

VamiGRC

Die *KI-native, agentische* GRC-Plattform *für das regulierte Europa.*

Integriertes Managementsystem · OSCAL-konforme Controls · ein abfragbarer Graph — und ein Dialog, der die Arbeit erledigt. Bereitgestellt als SaaS-Plattform, gehostet in der Open Telekom Cloud, made in Germany.

80–95%

Reduktion der manuellen
Compliance-Arbeit

Echtzeit

Time-to-Report
vs. 2–5 Tage manuell

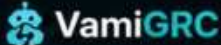
Powered by



THE AI-driven IT Security and GRC Experts

TRUSTED · HOLISTIC · ENGINEERED





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

VamiGRC verbindet integrierte Managementsysteme, agentische Automatisierung und graphbasierte Risiko-Intelligenz in einer AI-native Plattform.



AI-native



Graph-native



Audit-ready



Role-based Lenses

01 · INTEGRIERTES IMS

Ein IMS. Fünf Domänen.

Ein Datenmodell für integrierte Steuerung über mehrere Managementsysteme und Frameworks.



ISMS

· ISO 27001 · NIS2 · TISAX



AIMS

· EU AI Act · ISO 42001



PIMS

· DSGVO · ISO 27701



CSMS

· IEC 62443 · CRA



BCMS

· ISO 22301 · DORA

Einmal modellieren · mehrfach steuern · audit-ready by design

02 · AGENTIC AUTOMATION

Workflows auf Autopilot.

VamiAI unterstützt und automatisiert komplexe GRC-Prozesse – kontrolliert, nachvollziehbar und effizient.



Supplier Intelligence

OSINT, Ratings, AVV, Fragebögen



Risikoanalyse

von Kontext zu Register und Maßnahmenplan



Multi-Framework Audit

domänenübergreifend, weniger Redundanz



Trust Center

Inhalte mehrsprachig und konsistent bereitstellen

Ein Prompt · ein Workflow · der Mensch behält die Kontrolle

03 · GRC GRAPH

Zusammenhänge sichtbar machen.

Der GRC Graph verknüpft Risiken, Controls; Assets, Lieferanten, KI-Use-Cases und Evidenzen über Silos hinweg.



Kronjuwelen, Prozesse und Datenflüsse in einem Modell



Toxische Kombinationen und versteckte Abhängigkeiten sichtbar



Findings mit Quellen und Evidenzen zurückverfolgbar



Cross-domain KPIs, Heatmaps und Geo-Posture in einem Kontext

Silos auflösen · Zusammenhänge verstehen · fundierter entscheiden

Ausschnitte aus VamiGRC

Lenses & Domänen

Choose your Lens

One platform - 10 role-specific views. The Lens reshapes the entire dashboard – terminology, modules, KPIs, default filters – to match your role. Switch any time.

Full IMS

The full executive view across ISMS, AIMS, PIMS, CSMS, BCMS. Cross-domain risk, compliance posture, KPIs, all boards. Built for leadership who lead the integrated management system end-to-end.

ISMS Lens

The classic security view: Risk, Controls, Sub, Internal Audit, Incidents. Aligned to ISO 27001:2022 Annex B - 102 A, 21 TISAX, NIS2, AIMS, PIMS specified.

View all lenses

VamiAI Copilot

Ask VamiAI

Ask GRCsystem

TTT: Eu-Prod

Workflow: Balanced Creative

Lens: Full IMS

VamiAI: ready · scoped to your tenant · audit-logged

Hi Valeri! I'm grounded in your IMS, the GRC Graph and your active frameworks. I can query, analyse, draft and execute – every write goes through your autonomy policy.

Which gaps do we have regarding NIS2? Ask me analysis on asset Class

Pre-prepare this GAO questionnaire

Find toxic combinations across PIMS-AIMS

Geo Posture & Graph View

Worldmap · live geo posture

18 company locations · 1,234 assets · 87 suppliers · 498 data records · 412 people across 8 regions · 8,500 · 3,304 transfer documents

14 Locations · 124 Assets · 87 Suppliers · 89 Data · 498 Documents · 412 People

Berlin, Germany

14 Locations · 124 Assets · 87 Suppliers · 89 Data · 498 Documents · 412 People

Open location · Inventory



Für CISO, DPO, AI Officer, Risk & Compliance Leads – modular, prüfungsorientiert und skalierbar.

VamiGRC macht GRC operativ, intelligent und integrierbar.

VamiSec – Ihr Partner für IT-Sicherheit & Compliance

Relevante Expertise

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

Zertifizierte Berater

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

Inhabergeführt

Hersteller-, Produkt- und technologieunabhängig

Regulierte Industrien



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 / Honeybots
- Cloud Security
- Incident Response & Cyber-Resilience-Krisenübungen



GRC

- Compliance as a Service
- ISMS + CSMS + KIMS + DSMS = IMS
- vCISO & vISB & vKI-Beauftragter
- 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:**
 - ISMS as a Service
 - KI-Compliance & AI Officer as a Service
 - Compliance as a Service
 - vCISO- & vISB-Services
 - Lieferantenrisikomanagement
- **IT-Security Managed Services:**
 - MDR & SOC
 - Vulnerability Management & Bug-Bounty-Programme
 - Cloud Security Monitoring (CNAPP & CSPM)
 - Deception-Technologien / Honeybots
 - Incident Response & Cyber Resilience

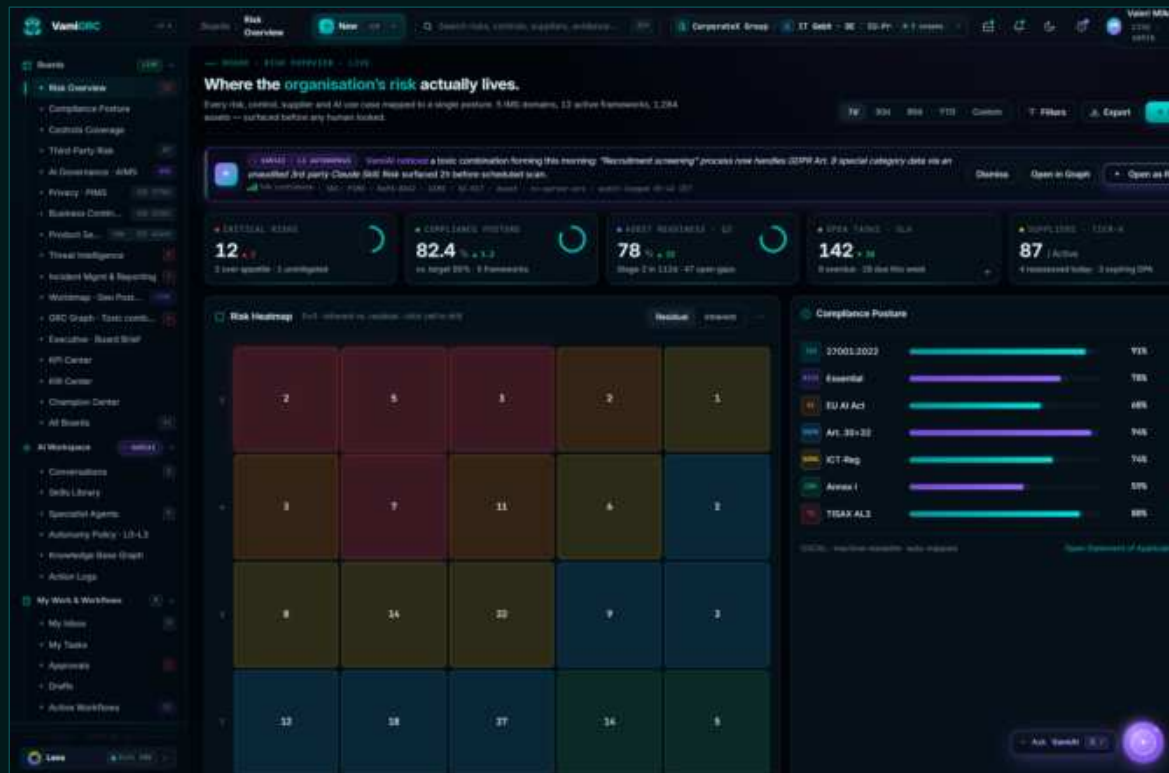


Zertifizierungen

- Training CISO & ISO
- ISO-27001-Zertifizierung für Mitarbeitende
- Awareness-Schulungen
- Zielgruppenspezifische Schulungen
- Schulungen für Administratoren
- Schulungen für Softwareentwickler und -architekten

Risikoübersicht — Ihr tägliches Command Center.

Heatmap, KPIs und Live-Framework-Status auf einen Blick — was Ihr CISO am Montag um 8:00 Uhr sieht.



GRC ist heute ein Engpass.

Dutzende Bildschirme. Eine Frage. Tagelange Verzögerung. Compliance sollte nicht von Heldentaten abhängen.

01

Regulatorische Überlast

CRA · AI Act · NIS2 · DORA · MDR · IEC 62443 — jeweils mit eigenen Nachweisen, Fristen und Audit-Logik.

02

Operative Überlast

Manuelle Risikoanalysen, Fragebögen und Gap-Analysen verbrauchen 60–80 % der Compliance-Kapazität. Teams kämpfen gegen Rückstände, nicht gegen Risiken.

03

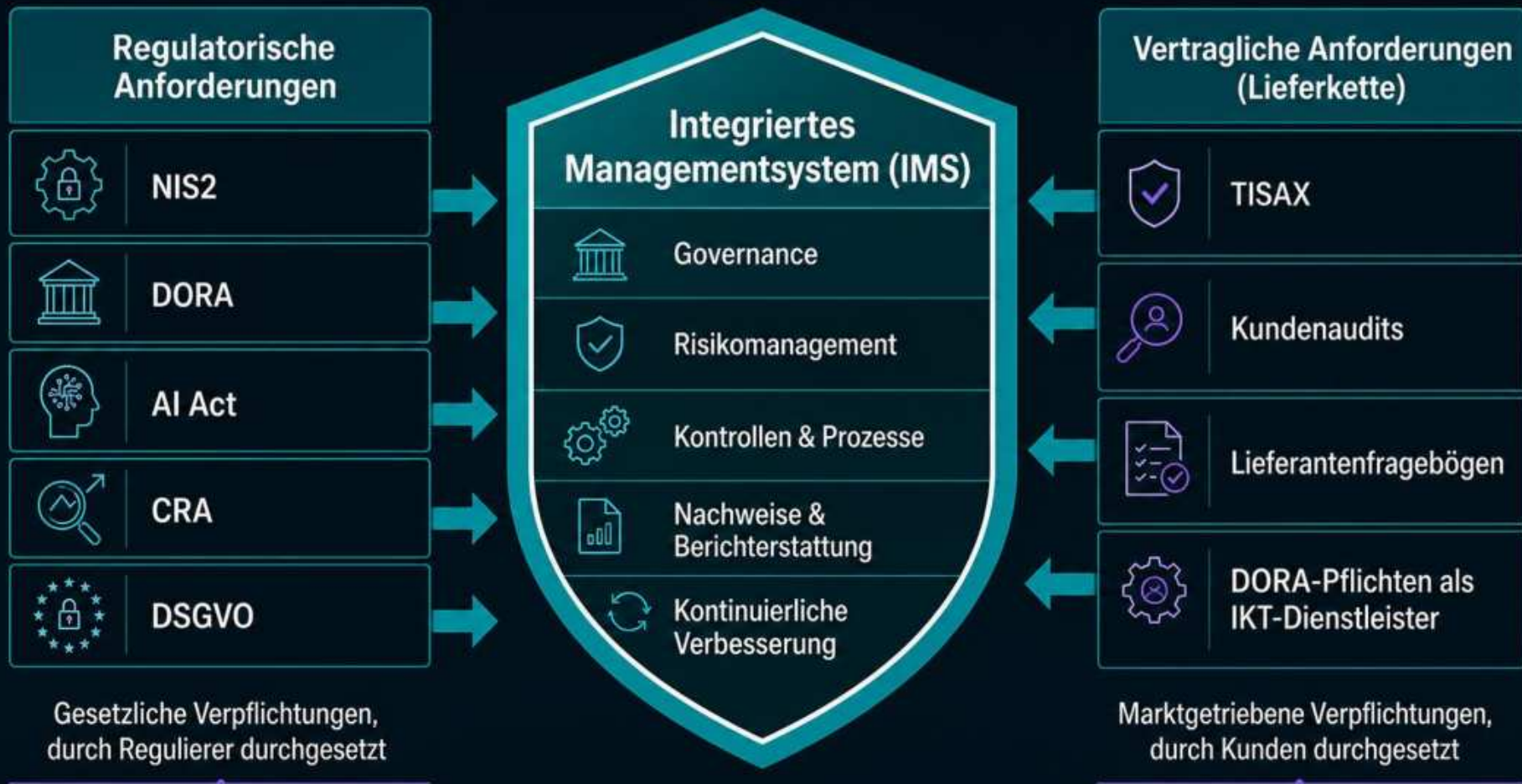
Voneinander getrennte Tool-Silos

ISMS, AIMS, PIMS, BCMS, CSMS — jedes in seinem eigenen Tool, mit eigenem Datenmodell. Redundante Nachweise. Kein einheitliches Bild.

04

Statische Chatbots

Beantworten FAQs, können Ihre Daten nicht abfragen, nicht handeln, nicht schlussfolgern. Tage bis zur Antwort an Auditoren. Wochen bis zum Schließen von Lücken.



EU-Regulatorik für IT-Sicherheit & Compliance



01

IMS-Fundament

Prozesse · Assets · Organisation · Identitäten · Projekte

Fünf IMS-Domänen. Eine Wissensbasis.

VamiAI versteht die gesamte regulatorische und Control-Landschaft — und wie alles zusammenhängt.

ISMS

Informationssicherheit

ISO 27001 · NIS2 ·
SOC 2

AIMS

KI-Management

ISO 42001 · EU AI
Act

CSMS

Produkt- & OT-
Sicherheit

IEC 62443 · CRA

PIMS

Datenschutzmanagem
ent

DSGVO · ISO 27701

BCMS

Business Continuity

ISO 22301 · DORA

Einmal fragen. Antworten über alle Domänen erhalten — mit automatisch sichtbar gemachten domänenübergreifenden Beziehungen.

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
-  Mit zertifizierbaren Kombi-Audits zum Wettbewerbsvorteil
-  Zentrale Risikosicht für das Management
-  Keine Redundanz & Silos

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

Regulierungen und Anforderungen ändern sich – Vami IMS bleibt.

Prozess-Layer — der Geschäftsprozess ist das Fundament.

DSGVO-relevant? → +PIMS-VVT-Layer. KI-gestützt? → +AIMS-Use-Case-Layer. Alles auf demselben Datensatz.

