed hands. The trust relationship is the vulnerability, not any device flaw.

TACTIC Reconnaissance

T1595 - Active Scanning

2 Endpoint / domain takeover

The attacker re-registers the lapsed domain or reclaims the bucket the fleet trusts, instantly inheriting the authority to serve those devices. No exploit is needed — the devices come to the attacker. This is supply-chain trust abuse at infrastructure level.

TACTIC Resource Development

T102.001 - Acquire Infrastructure: Domains

3 Malicious update delivered to the fleet

Devices fetch and apply a triggered firmware/update from the trusted endpoint, because they don't verify signatures or pin the source. A single malicious artifact reaches the whole installed base. The team must determine which devices updated and when.

TACTIC Initial Access

T1195 - Supply Chain Compromise

T1195.002 - Supply Chain Compromise: Compromise Software Supply Chain

4 Fleet-wide code execution

The malicious update runs across the installed base, giving the attacker control of many devices at once — potentially safety- or service-critical ones. Containment may require cutting the fleet off from the network. Business and possibly physical impact follows.

TACTIC Execution

T1059 - Command and Scripting Interpreter

5 Impact, eradication & signed-update enforcement

The team blocks the malicious endpoint, forces signed-update enforcement, reclaims or sinksinks the infrastructure where possible, and pushes clean firmware. Devices that can't be trusted may need re-imaging or the leaving fix is signature verification and endpoint lifecycle ownership.

Ask: Vansol

32/

Krisen live koordinieren.

Lagebild, Deadlines und Playbooks bleiben im virtuellen War Room synchron.

Crisis Log live führen

Eskalationen und Fristen steuern

Übung und Ernstfall gleich führen

The screenshot displays the 'Virtual Crisis War Room' interface for incident INC-2026-0002. The interface is divided into several sections:

- Header:** Shows the breadcrumb 'Incidents & BCM > Crisis War Room > INC-2026-0002' and a 'Back to crises' button.
- Incident Card:** Displays 'INC-2026-0002' with status 'CRISIS - L3' (red triangle icon) and severity 'LOW' (green circle icon). The title is 'Zero Day Wordpress' and the crisis manager is '-'. An 'Incident detail' button is on the right.
- Crisis log:** A section for logging events with a text input field 'Add a note to the crisis log... (⌘/Ctrl+Enter to send)' and an 'Add note' button.
- Regulatory deadlines:** A list of deadlines with 'NIS2' labels and 'Overdue' status:
 - Early warning (24h) - Open >
 - Notification (72h) - Open >
 - Final report (1 month) - Open >
- Escalation timeline:** Shows an 'escalated' status with a red dot, 'Analyst Orion', and a 'last month' timestamp.

Konzernweit lokal handeln.

Unternehmen, Töchter und
Business Units teilen Daten
kontrolliert.

01 STRUCTURE

Gruppen transparent abbilden

02 SHARING

Daten gezielt vererben

03 ACCOUNTABILITY

Verantwortung je Einheit erhalten

PROD · EU

Nach Unternehmen, Identifiern oder Schlagwörtern suchen...

Alle 3

Aktiv 3

Inaktiv 0

Demo-Daten 0

Freigaben 2

UNTERNEHMEN	IDENTIFIER	STATUS	DATENFREIGABE	AKTUALISIERT	AKTIONEN
STANDARD V VamiGroup 21. Apr. 2026	vamigroup	Aktiv	Lokal (nicht geerbt)	vor 2 Min.	↗ 👤 🗄
VG VamiSec GmbH 24. Apr. 2026	vamisec-gmbh	Aktiv	1 Quelle (geerbt)	vor 4 Min.	↗ 👤 🗄
SG softScheck GmbH 24. Apr. 2026	softscheck-gmbh	Aktiv	1 Quelle (geerbt)	vor 4 Min.	↗ 👤 🗄

Datenfreigabe & Vererbungsübersicht

Zeigt, welche Unternehmen Dokumente und Inventar von anderen erben. Klicken Sie auf einen Knoten für Details.

— erbt von ● Standard (Elternunternehmen)

STANDARD

V VamiGroup

vamigroup

Lokale Verantwortung

TOCHTERGESELLSCHAFT

VG VamiSec GmbH

vamisec-gmbh

Erbt 1 Quelle

TOCHTERGESELLSCHAFT

SG softScheck GmbH

softscheck-gmbh

Erbt 1 Quelle

Vererbte Inhalte

Dokumente, Richtlinien, Kontrollen und Inventar

Lokale Verantwortung

Jede Einheit bleibt für Risiken, Kontrollen und

Kontrollierte Freigabe

Nur freigegebene Quellen werden vererbt -

Weltkarte — Live Geo Status.