+ AIMS - LAYER

KI-Use-Case

wenn KI beteiligt · EU AI Act · ISO 42001

+ PIMS - LAYER

Verarbeitungstätigkeit (VVT)

wenn personenbezogene Daten · DSGVO Art. 30 · AVV · DSFA

BASIS · IMMER VORHANDEN

Geschäftsprozess

ISMS · BCMS · CSMS · Hierarchie · RACI · CIA · KPIs · Flowchart

IMS - MODUL - INTEGRATIONEN · BIDIREKTIONAL

Asset-Management

Prozess ↔ Asset · CIA-Kaskade

Controls

→ OSCAL · Lücke = Finding

Risikoregister

CIA → Eintrittswahrscheinlichkeit + Maßnahmen

Lieferanten

PIMS = Art.-28-AVVs

Dokumente

SOPs · Richtlinien · Review

Incidents

Betroffener Prozess · Eskalation

Domains (AIMS)

KI-Erkennung → Prozess automatisch anlegen

Personen · RACI

Owner / Vertretung / Reviewer

Informationswerte

Schutz-Kaskade · VVT

Geschäftseinheiten

BU-Filter · Prozesslandkarte

Einmal erfasst – überall genutzt. Keine Duplikation. Keine Fremdschlüssel-Komplexität.

Drei Rollen. Drei Tools. Drei Widersprüche.

Heute arbeiten CISO, Datenschutzbeauftragter und KI-Beauftragter parallel – aber nicht wirklich zusammen.

Mit **VamiGRC**: ein Datensatz, alle Sichten.

HEUTE · ISOLIERTE ROLLEN

CISO, DSB und KI-Beauftragter arbeiten parallel – nicht zusammen.

CISO



Managementsystem:
ISMS

Standards & Regulatorik:
ISO 27001 · NIS2

Eigenes Tool ·
eigenes Register

DSB



Managementsystem:
PIMS

Standards & Regulatorik:
DSGVO · VVT

Eigenes Tool ·
eigenes Register

KI-BEAUFTRAGTER



Managementsystem:
AIMS

Standards & Regulatorik:
EU AI Act · ISO 42001

Eigenes Tool ·
eigenes Register



MIT VAMIGRC · INTEGRIERTES IMS

Ein IMS. Drei Rollen. Eine Single Source of Truth.



CISO · ISMS



DSB · PIMS



KI-BEAUFTRAGTER · AIMS



VamiIMS · ein Datensatz, alle Sichten

- ✗ Derselbe Geschäftsprozess wird dreimal beschrieben – in drei Formaten.
- ✗ Befunde widersprechen sich registerübergreifend.
- ✗ Abstimmung kostet Zeit – Audit-Woche, Meetings, Reibung.
- ✗ GRC bleibt oft papiertigerartig – statt echte Risikoreduktion zu liefern.

- Ein Geschäftsprozess – gelesen als VVT, AI Use Case und Asset.
- Einmal umsetzen – NIS2, DORA, DSGVO und AI Act gleichzeitig adressieren.
- Keine Widersprüche. Keine Doppelarbeit. Ein gemeinsamer Graph.
- GRC wird operativ wirksam – und reduziert Risiken tatsächlich.

Von GRC als Excel als Datenbank mit UI zur agentischen GRC-Plattform.

Während andere GRC-Tools Formulare verwalten, führt VamiGRC Workflows aus. Jeder Compliance-Prozess wird zu einem intelligenten Agenten.

Traditionelle GRC

- ✗ Manuelle Prozesse und Pflege des ISMS
- ✗ Silo-Tools für ISMS, PIMS, AIMS
- ✗ Reaktiv
- ✗ Questionnaires und Gap-Analysen dauern Stunden bis Tage
- ✗ Mensch führt aus
- ✗ Formulare, Checklisten, Bildschirme



VamiAI Agentische GRC

- ✓ Autonome Agenten
- ✓ Vereinheitlichte IMS-Plattform
- ✓ Proaktiv & kontinuierlich
- ✓ Questionnaires und Reportings dauern Sekunden bis Minuten
- ✓ KI führt aus — Mensch genehmigt
- ✓ Dialog, Zitat, Aktion

Ein Prompt. Kompletter Workflow. Risikoregister · Mitigationsplan · Audit-Bericht.

Wiz Partner Alliance · gemeinsamer Markteintritt für regulierte Industrien.

Wiz führt Cloud Security auf G2 an. VamiGRC bringt denselben graphbasierten Ansatz in die GRC. Die Partnerschaft vereint beides für regulierte Unternehmen.



Cloud Security ↔ GRC

VamiGRC

WIZ · CLOUD

Security Graph

Bildet jedes Asset, jede Schwachstelle, jede Identität und jeden Netzwerkpfad ab. Deckt toxische Kombinationen in der Cloud auf.

WIZ × VAMIGRC

Gemeinsame Methodik

Beide ersetzen fragmentierte Befunde durch einen einzigen, abfragbaren Graphen, der toxische Kombinationen über alle Kronjuwelen hinweg sichtbar macht.

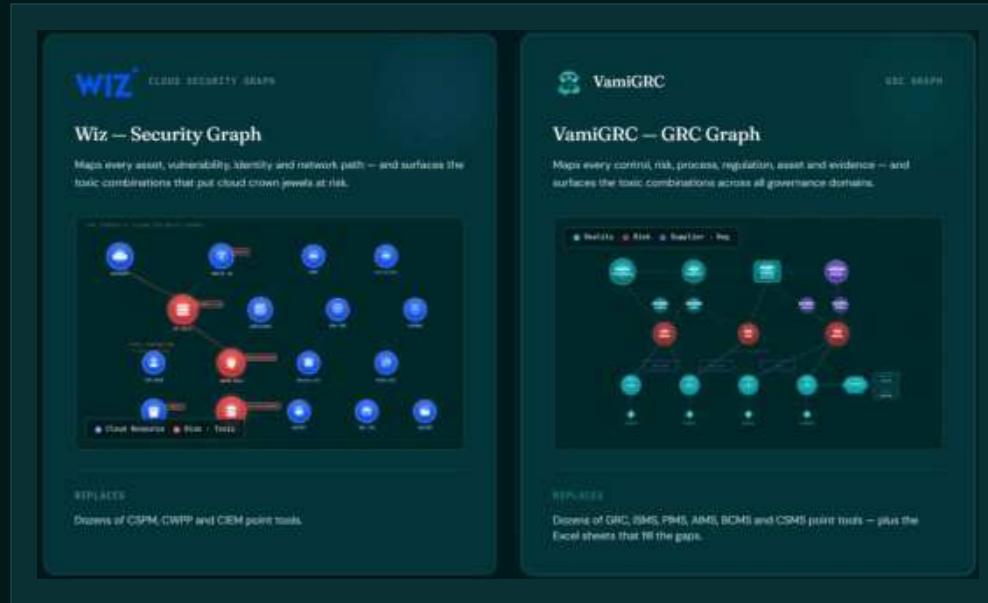
VAMIGRC · GRC

GRC Graph

Bildet jedes Control, Risiko, jeden Prozess, jede Regulierung, jedes Asset und jeden Nachweis ab. Deckt toxische Kombinationen über IMS-Domänen hinweg auf.

Wiz ist für Cloud Security das, was VamiGRC für GRC ist.

Beide ersetzen fragmentierte Befunde, Alarme und Risiken durch einen einzigen, abfragbaren Graphen, der toxische Kombinationen über Ihre Kronjuwelen hinweg sichtbar macht.



WIZ · ERSETZT

Dutzende CSPM- · CWPP- · CIEM-Punktlösungen.

VAMIGRC · ERSETZT

Dutzende GRC-, ISMS-, PIMS-, AIMS-, BCMS-, CSMS-Tools — plus Excel, das die Lücken füllt.

GRC Graph. Wir finden die toxischen Kombinationen über Ihre Kronjuwelen hinweg.

Jedes Asset, Risiko, jeder Lieferant, jedes Projekt und Control — und die Beziehungen dazwischen. Klicken Sie auf einen Knoten zur Inspektion; auf eine Kante, um zu erklären, warum sie existiert.



- **Toxische Kombinationen sichtbar gemacht**
Kritische Risiken · überfällige Nachweise · verwaiste Assets — fünf Statusringe, ein Canvas.
- **Fünf Knotentypen vereint**
Asset · Risiko · Lieferant · Projekt · Control — farblich kodiert über ISMS, AIMS, PIMS, CSMS, BCMS hinweg.
- **Audit-Ready by Design**
Klick auf einen Knoten zeigt Quellmodul, Owner, letzte Prüfung und verknüpfte Nachweise.

GRC-Graph — Schützen Sie Ihre Kronjuwelen: *1824 Knoten, 4 toxische Kombinationen.*

Domänenübergreifender Blast-Radius automatisch sichtbar gemacht. Der Wiz-for-GRC-Moment.



Bewerber-Screening. Eine toxische Kombination über drei Systeme hinweg.

Ein einzelner Geschäftsprozess — Bewerber-Screening — verkettet stillschweigend DSGVO Art. 9, Hochrisiko-Pflichten des EU AI Act und die gesamte Lieferkette eines KI-Anbieters. Erst die Abfrage des Graphen macht es sichtbar.



EIN PROZESS · EIN DATENSATZ

Bewerber-Screening ist eine Zeile im Geschäftsprozessregister — automatisch gelesen als VVT Art. 9 (PIMS) UND Hochrisiko-AI Use Case nach Anhang III (AIMS).

GESAMTE LIEFERKETTE · ASSET-HIERARCHIE

Claude (LLM) ist im Asset-Register. Anthropic liefert es direkt. Aber seine Skills cv-parser-pro und candidate-rater sind Sub-Assets — geliefert von unabhängigen Marketplace-Anbietern ohne AVV.

DIE TOXISCHE KOMBINATION · KRITISCH

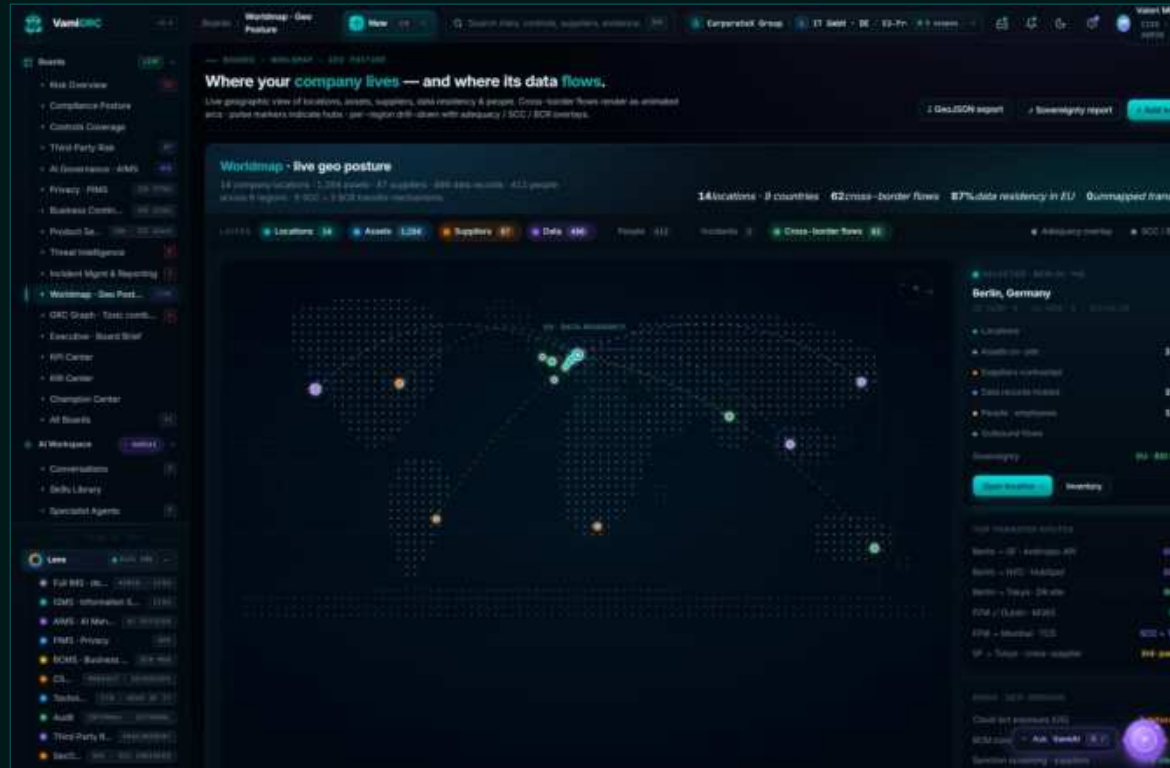
Besondere Kategorien personenbezogener Daten, verarbeitet durch ein LLM über ungeprüfte Drittanbieter-Skills, mit nicht mitigiertem Ursprungsrisiko und nicht implementierten abdeckenden Controls.

WARUM SIE ES NICHT SEHEN WÜRDEN

Jedes Silo sieht ein Teilstück. Nur der Graph sieht das Ganze. DSGVO Art. 9 · EU AI Act Anhang III · NIS2 Art. 21(2)(d) · CRA · DORA Art. 28.

Weltkarte — Live-Geo-Status.

14 Standorte · 9 Länder · 62 grenzüberschreitende Datenflüsse. Adequacy · SCC · BCR Overlays. Souveränitätsbericht auf Knopfdruck.



Integriertes Asset-Management — automatisierte Discovery.

Was Sie nicht kennen, können Sie nicht schützen. Kontinuierlicher Scan · 18 Kategorien · 60+ Felder · BIA auf Autopilot.

Automatisierte Discovery

12+ Quellen: Azure · AWS · GCP · K8s · Wiz · M365 · LeanIX · ServiceNow CMDB · Endpoint · DNS · SaaS.

BIA-Workflow

Owner-getriebenes CIA-Scoring · MTD/RTO/RPO · KI-Vorschläge aus Peer-Daten · Management-Freigabepipeline.

Vollständige IMS-Integration

Jedes Asset klassifiziert über ISMS, AIMS, PIMS, CSMS, BCMS — mit verknüpften Controls, Risiken und Lieferanten.

Schatten-IT-Erkennung

Kontinuierliche Discovery deckt nicht registrierte Cloud-, SaaS- und Dev-Umgebungen auf — leitet automatisch an die Governance weiter.

DISCOVERY → INVENTAR · ≤ 48 H

Erkennen



Dedupe



Klassifizieren



Owner zuweisen



BIA



Risiko



Freigegeben



Registrieren

≥95 %

Inventar-Vollständigkeit

≥80 %

Auto-Discovery-Quote

100 %

BIA-Abschluss (kritisch)

<48 Std.

Onboarding-Zeit

≥70 %

Reduktion des manuellen Aufwands

Organisations- & Unternehmensmanagement.

Gemacht für Konzernstrukturen. Ein IMS · viele Einheiten. Policies werden von Konzern an Tochtergesellschaften vererbt. Lokale Autonomie, wo sie zählt.

Policy-Vererbung

Konzern-Policies kaskadieren zu Tochtergesellschaften. Lokales Override erlaubt, wo lokales Recht oder Scope dies erfordert.

Tochtergesellschaft-Autonomie

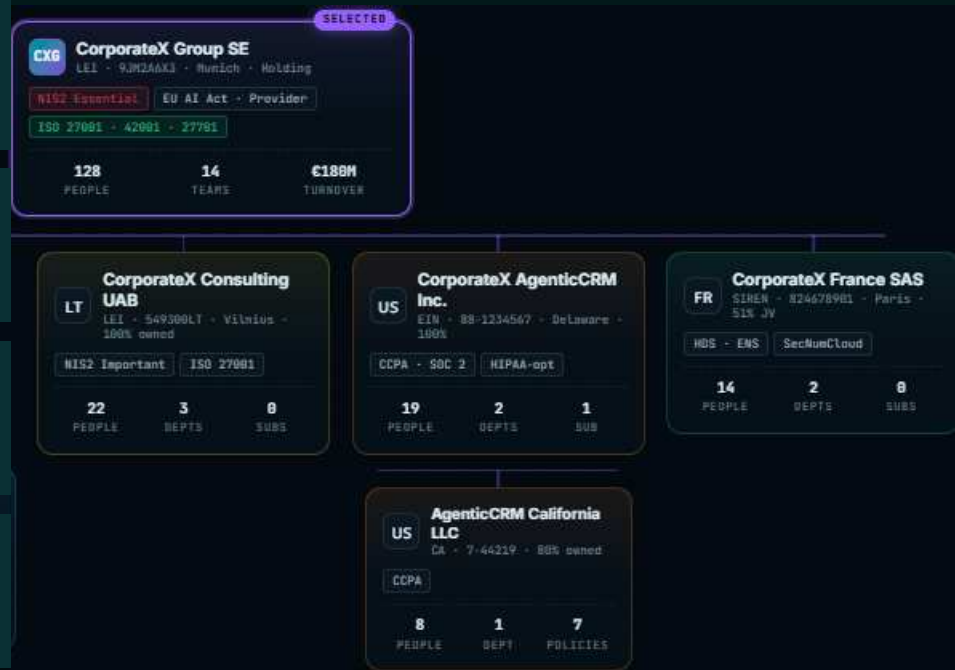
Tochterunternehmen können eigene Policies mit engem Geltungsbereich verfassen — ohne die Konzernkonformität zu brechen.

Rollen & Rechte · Least Privilege

Granulares RBAC: Konzern, Tochter, Geschäftseinheit, Asset. Jede Berechtigung auditierbar.

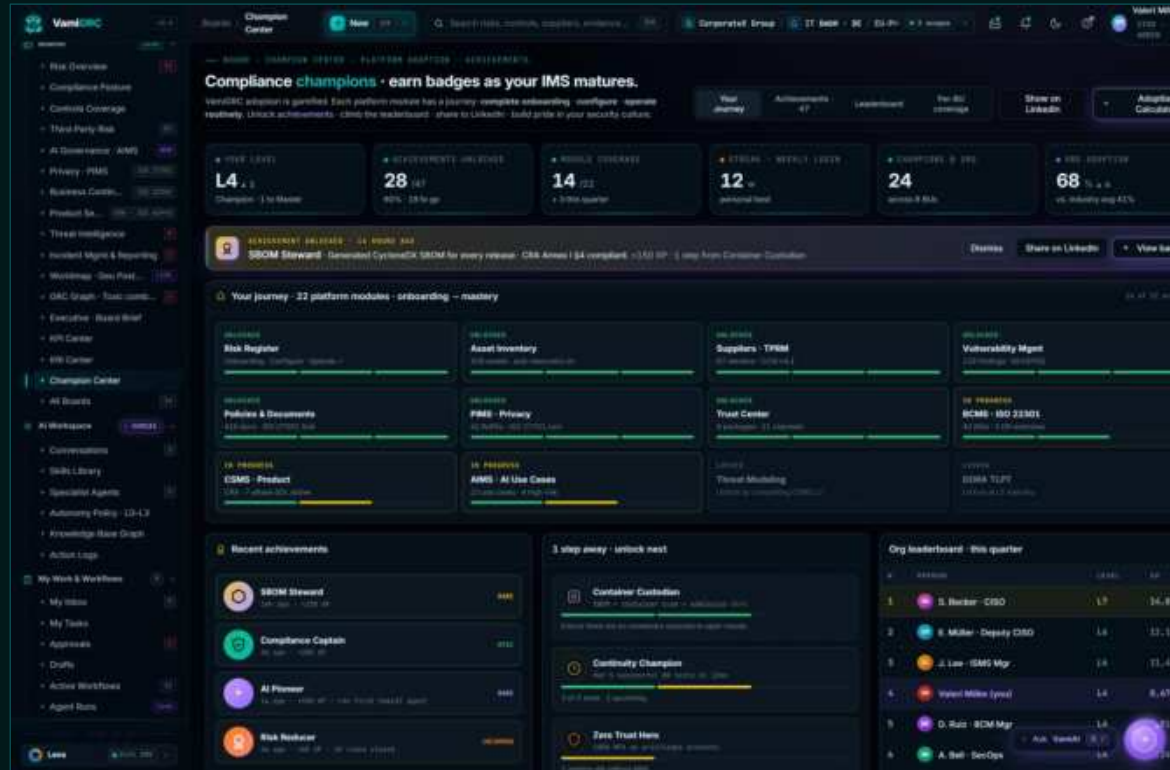
Gemeinsame Assets

Geteilte IT-Systeme, Standorte und Prozesse werden einmal definiert und sind für jede berechnigte Einheit sichtbar.



Champion Center — gamifizierte IMS-Einführung.

22 Module vom Risikoregister über BCMS und AIMS bis TLPT. Org-Leaderboard · auf LinkedIn teilen.



Personen- & Konten-Inventar — Least Privilege.

Azure Entra ID · Google Workspace · HR (SCIM) zusammengeführt in einem Identitätsgraphen. Joiner/Mover/Leaver automatisiert. Least-Privilege-Findings werden ins Risikoregister gepusht.

Search...

All564

Cloud Service Providers32

Kubernetes19

Container Registries9

Software-as-a-Service (SaaS)60

Identity & Directory21

Infrastructure-as-Code12

Endpoint & EDR8

Remediation & Response6

SIEM - Event Origins26

CI/CD5

Developer Tools12

GRC - Audit - Risk Tools14

Vulnerability Scanners11

Communication & Ticketing16

+ MCP Servers42

+ AI Providers5

Cloud Service Providers

Connect your cloud subscriptions for full inventory + posture

View all 32 →

AWS

Amazon Web Services

12 accounts · last sync 2 min

CONNECTED

Connect your AWS to gain visibility into subscriptions security.

Az

Microsoft Azure

tenant + 8 subscriptions

Connect your Microsoft Azure to gain visibility into subscriptions security.

Connect

GCP

Google Cloud Platform

org + projects via SCC

Connect your GCP to gain visibility into projects security.

Connect

OCI

Oracle Cloud (OCI)

tenancy - compartments

Connect Oracle Cloud Infrastructure to gain visibility into security posture.

Connect

vS

VMware vSphere

on-prem hypervisor

Connect vSphere clusters for VM inventory and security visibility.

Connect

SC

Scaleway · IONOS · Hetzner

EU sovereign cloud

Connect EU-sovereign clouds with data-residency guarantees.

Connect

Identity & Directory

SSO · IdP · directory · privileged access

View all 21 →

EN

Microsoft Entra ID

Tenant Azure AD - ingest users, groups, MFA state

CONNECTED

OK

Okta

SSO + lifecycle · Universal Directory + WIC

Connect

JC

JumpCloud

Open directory · device + identity

Connect

CY

CyberArk

PAM · privileged session monitoring

CONNECTED

+ AI Providers

Bring-your-own-LLM · model-routing · in-tenant inference

View all 10 →

A

Anthropic Claude

DEFAULT

G

Google Gemini

O

OpenAI · GPT

M

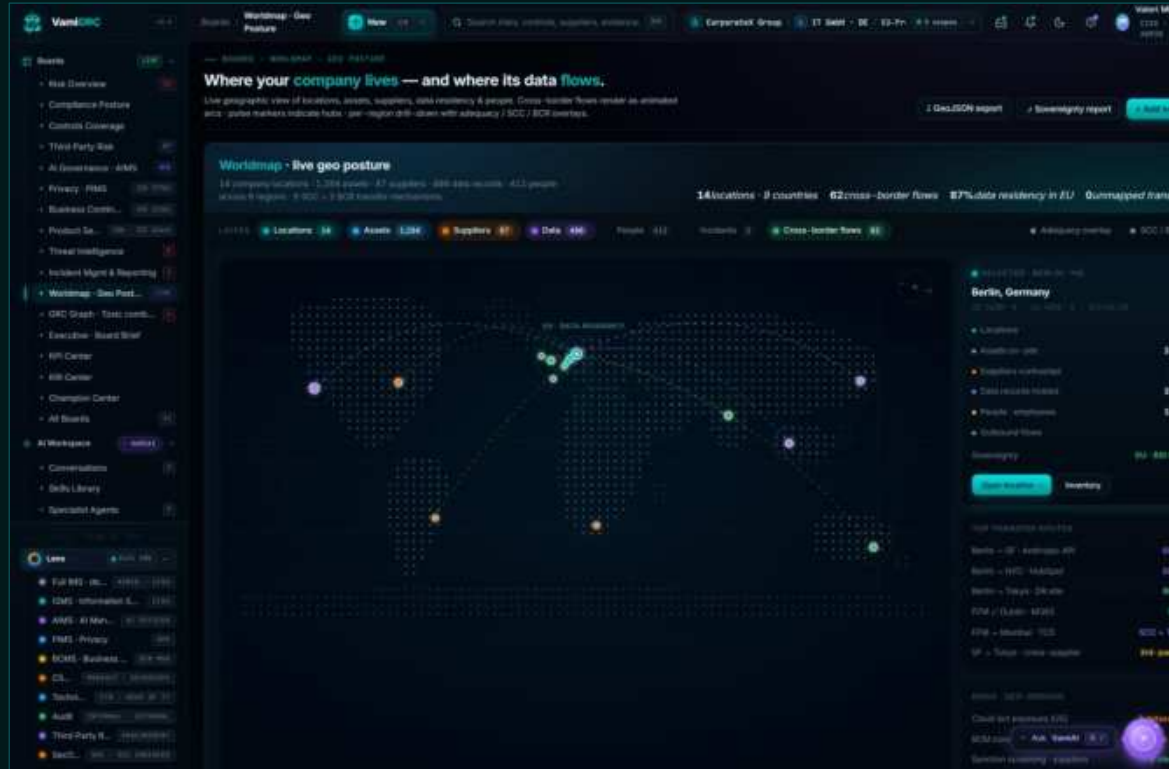
Mistral AI

L

Local · Llama / Ollama

Weltkarte.

14 Standorte · 9 Länder · 62 grenzüberschreitende Datenflüsse. Adequacy · SCC · BCR Overlays. Souveränitätsbericht auf Knopfdruck.



Produkt- & Projekt-Security-Lifecycle und -Management

Intake-Formular · 7-Phasen-Lifecycle mit Phasen-Gates · 81 Baseline-Controls automatisch zugewiesen · VamiRed-getriebenes Threat Modeling und Pentest.

CSMS · PRODUCT SECURITY LIFECYCLE · REGULATION-AWARE · AUDIT-READY

Product Security Lifecycle · CRA-first, multi-framework.

One source of truth for Secure Development Lifecycle, SBOM, PSIRT, CRA Annex II tech-doc, regulatory clocks and end-of-support. Switch the regulation pill to swap phases, gates and required artefacts (CRA · IEC 62443-4-1/4-2 · ISO 21434 · MDR / MDCG 2019-16 · NIST SSDF). All operational data is read from existing modules — Vulnerabilities · Suppliers · Risk Register · Documents · Project Inventory — no duplication.

Annex II pack

Notified Body

VamiAI gate review

PROJECT

PRJ-044 · NordGate X7 · Firmware 4.8

7-phase delivery · gate 5 of 7 · DevSecOps · 12 contributors

→

PRODUCT

NordGate X7 · Industrial IoT Gateway

CRA Class II · IEC 62443-4-1 cert · 10-year support · NXP iMX 8M Plus

5 / 7

SDI PHASE

Verify · pen-test scheduled

98.6 %

SBOM COMPLETENESS

CycloneDX 1.6 + SPDX 2.3 · 1,847 components

14

OPEN PRODUCT CVES

2 KEV · 1 active exploit · 11 backlog

17h 48m

ACTIVE CRA CLOCK

CRA Art. 14(2) · 72h notification

14

RELEASES · 12MO

v4.6.0 → v4.8.1 · OTA adoption 87%

8.2 yr left

EOL WINDOW

manufactured 2024 · 10y commitment

Regulation lens · phases & artefacts swap automatically

AUTO-MAPPED VIA OSCAL PROFILES

EU CRA 2024/2847

IEC 62443-4-1 SDL

IEC 62443-4-2 SL-2

ISO/SAE 21434 Auto

MDR · MDCG 2019-16 RedDev

NIST SSDF SP 800-218

ISO 27034 AppSec

Currently viewing EU CRA · phases reflect Annex I + Art. 13-14 · evidence matrix populated from your tenant. VamiAI can generate cross-framework gap reports per click.