Live-geografische Ansicht von Standorten, Assets, Lieferanten, Datenresidenzen und Personen.



Grenzüberschreitende Datenflüsse als animierte Bögen dargestellt.



Souveränitäts- und Residenzkontext in jedem Knoten.



Echtzeit-Übersicht. Umsetzbare Erkenntnisse.

Wo Ihr Unternehmen aktiv ist — und wohin Daten fließen.

Live-geografische Ansicht von Standorten, Assets, Lieferanten, Datenresidenzen und Personen. Grenzüberschreitende Datenflüsse als animierte Bögen dargestellt.

Filter und Markierungen zeigen Hubs an – pro Region, Datenresidenz, SCC / BCR-Overlays.

Geo/JSON exportieren

Souveränitätsbericht

+ Standort hinzufügen

Weltweite Live-Übersicht

14 Unternehmensstandorte • 1.264 Assets • 87 Lieferanten • 486 Datenaufzeichnungen • 412 Personen
in 9 Regionen • 9 SCC • 3 BCR-Übertragungsmechanismen

14

Standorte

9

Länder

62

grenzüberschreitende
Datenflüsse

87%

Datenresidenz in der EU

0

nicht gemappte Übertragungen

EBENEN

Standorte 14

Assets 1.264

Lieferanten 87

Daten 486

Personen 412

Vorfälle 9

Grenzüberschreitende Flüsse 57

Überlagerung: Angemessenheit

SCC / BCR-Overlays



AUSGEWÄHLTER STANDORT – BERLIN – HQ

Berlin, Deutschland

52.5200° N - 13.4050° E - UTC+01:00

Standorte	1
Assets vor Ort	248
Vertragliche Lieferanten	14
Datenaufzeichnungen	31,2 Tsd.
Mitarbeitende	1.167
Ausgehende Flüsse	18

Souveränität EU - DSGVO

Standort öffnen

Inventar

TOP-DATENÜBERTRAGUNGSROUTEN

Berlin → SE – Stockholm AWS	SCC
Berlin → NY – HubSpot	SCC
Berlin → Tokio – DC Blue	BCR
FFM → Dublin – M365	EU – Angem.
FFM → Mumbai – TCS	SCC + TIA
SYD → Tokio – Übertragungsbrücke	3rd-party SCC

RISIKEN – TOP-ABGELEITET

Cloud-Akt-Exposition (US)	Mittel (4)
BCR-Konzentration (EU)	Hoch (27)
Sanktions-Screening – Lieferanten	Niedrig

Compliance dauerhaft *steuern.*

Regulatorik, Umsetzung und Nachweise als kontinuierliches Betriebsmodell.

REGULATORISCHE BASIS

NIS2 · DORA · EU AI ACT · CRA · ISO/IEC 27001 · ISO/IEC 42001 · ISO 22301 · CSMS

GRC as a Service

Powered by VamiGRC · KI-native Plattform · VamiSec Delivery

DER KONTINUIERLICHE SERVICE-ZYKLUS

01 Gap & Baseline

Status, Scope und Handlungsbedarf sichtbar machen.



02 Roadmap & Priorisierung

Ziele, Reihenfolge und Verantwortliche festlegen.



03 Umsetzung & Nachweise

Maßnahmen umsetzen, Evidenz sichern und Audit Trail führen.



04 Monitoring & Verbesserung

KPIs, Reviews und kontinuierliche Verbesserung steuern.

EXPERTISE BEI BEDARF

Externer CISO · KI-Beauftragter · Policy- & Prozessdesign · Risikoanalysen & technische Maßnahmen

MANAGEMENT-MEHRWERT

■ CONTINUOUS COMPLIANCE

■ MANAGEMENT-TRANSPARENZ

■ WENIGER AUDIT-AUFWAND

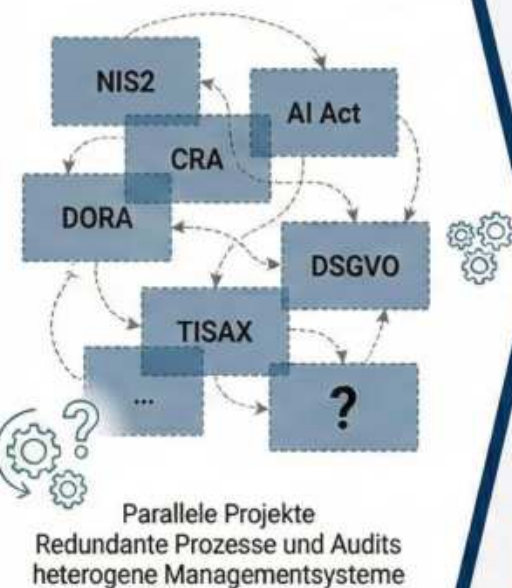
■ SKALIERBAR

■ AUDIT-BEREIT

Ein Betriebsmodell. Eine Datenbasis. Durchgängig audit-bereit.