7-phase Secure Development Lifecycle · NordGate X7 · v4.8.0

Switch product

Reduced gate (patch)

01

Reqs

CRA Annex I · PIA · TM scope

passed

62443 SR | SSDF PR

02

Threat Model

STRIDE · DFD · attack surface

approved

62443 SD | 21434 SR

03

Design

Crypto plan · CVE check

peer-reviewed

62443 SD | SSDF PR

04

Implement

SAST · SCA · MISRA-C · CWE Top 25

no Crit/High

62443 SI | SSDF PR

05

Verify

DAST · fuzz · pen-test · SBOM

in progress

62443 SVV | CRA Art. 13(1)

06

Release

Sign · Mender OTA · Annex II

awaiting verify

62443 SUM | SSDF PR

07

Operate

PSIRT · CVE monitor · advisories

awaiting release

62443 DM | SSDF RV | CRA Art. 14

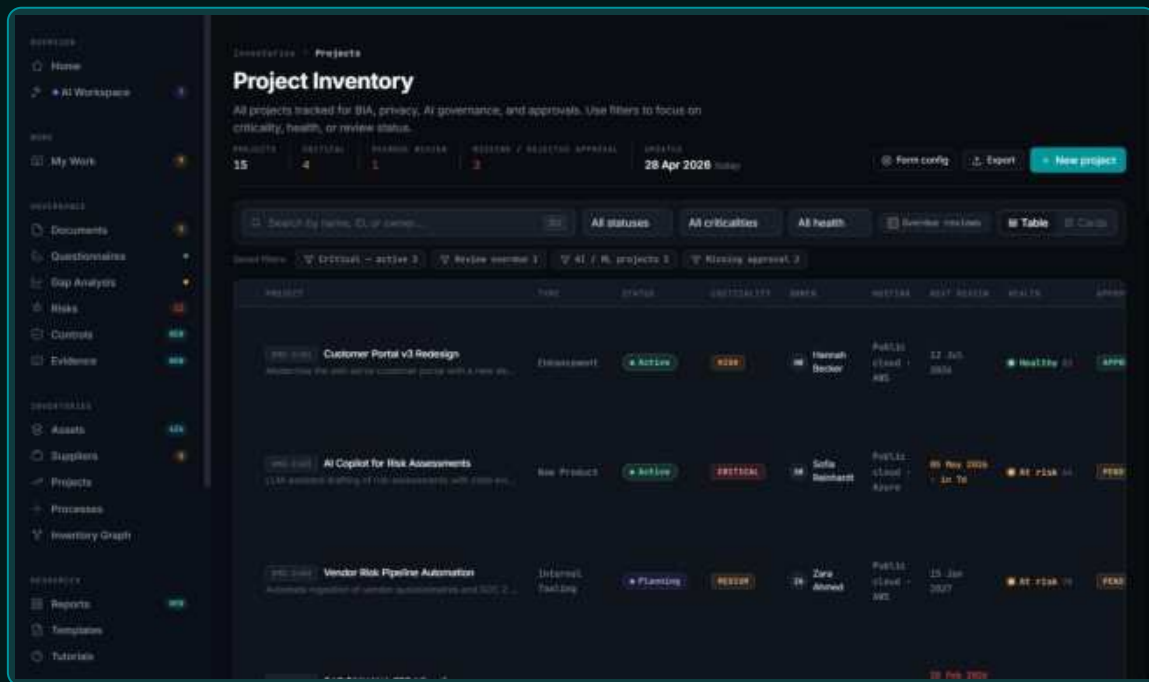
Regulatory clocks · live · CRA Art. 14 active for VLN-0419

Active exploit

Submit to ENISA

Projektinventar — Governance auf einen Blick.

Jedes Projekt nachverfolgt für BIA, Datenschutz, KI-Governance und Freigaben. Filtern nach Kritikalität, Health oder Review-Status — eine Single Source of Truth.



The screenshot displays a 'Project Inventory' dashboard. On the left is a sidebar with navigation links: Home, AI Workspace, My Work, Documents, Questionnaires, Gap Analysis, Risks, Controls, Evidence, Assets, Suppliers, Projects, Processes, Inventory Graph, Reports, Templates, and Tutorial. The main content area is titled 'Project Inventory' and includes a summary of 15 projects, 4 critical, 1 planned, and 3 missing approval, as of 28 Apr 2026. Below this is a search bar and filter buttons for 'All statuses', 'All criticalities', 'All health', and 'Review timeline'. A table lists three projects: 'Customer Portal v3 Redesign' (Active, Critical, Health 80), 'AI Copilot for Risk Assessments' (Active, Critical, Health 80), and 'Vendor Risk Pipeline Automation' (Planning, Critical, Health 80). Each project entry includes details like owner, status, and next review date.

PROJECT	TYPE	STATUS	CRITICALITY	OWNER	NEXT REVIEW	HEALTH	APPROVAL
PROJ-001 Customer Portal v3 Redesign	Enhancement	Active	Critical	Hannah Becker	Pub/131 (Lead - AGS) 22 Jul 2026	Health 80	APPR
PROJ-002 AI Copilot for Risk Assessments	New Product	Active	Critical	Sofia Reinhardt	Pub/131 (Lead - AGS) 06 Nov 2026 1st To	At Risk 40	PRSR
PROJ-003 Vendor Risk Pipeline Automation	Internal Tooling	Planning	Critical	Zara Ahmed	Pub/131 (Lead - AGS) 15 Jan 2027	At Risk 70	PRSR

WARUM DAS ZÄHLT

● 15 Projekte · 4 kritisch

Live-Zählung für überfällige Reviews, fehlende Freigaben und Health-Status — kontinuierlich aktualisiert.

● Gespeicherte Filteransichten

Kritisch-aktiv · Review überfällig · KI/ML-Projekte · fehlende Freigabe — je ein Klick.

● Projekt-Profil

Typ · Status · Kritikalität · Owner · Hosting · nächstes Review · Health Score · Freigabestatus.

Integriertes Control-Inventar — eine Bibliothek, jedes Framework.

Cross-Mapping-Engine: einmal umsetzen, mehrfach erfüllen. Statement of Applicability automatisch generiert für ISO 27001 + ISO 42001 + Unified IMS.

QUELL - FRAMEWORK - BIBLIOTHEK

TIER 1 Kernstandards & Regularien

ISO 27001 · ISO 42001 · NIS2 · DORA · AI Act · DSGVO · CRA · IEC 62443 · ISO 22301

TIER 2 Erweiterte Standards

ISO 27002 · ISO 27701 · TISAX · BSI Grundschutz · BSIG §8a · SOC 2

TIER 3 Best-Practice-Frameworks

CIS Controls · NIST CSF · COBIT · OWASP · SOC2 TSC · MITRE ATT&CK

CROSS - MAPPING - ENGINE

n-zu-n-Control-Beziehungen.

- ISO 27001 A.5.7 ↔ NIS2 Art. 21(2)(h) ↔ DORA Art. 9 — einmal umsetzen, dreifach erfüllen.
- KI-gestützte Control-Discovery: regulatorischer Scan, risikobasiert, Peer-Benchmark, Gap-Analyse.
- Automatisch generiertes Statement of Applicability (ISO 27001 + ISO 42001 + Unified-IMS-Sicht).
- Shared-Responsibility-Modell: pro Projekt, pro Lieferant, pro Control — per RACI nachverfolgt.

Einmal umsetzen. Mehrfach erfüllen. Audit-Ready by Design.

Auf OSCAL aufgebaut. Von Excel zu maschinenlesbaren Controls.

Die vom NIST geführte Open Security Controls Assessment Language als Rückgrat. Jede Regulierung, jeder Standard und jedes Framework als maschinenlesbares XML / JSON / YAML. Audit-Zyklen in Tagen, nicht Monaten.

Tier 1 - Primary Tier 2 - Secondary Tier 3 - Technical Guidelines @ Custom - via OSCAL

Regulations

7 + custom

PRIMARY

NIS2 | ERM AI Act | AIMS GDPR | FIMS

CRA | CMS DORA | RIMS

SECONDARY

DORA | ERM MDR | CMS

TECHNICAL GUIDELINES

EnWG & Sicherheitskataloge HIPAA SOX

PCI DSS SOC 2

YOUR OWN - OSCAL IMPORT

+ Custom regulation

Standards

12 + custom

PRIMARY

ISO 27001 ISO 31000 ISO 27701

IEC 62443 ISO 22301 BSI Grundschutz

SECONDARY

ISO 27002 ISO 42001 ISO 27005

ISO 27014 SAE 21434 ISO 27034

MDCG 2019-16

TECHNICAL GUIDELINES

ISO 27017 / 27018 / 27019

YOUR OWN - OSCAL IMPORT

+ Custom standard

Frameworks

8 + custom

PRIMARY

Cloud Controls Matrix & CAIQ v4.1

CIS Critical Security Controls NIST CSF

SECONDARY

OWASP ASVS OWASP MASVS

OWASP ASVS

YOUR OWN - OSCAL IMPORT

+ Custom framework

BRING YOUR OWN Custom regulations, sector standards or internal frameworks — drop in OSCAL JSON / XML / YAML, and they're live.

EXPORT ANYWHERE Push your full control catalogue, SoA and assessment results out as OSCAL — auditor-ready, machine-verifiable.

CROSS-MAP SPACE Implement an ISO 27001 control once — automatically satisfy NIS2 Art. 21, DORA Art. 9 and your custom framework.

→ BRING YOUR OWN

Eigene Regulierungen, Branchenstandards oder interne Frameworks — OSCAL JSON / XML / YAML einspielen und sie sind live.

→ EXPORT ANYWHERE

Exportieren Sie Ihren gesamten Control-Katalog, SoA und Assessment-Ergebnisse als OSCAL — auditorbereit, maschinell verifizierbar.

→ EINMAL CROSS-MAPPEN

Setzen Sie ein ISO-27001-Control einmal um — und erfüllen Sie automatisch NIS2 Art. 21, DORA Art. 9 und Ihr eigenes Framework.

Maschinenlesbar · Cross-mappbar · Auto-validiert · API-nativ · eigene Frameworks via OSCAL-Import.

Framework-Anwendbarkeit — was, warum, welcher Scope.

OSCAL-basierter Katalog · drei Anwendbarkeits-Treiber · automatisch abgeleitete Baseline · gap-aware ab Tag eins.

TREIBER 1

Rechtsregister

Vorab geladene EU- & nationale Pflichten.
Organisationsprofil (Hauptsitz, Sektor, Größe, KRITIS) wird auf NIS2, DORA, AI Act, DSGVO, CRA, BSI Grundschutz abgebildet.

TREIBER 2

Kundenanforderungen

Verträge, RFPs, Security-Fragebögen. IDP-extrahierte Klauseln binden spezifische Frameworks (ISO 27001, TISAX, SOC 2).

TREIBER 3

Strategische Wahl

Freiwillige Zertifizierungen und Best-Practice-Frameworks (CIS Controls, NIST CSF, ISO 42001), vom Management ausgewählt.

OSCAL - ANWENDBARKEITS - ENGINE · CATALOG → PROFILE → SSP

1

Framework-Katalog

OSCAL-Katalog: vollständige Control-Bibliothek pro Regulierung/Standard.

2

Anwendbarkeits-Profil

Organisationsspezifische Auswahl: welche Kataloge · welches Baseline-Level.

3

Org-Profil-Wizard

Branche · Länder · Größe · KRITIS · KI-Risikoklasse · Cloud-Nutzung.

4

Abdeckungsmatrix

Frameworkübergreifende Sicht: wo ein Control mehrere abdeckt.

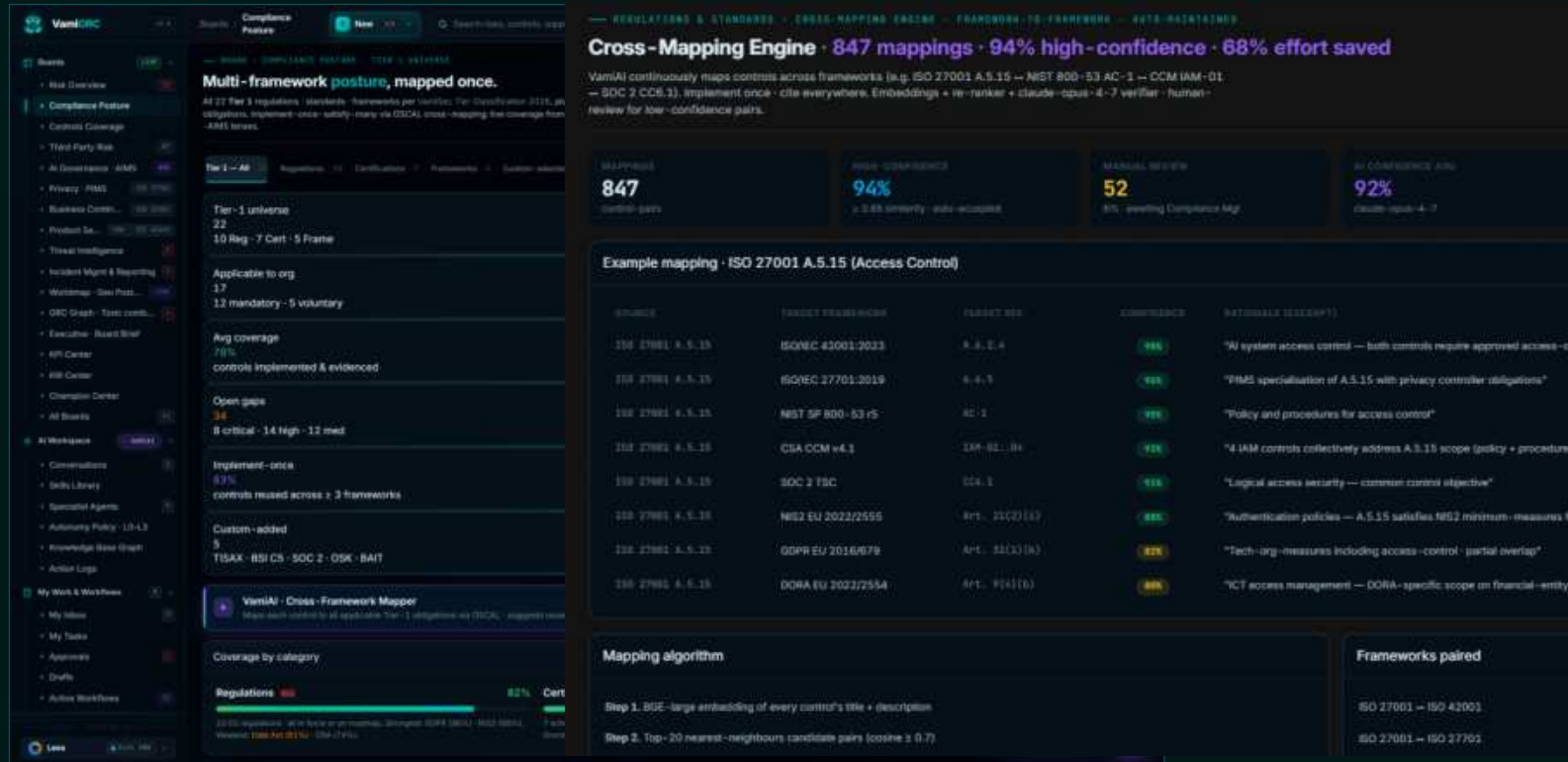
5

Gap-Engine

Ausgewählt ≠ umgesetzt: jede Lücke ein Finding mit Verantwortlichem & Fälligkeitsdatum.

OSCAL Cross-Mapping — einmal umsetzen, mehrfach erfüllen.

22 Tier-1-Pflichten · 81 % Control-Wiederverwendung über 3+ Frameworks · BYO-Frameworks via OSCAL JSON.



Vertragliche Anforderungen — extrahieren, verifizieren, überwachen.

Intelligent Document Processing für Kundenverträge, Partnervereinbarungen und SLAs. KI extrahiert Sicherheitsklauseln; VamiAI verifiziert sie gegen Ihr IMS.

Contracts in · security requirements out · in 6 minutes.

Upload Customer MSA, vendor DPA, MSA, SLA - **scrape** extracts every pending security clause (ISOM provision, MP/ISO, ISO 27001 certification, NIS2/DORA compliance, backup & recovery RTO/RPO, encryption, audit rights, incident notification SLAs), maps each clause to your ISO controls, flags gaps, and triggers risk + workflow tasks. Confidence scored. Audit-logged. Bilingual (EN - DE).

Active contracts | Vendor DPAs | SLAs | Penalty | Clause library | Run history | **+ Upload contract**

ACTIVE CONTRACTS

142 +1

87 customer · 55 vendor

RPN SCORE

18 +1

7 critical · 12 medium

SLA STATISTICS - ISO

2

1 partner · 1 incident notice

NIS2AI EXTRACTED

2,847

requirements parsed · cited

TASKBOARD

94 %

no. backlog NIS2 controls

AUD PROGRESSBAR

5 / 100%

no. 3rd manual/legal review

NEW MSA-2026-087 · Address ISO updated 12 min ago · CI binding requirements extracted · 4 gaps (ISO CS attestation pending) · 4B incident SLA stricter than current 34B

Annual right-to-audit · drafted 1.000000 · 6 implementation tasks for CSO approval.

MSA-2026-087 · SIA · MS-2026-087.pdf · 1 clause LLA · 20% Gap · audit loggap 44 KB PDF

Upload contract - IDP pipeline

+ IDP PIPELINE · **IN DEV**

Drop or click to upload

MSA - DPA - MSA - SLA - MP Agreement - Code of Conduct - Transferor's agreement -
 AUP-language EN - DE - FR - ES - GCH - other parsing
PDF · DOCX · RTF · TXT · CSV · excel

Vendor: **8 emp** IDP: **Claudia** → Extract → Map to controls → Generate gap plan

MOST RECENT EXTRACTS · 52 OVERVIEW

- Security controls** (MFA - SSP - encryption)
- Regulatory** (NIS2 - GDPR - GPPG - CCPA)
- Backup - RTO - RPO - DR test**
- SIEM - SIEM disclosure** (CyberSec/SIEM)
- Right to audit** - pen-test rights
- AI clauses** - AI At Act - model use
- Certifications** (ISO 27001 - SOC 2 - ISO CS)
- Uptime / latency / availability**
- Incident-notification** (clause 34B/73B)
- Sub-processors** - transfers - Art. 28
- Data residency** - jurisdiction
- Exit rules** - return - destruction

Each requirement → mapped to your ISO/NIS2/DORA/GDPR controls → gap extracted → workflow triggered → **VALIDATE** approval required.

Recently processed contracts · click to inspect extracted clauses

NO | Customer | Vendor | Run again | HISTORY

CONTRACT	FILE	STATUS/REMARKS	RPN SCORE	TOP REQUIREMENTS	GAPS	PROCESSING
MSA-2026-087 Master Services Agreement · 14 pages · PDF	Contract	Allroad SE	-15 / 7 open	ISO CS attestation · 4B incident SLA	3 In review	22 min ago
DPA-2026-042 Data Processing Agreement · 8 pages · PDF	Vendor DPA	Anfrispic	10 / 3 open	Sub-processors for transfer mechanism	1 Solved	1 hour ago
SLA-2026-019 Service Level Agreement · 22 pages · PDF	SLA	Microsoft Ireland	10 / 4 open	SLA uptime · 24x7 P1 support	1 Solved	1 hour ago
MSA-2026-081 Master Services Agreement · 19 pages · PDF	Contract	Deutsche Bank AG	10 / 7 open	GDPA · TLP1 - ICT 3rd-party register	1 In review	

MSA-2026-087

VamiAI – In natürlicher Sprache fragen und Anweisungen geben. Antworten erhalten und ausführen lassen.

VamiAI verwandelt Fragen in Graph-Abfragen — gefiltert nach Ihren Berechtigungen, gestützt auf Ihre Nachweise.

The screenshot displays the VamiAI interface, which is designed for natural language interaction with a risk management system. The interface is divided into a sidebar on the left and a main chat area on the right.

Sidebar (Left):

- Top Bar:** Shows the user's name "Ask VamiAI" and the version "v4.7".
- Navigation:** Includes tabs for "contracts", "Vendor DPAs", and "SLAs".
- Coverage:** A green bar indicates "94% COVERAGE" compared to the "Internal IMS control".
- SLA Section:** A section titled "lent SLA stricter than current 24h" is visible.
- Extracts:** A list of 12 categories of extracts, including "Security controls (MFA · SSO · encryption)", "Regulatory (NIS2 · DORA · GDPR · C)", "Backup · RTO · RPO · DR test", "SBOM disclosure · CycloneDX/SPDX", "Right-to-audit · pen-test rights", "I clauses · EU AI Act · model use", "Requirement - mapped to ISO 27001 approval required.", "Requirement", "estation · 4h incident SLA", "error list · transfer mechanism", "time · 24x7 P1 support", "PT · ICT 3rd-party register", and "Compliance scope".

Main Chat Area (Right):

- Header:** Shows the user's name "Ask VamiAI" and the version "v4.7".
- Buttons:** Includes "Precise", "Balanced", "Creative", and "Lens · Full IMS".
- Chat History:** A list of previous messages, including "VamiAI - ready · scoped to your tenant · audit-logged", "Hi Valeri! I'm grounded in your IMS, the GRC Graph and your active frameworks. I can query, analyse, draft and execute — every write goes through your autonomy policy.", "Which gaps do we have regarding NIS2?", "Run risk analysis on asset Claude", "Pre-answer this CAIQ questionnaire", and "Find toxic combinations across PIMS+AIMS".
- Current Message:** A message from the user asking "Which gaps do we have regarding NIS2?".
- Response:** A response from VamiAI stating "I queried the Risk Inventory, Controls Catalog and the NIS2 OSCAL profile. 14 gaps against Art. 21(2) — split by severity:". The response includes a table of gaps:

Severity	Gap
4 Critical	no covering control
7 Partial	maturity below 'Effective'
3 Minor	documentation update

The response also includes a section titled "Want me to take the 4 critical into the Risk Register and create remediation tasks?" with buttons for "Show details" and "Open in Gap Analysis". Below this, there are buttons for "Yes — create risks & tasks" and "Yes — take the 4 critical into the Risk Register and".

Footer: Includes a section for "Skills · Context-Aware" with two cards: "vami-grc-risk-analysis" (ISO 31000/27005 - one-prompt risk register) and "vami-grc-vendor-questionnaire" (CAIQ/SIG/custom - cited - < 5 min). At the bottom, there are buttons for "Attach", "Voice", "Cite", and "Compliance scope".

VamiAI — NIS2-Gap-Analyse, zitiert.

Frage in natürlicher Sprache. 14 Lücken in 8 Sekunden mit zitierten Nachweisen. Anschließend 4 kritische ins Risikoregister übernehmen.

VamiAI in Microsoft Teams — Awareness und Sichtbarkeit über die MS-Teams-Integration maximieren.

ich möchte eine KI-basierte Anwendung entwickeln und in der Azure-Cloud betreiben, welche Regelungen treffen dabei zu?

Zuletzt gesehen

ISMS-Assistent v2 08/11

Bei der Entwicklung und dem Betrieb einer KI-basierten Anwendung in der Azure-Cloud müssen mehrere Regelungen und Richtlinien beachtet werden, um sowohl die gesetzlichen Anforderungen als auch die internen Sicherheitsrichtlinien von VamiSec zu erfüllen. Hier sind die wichtigsten Punkte, die zu berücksichtigen sind:

1. Einhaltung des AI Act:
Die Entwicklung und der Betrieb von KI-Systemen unterliegen spezifischen Regelungen gemäß dem AI Act. Dies beinhaltet besondere Verantwortlichkeiten entlang der gesamten KI-Wertschöpfungskette. Entwickler und Betreiber von KI-Systemen müssen sicherstellen, dass ihre Systeme den gesetzlichen und regulatorischen Anforderungen entsprechen, einschließlich Datenschutz, Urheberrecht, Arbeitsrecht, Gleichstellungsrecht und Schutz von Geschäftsgeheimnissen.

2. Datenschutz und Urheberrecht:
Es ist wichtig, dass die KI-Anwendung keine Urheberrechtsgesetze verletzt, insbesondere bei der Nutzung von Daten, die das System verarbeitet oder erstellt. Zudem müssen Techniken zur Anonymisierung und Pseudonymisierung personenbezogener Daten angewendet werden, um den Datenschutzbestimmungen gerecht zu werden.

3. Verwendung von Cloud-Diensten:
Bei der Nutzung der Azure-Cloud müssen die spezifischen Verantwortlichkeiten im Rahmen des SaaS- (Software as a Service) und FaaS- (Function as a Service) Modells beachtet werden. Während der Cloud-Anbieter die Infrastruktural- und Plattform-Sicherheit übernimmt, ist VamiSec verantwortlich für die Verwaltung von Benutzerkonten, Zugriffsrechten und Datenmanagement. Im FaaS-Modell ist VamiSec für die Sicherheit des Codes verantwortlich, der als Funktionen ausgeliefert wird, sowie für die Kontrolle der Funktionsausführung und das Management von Benutzerberechtigungen und Identitätszugriff.

4. Sicherheitsmaßnahmen:
Es müssen Sicherheitsmaßnahmen angewendet und die Anwendungsumgebungen kontrolliert werden, um die Datenintegrität und -sicherheit zu gewährleisten. Dies umfasst auch die Verwaltung von Benutzerberechtigungen und Identitätszugriff, um unbefugten Zugriff zu verhindern.

5. Regelmäßige Überprüfung und Compliance:
Die Einhaltung der AI- und Cloud-Richtlinien sollte regelmäßig überprüft werden, um sicherzustellen, dass alle gesetzlichen und internen Anforderungen erfüllt werden. Dies beinhaltet auch die Durchführung von Sicherheitsüberprüfungen und Audits, um potenzielle Schwachstellen zu identifizieren und zu beheben. Durch die Beachtung dieser Regelungen und Richtlinien kann sichergestellt werden, dass die Entwicklung und der Betrieb der KI-basierten Anwendung in der Azure-Cloud sowohl sicher als auch gesetzeskonform erfolgt.

Referenced Documents

- Use Of AI Systems PDF Policy
- Use Of Cloud Services PDF Policy

Nachrichte eingeben



Vier Autonomiestufen. Sie entscheiden, wo jede Aufgabe verortet ist.

Adaptiert aus OWASP APTS für die GRC-Domäne. Jeder Schreibvorgang fällt in eine definierte Autonomiestufe. Keine stille Automatisierung. Immer auditierbar.

LEVEL	NAME	AUSFÜHRUNG	FREIGABE	USE CASES	RISIKO
L0	Manuell	Mensch führt alle Arbeiten aus. KI leistet keine Unterstützung.	Standard-Workflow	Ad-hoc · sensible Entscheidungen · Management-Reviews · Budget-Freigaben	Keines
L1	KI-unterstützt	Mensch führt aus; KI liefert Entwürfe und Vorbefüllungen.	Standard-Workflow	Risikobewertungen (KI schlägt Scores vor) · Policy-Reviews · Fragebogenanalyse	Niedrig
L2	KI-ausgeführt + Freigabe	KI führt autonom aus. Ergebnis erfordert menschliche Freigabe.	Verpflichtend vor Abschluss	Lieferanten-Assessments · Gap-Analysen · Access-Reviews · Nachweis-Entwürfe	Mittel
L3	Vollständig autonom	KI führt aus und schließt ab — ohne menschlichen Eingriff.	Nur Information · auditiert	Kontinuierliches Monitoring · Zertifikatsablauf · OSINT-Anreicherung · Routine-Scans	Hoch

VOLLSTÄNDIGE AUDITIERBARKEIT Jeder Prompt, Tool-Aufruf und Schreibvorgang wird mit Zeitstempel, Modellversion und Reasoning-Trace protokolliert.	AI ACT READY Audit-Trails erfüllen die Logging-Anforderungen aus EU AI Act Art. 12. Exportierbar für Aufsichtsbehörden.	HUMAN IN THE LOOP L2 erzwingt verpflichtende menschliche Freigabe. L3 kann jederzeit pausiert, überprüft und zurückgesetzt werden.
--	---	--

AIMS — ISO 42001 + EU-AI-Act-Board.

23 KI-Use-Cases · 5 Hochrisiko-Anhang-III · FRIA-Timer · Post-Market-Monitoring · ISO-42001-Abdeckung 81 %.



02

Security Operations

Pentest · VPS · ASM · Risiko · Audit

Pentesting-Management.

Planen. Autorisieren. Durchführen. Verifizieren.

— Findings = Schwachstellen, end-to-end gesteuert.

DREI URSPRUNGS - PFADE

01

Aus einem Projekt

Ausgelöst am Build- & Test-Gate.
Findings blockieren Go-Live.

02

Aus einem Asset

"Pentest planen"-Button pro Asset.
Wiederkehrend nach Kritikalität.

03

Standalone

TLPT (DORA), KRITIS, M&A, Bug-Bounty-Triage.

— OPERATIONS · PENTESTS · 3 ORIGINATION PATHS · 10-PHASE LIFECYCLE · 18 FRAMEWORKS · 4 VAMIRED ENGINES · 9 AI SUB-AGENTS

Pentests · 12 active engagements · 87 open findings

Complete pentest management aligned to PTES · OSSTMM · NIST SP 800-115 · BSI IS-Pentest plus the OWASP family (WSTG · MASTG · ASVS L1/L2/L3 · MASVS · AISVS · ISVS · SCVS). Engagements originate from **Projects** (auto on Build & Test or Go-Live gate · SEC-01), from **Assets** (recurring per criticality: Critical 6m / High 12m / Medium 24m / Low 36m), or as **Standalone** (TLPT · DORA · KRITIS · Bug-Bounty · M&A). Every engagement carries a signed **Letter of Authorisation** · scope is **frozen post-authorisation** · evidence is **chain-of-custody-tracked**. Findings flow into the unified **Vulnerability inventory** with **VPS** scoring and SLA-based remediation. **VAMIRED** automates 4 specialised engines (IT · AppSec · Mobile · AI) and 9 AI sub-agents handle triage, scoping, authorisation, import, asset correlation, framework classification, deduplication, and retest.

ENGAGEMENTS ACTIVE

12

2 fieldwork · 4 reporting · 3 verification
· 3 scheduled

PENTEST COVERAGE RATE

94%

Critical assets within SLA · target ≥ 90%

MTTR - CRITICAL

5.2 d

SLA 7 d · + -1.4 d QoQ

SLA ADHERENCE

96%

target ≥ 95%



VamiAI Pentest Programme: Project P-2026-Talent-AI just entered Build & Test → I auto-created PEN-2026-0042 (AI Red Team · AISVS + LLM Triaging) · Letter of Authorisation drafted · awaits AI Officer + DPO. **Heads-up:** 2 Critical findings in PEN-2026-0038 are 6 days into the 7-day SLA — escalation auto-drafted.