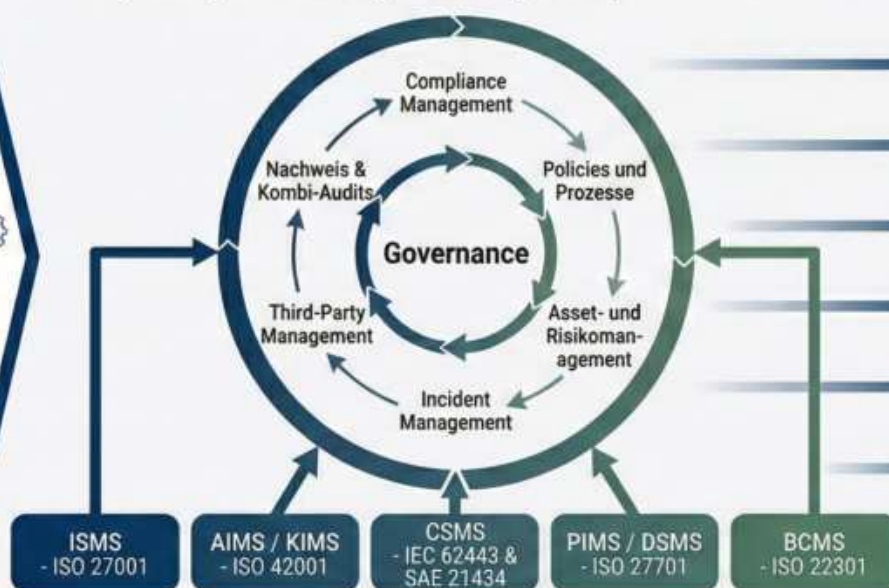
Mit Vami IMS Framework zur integrierten Steuerung regulatorischer und vertraglicher Anforderungen

Fragmentierte Compliance



Vami IMS Framework

Regulierung & Anforderungen → Managementsystem → Standard



Zertifizierbare Compliance



Integrierte Steuerung für nachhaltige Compliance

- Compliance und Nachweisfähigkeit als Vertrauensanker
- Zentrale Risikosicht für das Management

- Mit zertifizierbaren Kombi-Audits zum Wettbewerbsvorteil
- Keine Redundanz & Silos

- Skalierbar für neue Regulierungen
- Nachhaltige Compliance statt Projekt-Compliance

Regulierungen und Anforderungen ändern sich – Vami IMS bleibt.

Regulatorische Anforderungen



NIS2



DORA



KI-Gesetz



CRA



DSGVO

Gesetzliche Verpflichtungen,
durch Aufsichtsbehörden durchgesetzt

Integriertes Managementsystem (IMS)



Governance



Risikomanagement



Kontrollen & Prozesse



Nachweise & Berichterstattung



Kontinuierliche
Verbesserung

Vertragliche Anforderungen (Lieferkette)



TISAX



Kunden-Audits



Lieferantenfragebögen



DORA-Verpflichtungen als
IKT-Dienstleister

Marktgetriebene Verpflichtungen,
durch Kunden durchgesetzt

Berechnen
Sie Ihre
Sicherheits-
investition
nach **ROSI**.

Quantifizieren
Sie Ihre jährlichen
Risikokosten.



01 PARAMETER – EINGABEN

Aus dem Modell abgeleitet – nicht aus Kalkulationstabellen.



UNTERNEHMENSPROFIL

IT-Services • KRITIS • 487 FTE • 130 Mio. € Umsatz

GESCHÄFTSPROZESSE –
BUSINESS IMPACT ANALYSE (BIA)

42 Prozesse • 7 kritisch • MTPD ≤ 4 h an 3



VORGABEN – ANWENDBAR

NIS2 • DORA • GDPR • CRA • EU AI Act



RISIKOLANDSCHAFT – MAXIMUM

GDPR • 4 % Umsatz • 7,2 Mio. €

NIS2 • 2 % • 10 Mio. €

EU AI Act • 7 % / 654 % • 112 Mio. €



VERLUSTMODELL

FAIR • LEF • LM (Monte Carlo • 10.000 Läufe)

02 HAUPTFAKTOR

Kalibrierungsfaktor – Plausibilitätsprüfung
mit Finanzdaten.