Project-origin

01

From a Project (auto)

Auto-triggered on Build & Test or Go-Live phase-gate when SEC-01 is in scope. Scope = linked project assets. Findings flow back as a phase-gate verdict (Critical/High open ⇒ blocks Go-Live).

Owner: Security Assessor · Authoriser: PM · Business Owner

Asset-origin

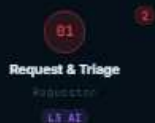
From an Asset (recurring)

Manual ("Plan Pentest" button on every asset detail) or scheduled (recurring per criticality: Critical 6m / High 12m · Medium 24m · Low 36m or on-change. Refreshes findings, score, vulnerability counts).

Owner: Application Owner · Authoriser: Business Owner + DPO

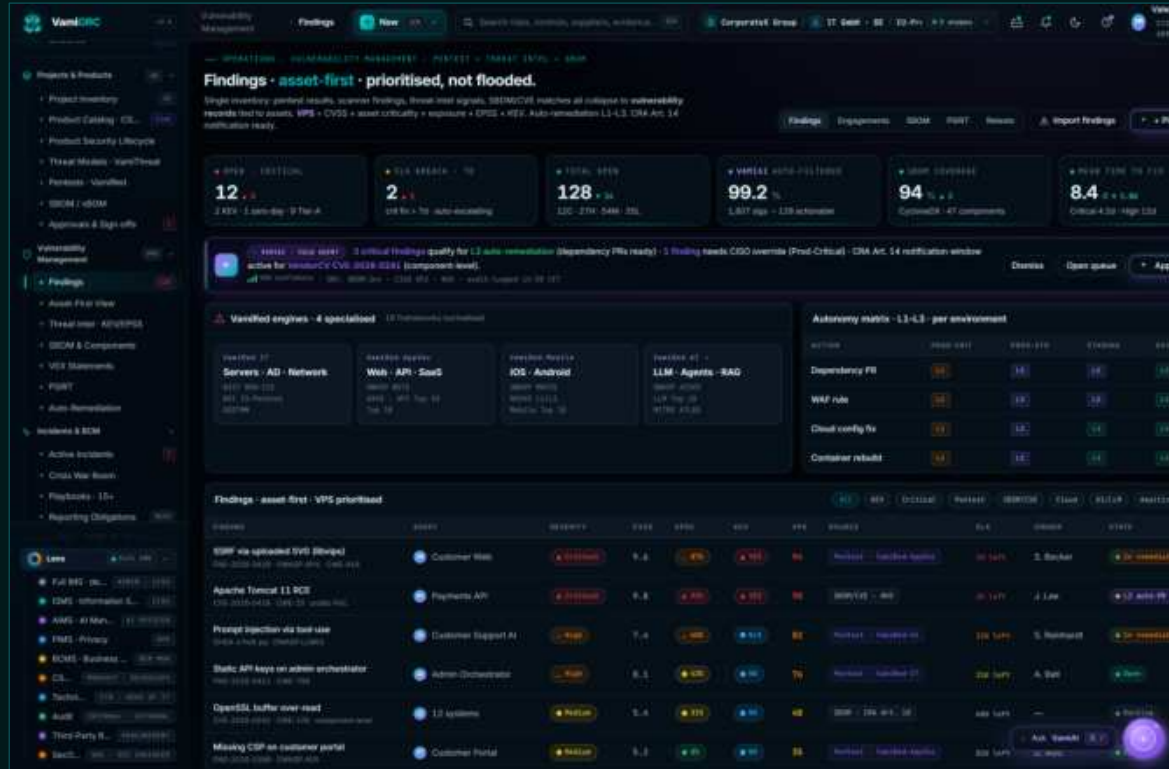
10-phase engagement lifecycle

Each phase has a defined owner and an autonomy level (L1 max)



VPS — Asset-First Vulnerability Management.

1.800 CVEs/Tag gefiltert auf ~8, die Sie tatsächlich betreffen. Auto-Remediation L1-L3. VEX eliminiert 75 % des Scanner-Rauschens.



Vulnerability Management & Threat Intelligence.

Asset-first-Inventar · Zero-Day-proaktive Abwehr · KI-Korrelation & VPS-Priorisierung · Auto-Remediation mit Autonomie-Matrix.

Asset-First-Inventar

Jede Schwachstelle wird einer Asset-ID zugeordnet. Pentest, SAST, DAST, SCA, Cloud, CVE-Feeds — dedupliziert.

Threat-Intel-Engine

Zero-Day-Workflow: 4-Stunden-proaktive Impact-Analyse · KEV · EPSS · Vendor Advisories · OSV.

SBOM · KOMPONENTEN-LEVEL-TRACKING

CycloneDX & SPDX pro Release · Sub-Asset-Tracking für CSMS · VEX-Statements · transitive Dependency-Reichweite.

Threats that touch your assets.

CVE · KEV · EPSS · vendor advisories · zero-day signals — correlated against your asset graph in real time. VamiAI filters the 1,800+ CVEs/day to the 8 that touch you.

• TOUCHES YOU · OPEN

8 ▲ 3

2 KEV · 1 zero-day · 5 high-EPSS

• KEV NOT PATCHED · 140

2 ▲ 1

Tier-A assets · SLA breach soon

• VENDOR ADVISORIES · 24H

142 ▼ 18

Microsoft 47 · Cisco 22 · Atlassian 8



VAMI AI · THREAT INTEL AGENT

CVE-2026-0418 (Apache Tomcat RCE) went KEV 47 minutes ago · 3 of your Tier-A assets affected · public PoC

96% confidence · SRC: NVD · CISA KEV · GitHub PoC · Asset-Reg · audit-logged 14:55 CET

Active threats · scoped to your assets

live · refreshes every 5 min

CVE	TITLE	EPSS	KEV
CVE-2026-0418	Apache Tomcat 11 — RCE via crafted request Public PoC · 47m ago · CWE-20	▲ 92%	▲ YES
CVE-2026-8392	Cisco ASA — auth bypass on web UI Vendor advisory · 6h ago	▬ 78%	▬ PEND
CVE-2026-0287	Microsoft Exchange — info disclosure Patch Tuesday · 12h ago	◆ 42%	■ NO
CVE-2026-0241	OpenSSL — buffer over-read Maintainer advisory · 1d ago	◆ 31%	■ NO
GHSA-x7w9-pq	Anthropic SDK — prompt injection on tool use GitHub advisory · 3h ago · DWASP LLM01	▬ 68%	■ N/A

Domains & Attack Surface Management.

Ihr externer Footprint, kontinuierlich erkannt, bewertet und überwacht.

Attack Surface · your external footprint, continuously assessed.

Every domain, host, subdomain, certificate, exposed service, AI feature, GDPR signal — plus dark-web leaks, brand abuse, code-secret exposure, supply-chain ASM. 23 compliance signals auto-mapped to ISO 27001 / NIS2 / GDPR / EU AI Act.

Domains Hosts Subdomains

• DOMAINS TRACKED

42

7 verified · 23 active · 12 shadow

• EXTERNAL FINDINGS

23

3 critical · 8 high

• DARK-WEB LEAKS

14

9 cred. · 3 paste · 2 RW leak

• BRAND ABUSE

7

5 typosquat · 2 lookalike cert

• SUBDOMAIN TAKEOVER

2

orphan CNAMEs · auto-escalate

VARIAI · ASN AGENT New credential leak detected on *Combolist 2026-Q2* · 9 corporate emails affected · 1 with admin role (S. Becker — rotated automatically) · concurrent typosquat domain
"vam1sec.com" registered 47 min ago, MX provisioned.
92% confidence · SRC: HIBP · DeHashed · IntelX · CT logs · audit logged 14:59 CET

Domain workbench · composite risk: 0-100 · explainable

All Verified Shadow

DOMAIN	OWNER	DNSSEC	DMARC	SPF	MTA-STS	BIMI	TLS
vam1sec.com primary · CT-monitored · BIMI live	IT Security	✓	quarantine	✓	✓	✓	A+
app.vam1sec.com customer portal · 5 web apps	Engineering	✓	none	✓	testing	none	A
marketing.vs A orphaned subdomain · CT delta	Marketing	✗	✗	✗	✗	none	B
legacy-portal.vs deprecated · removal scheduled	Unassigned	✗	✗	✗	✗	none	F

Dark Web Monitoring 14 active · HIBP + IntelX + DeHashed + Tor crawler

IDENTIFIER	TYPE	SOURCE	FIRST SEEN	RECORDS	SEVERITY
valeri.milke@vam1sec.com	Credential Leak	DeHashed · Combolist 2026-Q2	today · 14:55	1	Critical
api-key matching pattern	Paste Leak	IntelX · pastebin.com/raw/xK	2d ago	3	High
vam1sec.com mention	Ransomware Leak	Tor · ALPHV portal	4d ago	—	High
9 corporate emails	Combolist	HIBP API	today	9	Critical
Telegram channel mention	Forum mention	Telegram · @breachforum_dump	9d ago	—	Medium

Brand Protection 7 lookalikes

LOOKALIKE	TYPE
vam1sec.com	Typosquat
vam1sec-login.com	Phishing p
vam1sec.com (cyrillic c)	Homoglyph
CT-log: cert for vam1grc-help.com	Lookalike

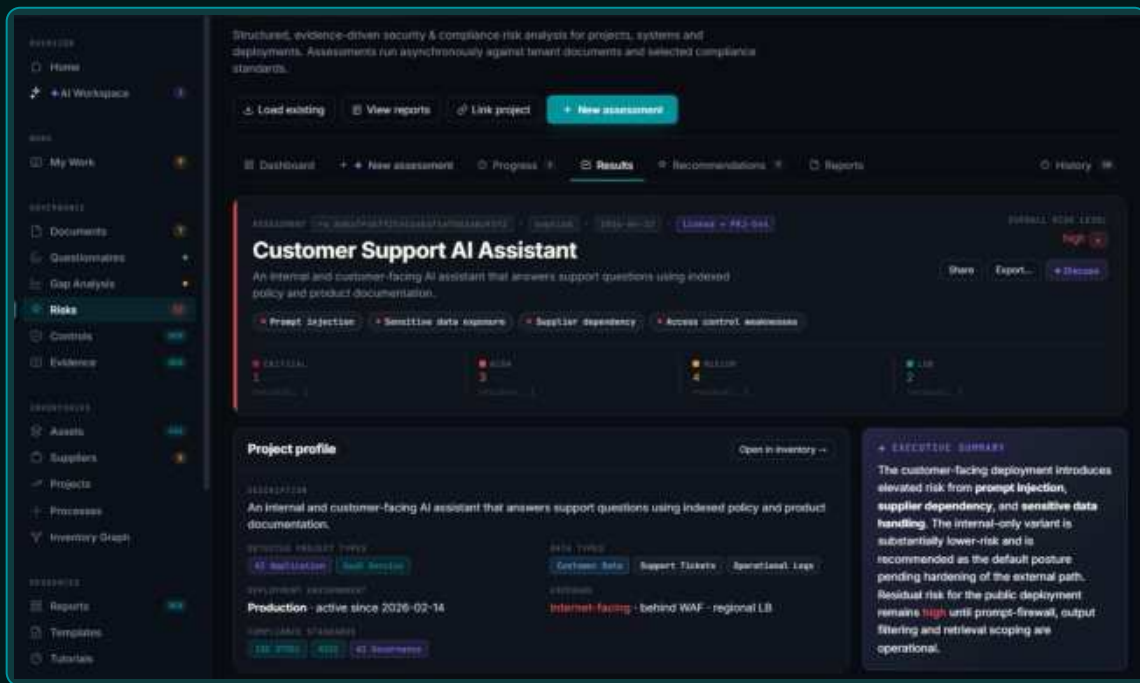
Code Leak Detection 2 active

AI Detection 11 features · auto-classified

GDPR Auto-Audit

KI-Risikobewertung — kontextbewusst, nachweisgetrieben.

Strukturierte Sicherheits- & Compliance-Risikoanalyse für Projekte, Systeme und Deployments. Verknüpft mit dem Projektdatensatz. Abgebildet auf ISO 27001, NIS2, AI Governance.



WARUM DAS ZÄHLT

● Risikoansicht je Deployment

Customer-Support-KI-Assistent · verknüpft mit PRJ-044 · bewertet Kritisch 1 · Hoch 3 · Mittel 4 · Niedrig 2.

● Erkannte Risikovektoren

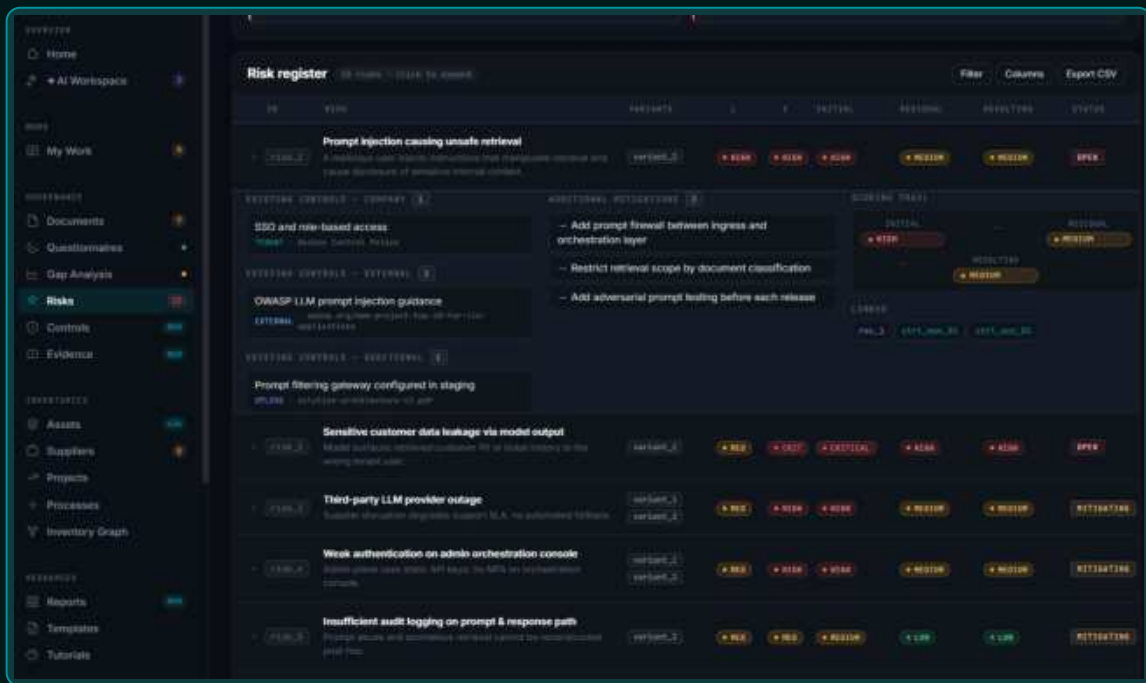
Prompt Injection · Offenlegung sensibler Daten · Lieferantenabhängigkeit · Schwächen der Zugriffskontrolle.

● Executive Summary, generiert

Klare Erläuterung für den Vorstand — mit Nachweisverweisen und empfohlener Haltung.

Risikoregister — inhärent vs. Rest, mit Behandlung.

Jedes Risiko erhält Owner, bestehende Controls (Unternehmen · extern · zusätzlich), vorgeschlagene Maßnahmen und eine vollständige Scoring-Historie — initial → Rest → resultierend.



WARUM DAS ZÄHLT

- **Bestehende Controls · 3 Ebenen**

Unternehmens-Controls · externe Leitfäden (z. B. OWASP) · zusätzliche Uploads — alles verknüpft.

● Vorgeschlagene Maßnahmen

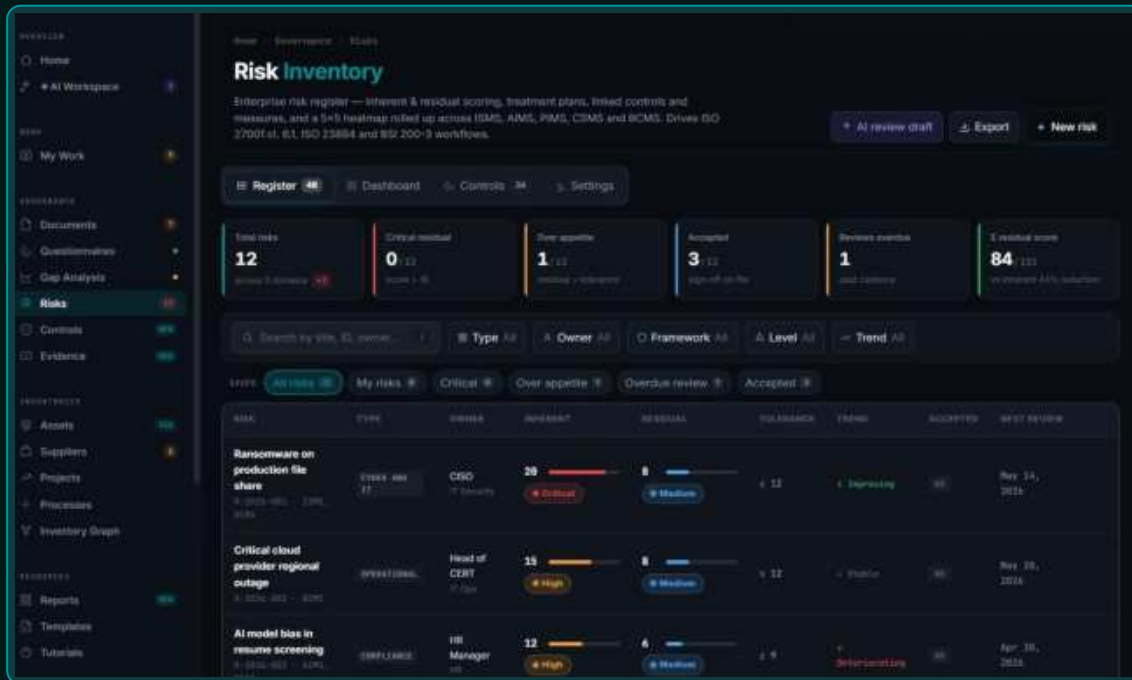
KI schlägt die nächsten Schutzmaßnahmen vor:
Prompt-Firewall · Einschränkung des Retrieval-
Scopes · Adversarial Testing.

- **Scoring-Historie sichtbar**

Initial · Rest · resultierende Stufen werden nebeneinander mit verknüpften Empfehlungen und Controls dargestellt.

Enterprise-Risiko-Inventar.

Inhärentes & Restrisiko-Scoring · 5x5-Heatmap aggregiert über ISMS, AIMS, PIMS, CSMS und BCMS · Trendanalyse · Akzeptanz-Workflow.



WARUM DAS ZÄHLT

● 12 Risiken · 5 Domänen

Kritisch (Rest) · über Appetit · akzeptiert · Reviews überfällig — ein Dashboard, sechs Sichten.

● Inhärent → Rest-Delta

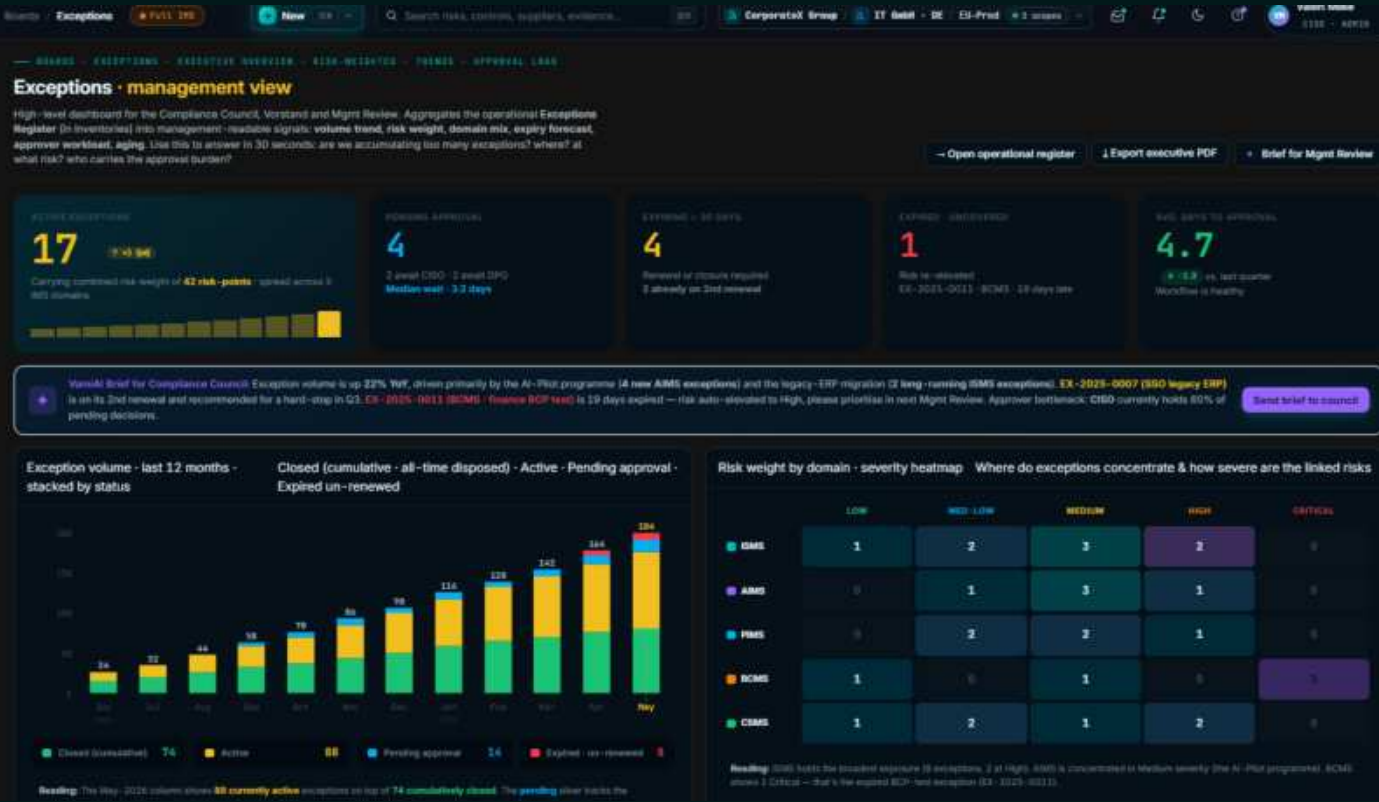
44 % Reduktion auf Registerebene sichtbar — Score, Typ, Owner und Toleranz pro Zeile.

● Trend & nächste Prüfung

Pfeile für „verbessernd · stabil · verschlechternd“. Kadenz erzwungen, akzeptierte Risiken mit Audit-Trail.

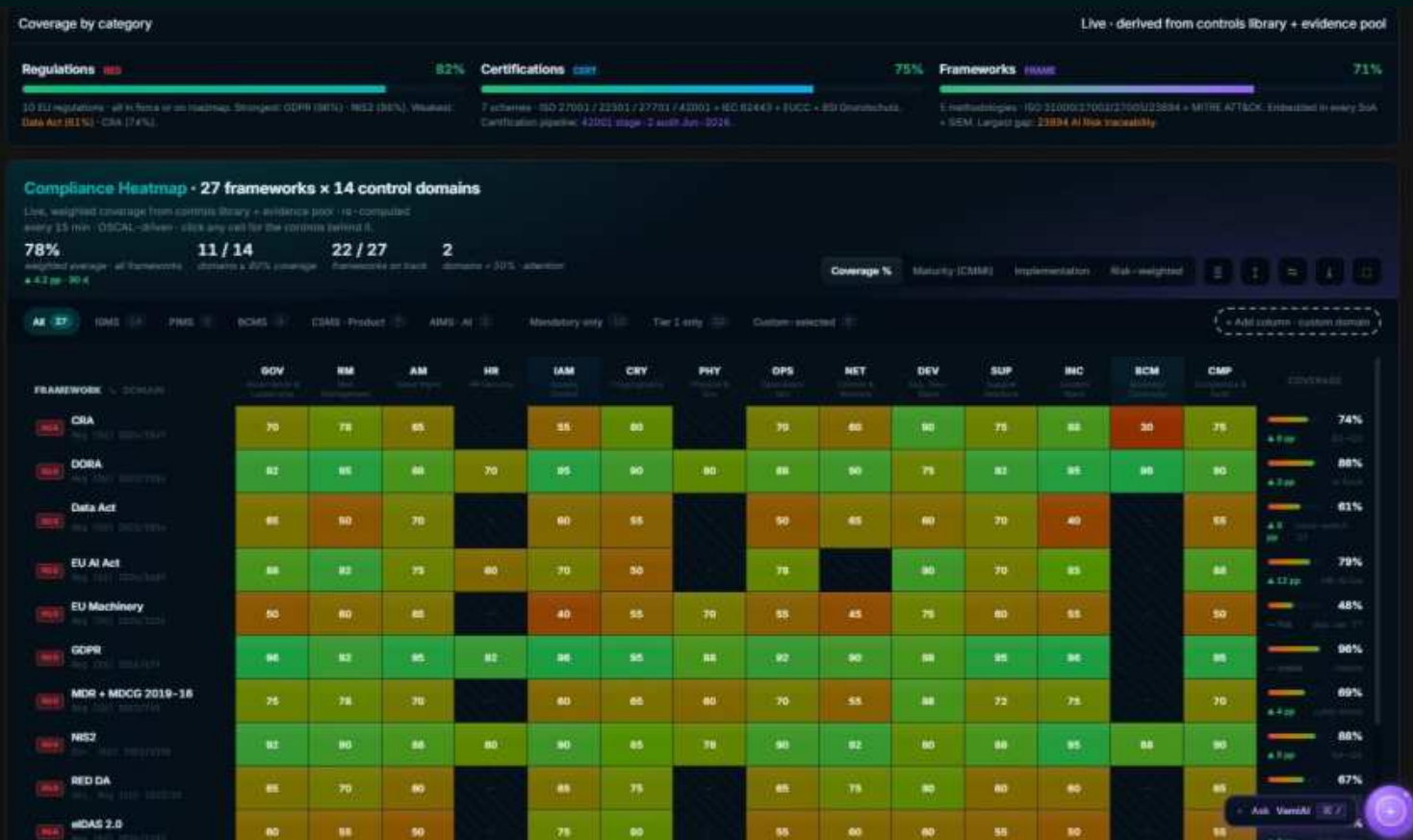
Ausnahmemanagement zur Risikofreigabe.

Inhärentes & Restrisiko-Scoring · 5x5-Heatmap aggregiert über ISMS, AIMS, PIMS, CSMS und BCMS · Trendanalyse · Akzeptanz-Workflow.



Risikoanalyse & Multi-Framework-Gap-Assessment.

Risikoregister auf einen Prompt · ISO-31000/27005-konform · auditbereite PDF- + Excel-Exporte.



Internes Audit & Gap-Analyse — drei Modi, Multi-Framework.

Vollautomatisiert · interviewbasiert · hybrid. ISO-9.2-Audits · ISO 27001 + 42001 + NIS2 + DORA + CRA in einem Durchgang.

MODUS 1

Vollautomatisierte KI

Agenten bewerten ISMS/AIMS-Dokumente gegen Framework-Controls. Findings mit Confidence-Score.

0 Personenstunden

MODUS 2

Interviewbasiert

Auditee-Portal · strukturierte Interview-Workshops · ISO-19011-Walkthroughs · Stichprobenverfahren.

Workshop-Stil

MODUS 3

Hybrid (empfohlen)

KI bewertet alles vor. Auditor prüft und vertieft per Interview nur dort, wo nötig.

Best of Both

KOMBINIERT MULTI-FRAMEWORK

ISO 27001 + NIS2 + DORA in einem Assessment.

Cross-Mapping-Engine dedupliziert Auditfragen:

≈ 40 % weniger Fragen · ein Nachweis-Durchgang · ein Berichtssatz

FINDING-REGISTER · CAPA-TRACKING

Major-NK → legt automatisch Risiko + CAPA an · Eskalation

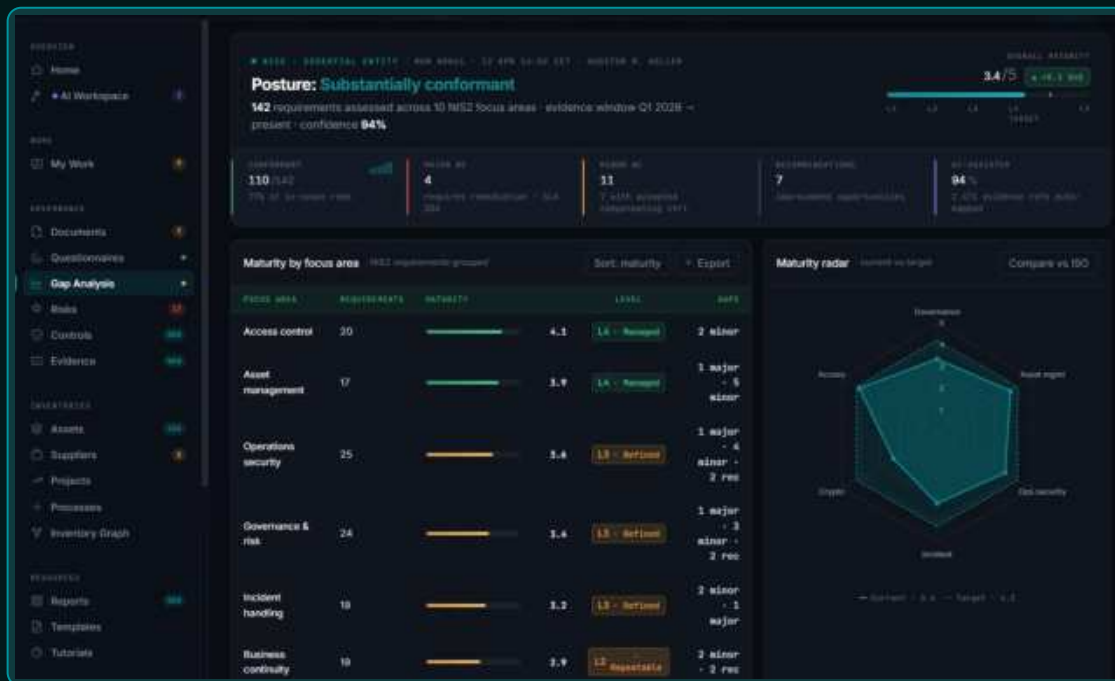
Minor-NK → Korrekturmaßnahme · Fälligkeit · Owner

Beobachtung → nachverfolgt, getrendet, im Management-Review geprüft

OFI → Improvement-Backlog · priorisiert

Kontinuierliches Framework-Assessment — Reifegrad in Echtzeit.