0,66%

DER GESAMTEN ADRESSIERBAREN RISIKOFLÄCHE
ÜBER EINEN ZEITRAUM VON 5 JAHRENAnpassbar je nach Konzern, Tochtergesellschaft
oder Einzelgesellschaft.Jede Änderung wird revisionssicher mit Begründung,
Verantwortlichem und Genehmigung protokolliert –
im Rahmen unserer Board-Meetings und Audits.

FAIR

ISO 31000

Monte Carlo

FMEA

DREAD

03 MONETÄRES RISIKO – OUTPUT

So sieht es der Vorstand.

JÄHRLICHE EXPOSURE – GRUPPE

18.121.988 € /Jahr

▼ -18 % YoY

aggregiert • vor der Risikominderung (Residual)
± 12 % KI • 10 % Konfidenzintervall

AUFSCHLÜSSELUNG – NACH GESCHÄFTSEINHEIT

Unternehmens-IT GmbH • EU • 89 kritisch	9.706.388 €
Consulting LAB • IT • 22 kritisch	4.418.233 €
AgenticC&M Inc. • US • 19 kritisch	2.997.378 €
Shared Services • Gruppe-EU	999.989 €

AUFSCHLÜSSELUNG – NACH RISIKOTYP

ANTEIL AN GRUPPEN-EXPOSURE

REGULATORISCH • Bußgelder & Verstöße	7.892.141 €	43,6 %
• GDPR Art. 19 / Art. 32 • personeebezogene Daten	1.245K €	
• NIS2 • Lieferkettenkonzentration & Vorfälle	2.451K €	
• EU AI Act • KI-Risiken • KI im Einsatz	1.536K €	
• DORA Art. 28 • IKT-Drittanbieter-Risiken	846K €	

OPERATIONAL • Ausfall & Ransomware	6.847.229 €	37,8 %
• Ransomware-Ausfall • KRITIS • MTPD ≤ 4 h	4.128K €	
• Lieferketten-Störung • Single-Source SaaS	1.612K €	
• Identität • IAM • Berechtigungen kompromittiert	1.107K €	

OPPORTUNITÄT • Umsatz & Image	3.382.618 €	18,6 %
• Umsatzverlust • CAIO / STAR nicht vorgelegt	1.684K €	
• Kundenabwanderung • Vertrauen / PR-Verlust	928K €	
• Marke & Reputation • Schaden für Lieferkette	878K €	



OSCAL-KOMPATIBEL

CFD-BEREIT

AUDITOR-BEREIT



EXPORTS NACH

FAIR-CAM JSON

EXCEL

POWER BI

VamiSec × softScheck

Regulatorische Exzellenz und technische Tiefe — seit 04/2026 eng verzahnt aus einer Hand.



THE AI-driven IT Security and GRC Experts
TRUSTED · INNOVATIVE · SCALABLE

AI-driven IT Security & GRC

- Integrierte Managementsysteme: ISMS · AIMS · CSMS
- Regulatorik: NIS2 · DORA · CRA · AI Act · ISO 27001/42001
- VamiGRC, Audit Readiness, Evidenz und Management Reporting
- Cloud Security und CNAPP-Umsetzung mit Wiz

 **Bonn** / Germany

Mehrwert für Kunden

Ein Partner statt zwei Beratungen

- **Strategie** Regulatorische Roadmap und Zielbild
- **Umsetzung** Controls, Prozesse und Plattformen
- **Prüfung** Technische Verifikation bis Code und Produkt
- **Nachweis** Auditfähige Evidenz und belastbare Reports



Technische Produkt- & Applikationssicherheit

- Penetration Testing, Threat Modeling und Secure SDLC
- SAST · SCA · SBOM · DAST · Fuzzing
- CI/CD Pipelines, Firmware, Microcode und Software Supply Chain Security
- GRC Kompass für schnelle Gap-Analysen

 **Sankt Augustin** / Germany

— Vom Compliance-Zielbild bis zur technischen Belastbarkeit: klare Prioritäten, weniger Reibungsverluste, schnellere Audit- und Kundenfähigkeit. —

Unsere Expertise ist Ihr Wettbewerbsvorteil.



THE AI-driven IT Security and GRC Experts

TRUSTED · HOLISTIC · ENGINEERED

softScheck
— We identify security vulnerabilities —

Unser Expertise und Branchenerfahrung auf einem Blick - für Ihren Wettbewerbsvorteil

*Wir verbinden tiefe technische Expertise mit regulatorischer Klarheit —
unsere Expertise wird damit zu Ihrem Wettbewerbsvorteil.*

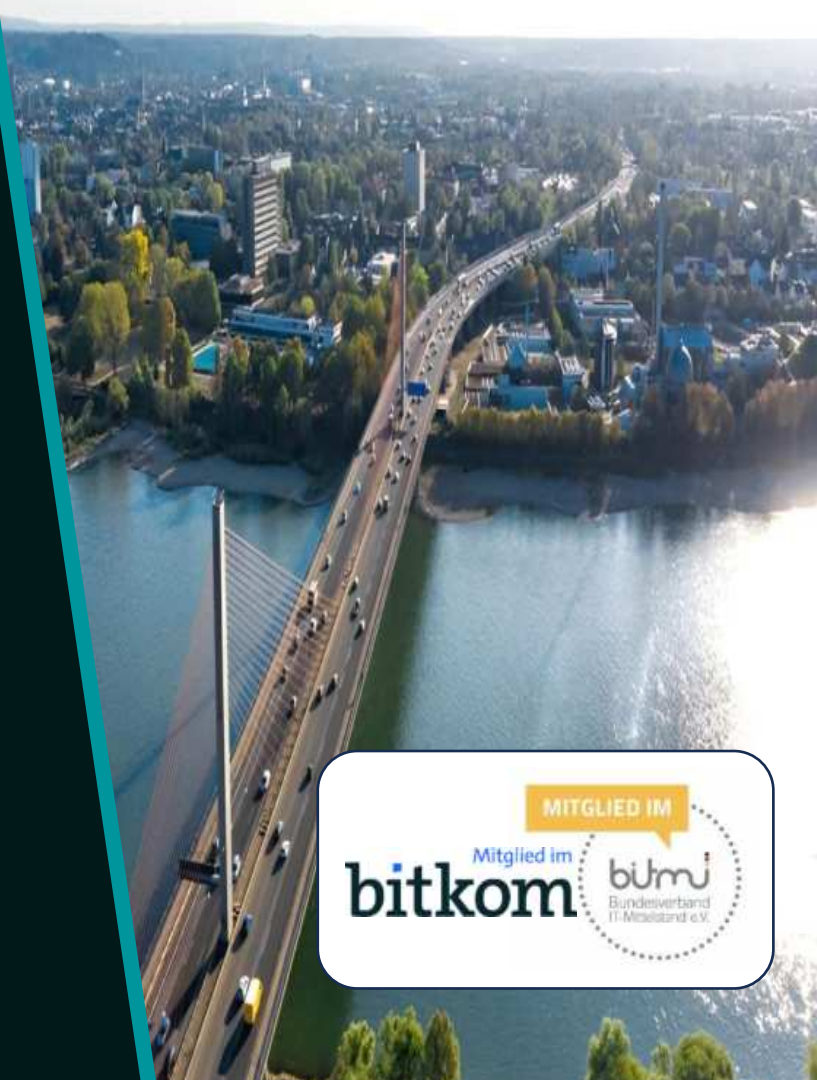


PECB

WIZ



B o n n - 2 0 2 6



VamiSec – Ihr Partner für IT-Sicherheit & GRC



Mehr als 20 Jahre relevante Expertise

- IT-Sicherheit und Compliance
- ISO 27001, CRA, NIS2, DORA, BSIG & KRITIS, BSI IT-Grundschutz, TISAX
- IEC 62443 & SAE 21434 & OWASP SAMM
- Secure Software Development, DevSecOps, Secure CI/CD Pipelines
- Application Security, Threat Modeling, OWASP & CWE
- Produkt- und technologieunabhängige Expertise

Zertifizierte Berater

- ISO 27001 Lead Auditor
- ISO 42001 Lead Auditor
- Zusätzliche Prüfverfahrenskompetenz nach BSIG §8a
- KI-Beauftragter (EU AI Act)
- BSI-IT-Grundschutz-Praktiker
- Datenschutzbeauftragter (IHK)
- NIS2- und CRA-Berater

Inhabergeführt

Hersteller-, Produkt- und technologieunabhängig

Regulierte Branchen



Verteidigung & Luft- und Raumfahrt



Banken & Versicherungen



Kritische Infrastruktur: Pharma, Krankenhäuser & Versorger



Automobil & Transport



Industrie & Fertigung



Softwarehersteller



Fintech- & Krypto-Unternehmen



Handel & Immobilien



Öffentlicher Sektor



National & international



Unsere weitere Expertise



IT-Sicherheit

- Application Security & SDL & OWASP SAMM
- Penetration Testing & Red Teaming
- IT-Security-Audits & Threat Modeling
- M&A-Cybersecurity-Due-Diligence
- Vulnerability Management & Bug-Bounty-Programme
- Threat Detection: Logging & Monitoring
- Deception-Technologien / Honeypots
- Cloud Security (Wiz Partner)
- Incident Response & Cyber-Resilience-Krisenübungen



GRC

- ISMS + CSMS + KIMS + PIMS = IMS
- IT-Notfallmanagement & Business Continuity
- Lieferantenmanagement
- Audits & Zertifizierung
- KI-Compliance & EU-AI-Act-Compliance
- KI-Beauftragter
- ISMS AI-MS KI-Assistent
- ISO 27001, CRA, NIS2, DORA, BSIG & KRITIS, BSI IT-Grundschutz, TISAX
- IEC 62443 & SAE 21434



Managed Services

- **GRC Managed Services:**
 - GRC as a Service
 - vCISO- & vISB-Services
 - KI-Compliance & AI Officer as a Service
 - Compliance as a Service
 - Lieferantenrisikomanagement
- **IT-Security Managed Services:**
 - WIZ: Cloud Security Monitoring (CNAPP & CSPM)
 - MDR & AI SOC
 - Vulnerability Management & Bug-Bounty-Programme
 - Deception-Technologien / Honeypots
 - Incident Response & Cyber Resilience



Zertifizierungen

- PECB Partner
- Training CISO & ISO
- ISO-27001-Zertifizierung für Mitarbeitende
- Awareness-Schulungen und Phishing Kampagnen as a Service
- Zielgruppenspezifische Schulungen (HR, Procurement, Legal,...)
- Schulungen für Administratoren
- Schulungen für Softwareentwickler und -architekten

Vami Group.

20 Jahre technische Sicherheits-DNA, vereint mit AI-nativer GRC-Kompetenz — verbunden durch eine Person von Tag eins nun in einer Hand.

softScheck
— We identify security vulnerabilities —



Prof. Dr. Hartmut Pohl

2006 / 2010

12.04.2011

Forschungsprojekt SoftScheck

H-BRS — Initiator Prof. Dr. Hartmut Pohl. BMBF-gefördert; Partner: Microsoft, SAP, GI/DIA, ULD. Threat Modeling (STRIDE) und DAST/Fuzzing.

softScheck GmbH

Gründung durch Prof. Dr. Hartmut Pohl. Valeri Milke maßgeblich verantwortlich für den operativen Aufbau der technischen Produkt- und Applikationssicherheit als Marke und Praxis mittels des Security Testing Prozess.

04 / 2026



Vami Group
VAMISEC · softScheck

VamiSec und softScheck vereinen sich.
softScheck zu 100% Teil der Vami Group.

Valeri Milke



Gründung VamiSec GmbH

Valeri Milke gründet VamiSec mit dem Anspruch, GRC AI-nativ und integriert neu zu denken.

VamiAI auf OTC

VamiAI zieht von MS Azure auf Open Telekom Cloud — souveräne deutsche Cloud.

Wiz & PECB

Strategische Partnerschaften mit führenden IT-Security- und GRC-Experten: Wiz & PECB

VamiGRC

1. AI-native agentische GRC-Lösung.

2024

11/2025

1/2026

2026



THE AI-driven IT Security and GRC Experts

TRUSTED · HOLISTIC · ENGINEERED



Ihr Ansprechpartner für GRC, Cyber Security und Compliance.

Von der Strategie bis zur auditfähigen Umsetzung.



Valeri Milke

CEO · GRC & Cyber Security Advisor

Erfahrung, die Umsetzung trägt.

- 15+ Jahre Beratung und operative Umsetzung
- Lead Auditor ISO/IEC 27001 & ISO/IEC 42001 · BSI IT-Grundschutz
- Expertise für NIS2, DORA, CRA und den EU AI Act

VAMISEC IN ZAHLEN

20

Experten

150+

Projekte

70+

Kunden

Erstgespräch vereinbaren

QR-Code scannen



Sprechen wir über Ihre nächsten Schritte.