Jedes Control, jede Policy und jedes Log gemappt gegen Ihre aktiven Frameworks. NIS2, ISO 27001:2022, CRA — per Klick umschaltbar. Offene Lücken bis zur Behebung verfolgt.



WARUM DAS ZÄHLT

● Im Wesentlichen konform

142 Anforderungen bewertet · 110 konform · 4 Major-NK · 11 Minor · Confidence 94 %.

● Reife-Radar vs. Ziel

Pro Fokusbereich aktuelle vs. Ziel-Reife — Governance · Asset · Crypto · Incident · Ops · Access.

● Audit-Bereitschaft bewertet

78 % Q3-Audit-Bereitschaft · +12 Punkte · 112 Tage entfernt — jede Änderung mit Nachweis verfolgt.

Gap-Copilot — sprechen Sie mit Ihren Lücken.

KI-Assistent, eingegrenzt auf den aktuellen Scan. Lücke erklären · Behebung entwerfen · Controls über Frameworks mappen · Nachweise finden · Auditor simulieren — in einem Thread.

WARUM DAS ZÄHLT

● Priorisierung der Audit-Exposure

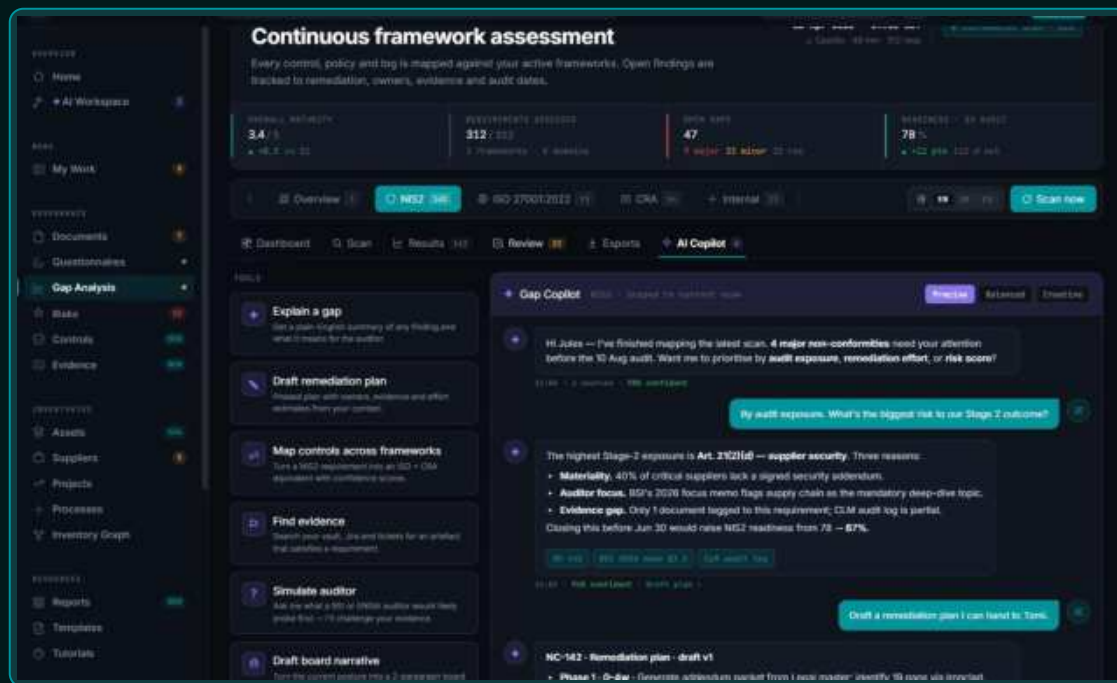
„Höchste Stage-2-Exposition ist Art. 21(2)(d) — Lieferantensicherheit“ — mit 3 Begründungen, alle belegt.

● Das Schließen erhöht die Readiness

Konkretes Delta sichtbar: 78 → 87 %, wenn NK-142 vor dem 30. Juni geschlossen wird — umsetzbar, nicht theoretisch.

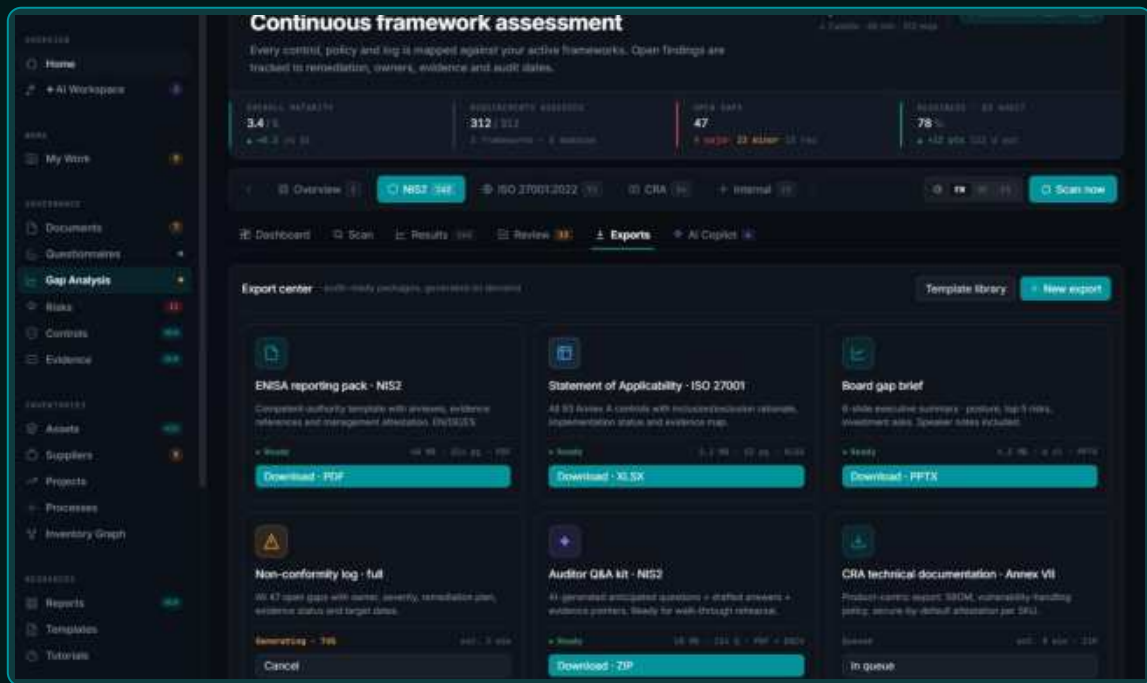
● Erstellt den Behebungsplan

Phase 1 (0–4 W) · Phase 2 (4–8 W) · Owner und Aufwandsschätzungen aus Ihrem Kontext gezogen.



Export Center — auditbereite Pakete auf Knopfdruck.

ENISA-Reporting-Pack · Statement of Applicability · Board-Gap-Brief · Non-Conformity-Log · Auditor-Q&A-Kit · CRA-technische Dokumentation. Generiert, nicht zusammengebaut.



WARUM DAS ZÄHLT

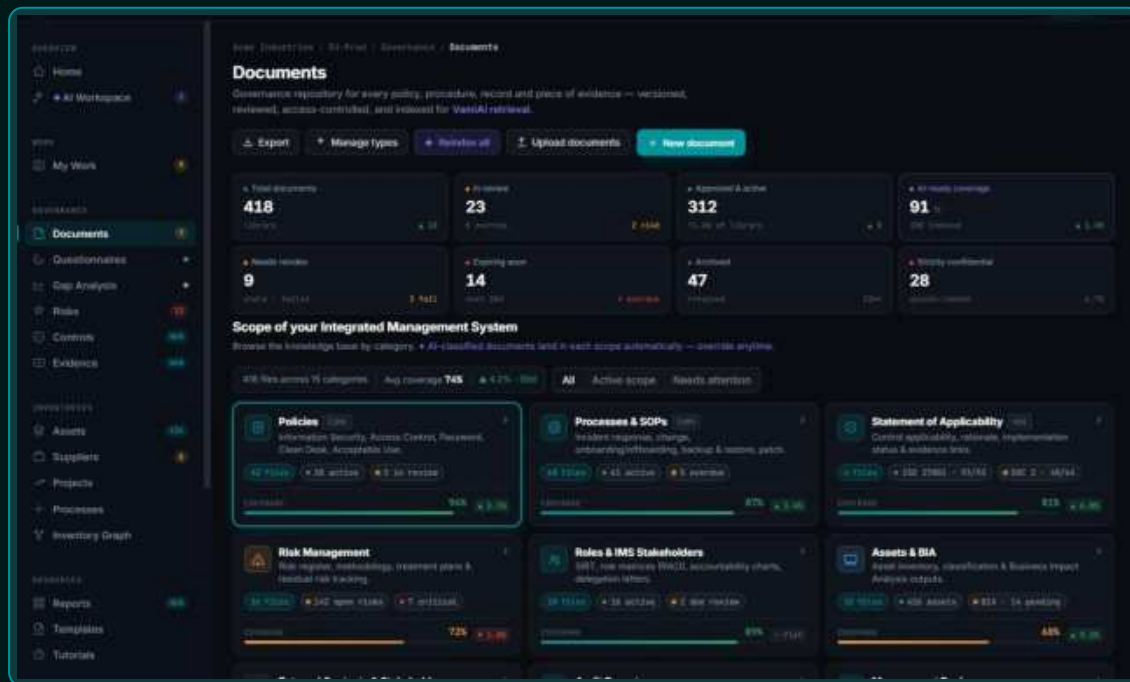
- **Sechs Pakettypen · framework-parametrisch**
PDF · XLSX · PPTX · ZIP als Output — NIS2, ISO 27001, CRA, intern — gleiche Engine.
- **Multi-Sprach-nativ**
EN · DE · ES aus einer Quelle generiert. Keine erneute Übersetzung. Kein Drift.
- **Status: bereit oder in Erstellung**
Echte ETA, echter Fortschritt, echte Bytes — Vorlagen für zuständige Behörden mit Anhängen und Bestätigung.

Dokumenten-Repository — KI-klassifiziert, auditiert.

Governance-Repository für jede Policy, Verfahrensanweisung, jeden Datensatz und Nachweis — versioniert, geprüft, zugriffskontrolliert und für die VamiAI-Suche indexiert.

WARUM DAS ZÄHLT

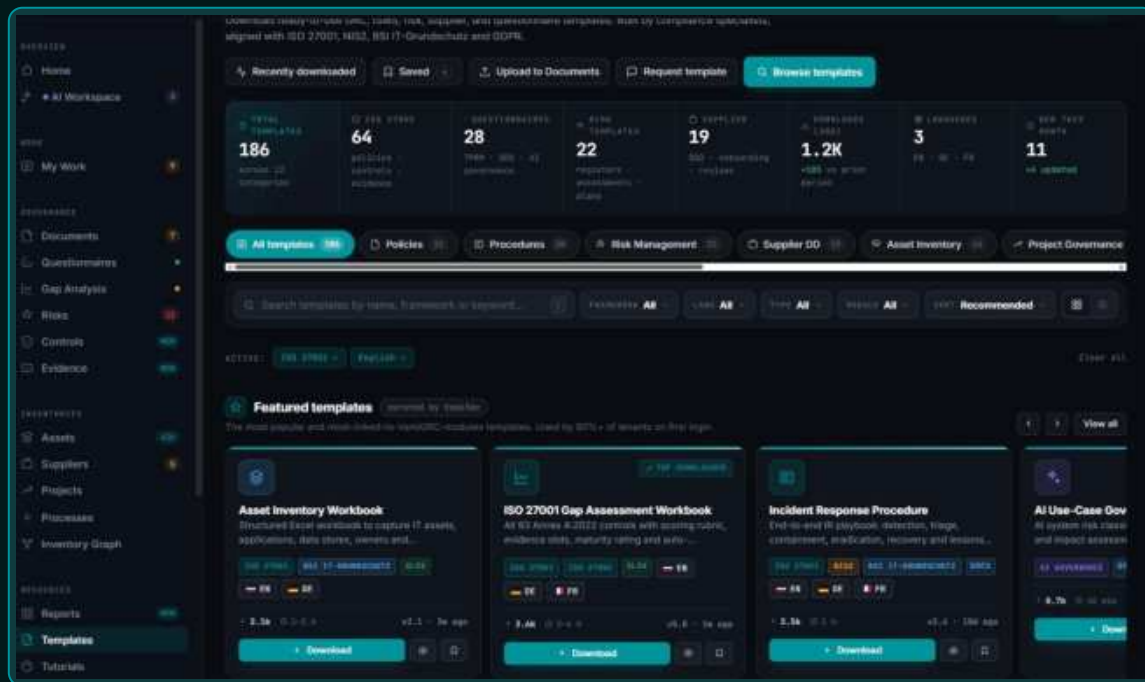
- **418 Dokumente · 91 % KI-ready**
Gesamt · in Prüfung · freigegeben · läuft bald aus · archiviert · streng vertraulich — auf einen Blick.
- **Auto-klassifiziert · 15 Kategorien**
Richtlinien · SOPs · Statement of Applicability · Risikomanagement · Rollen & Stakeholder · Assets & BIA...
- **Abdeckung pro Kategorie nachverfolgt**
Live-Abdeckung in % · Trend-Deltas · Anzahl in Prüfung — gekennzeichnet, wenn Aufmerksamkeit nötig.



Vorlagenbibliothek — 186 einsatzbereite, framework-getaggte

Vorlagen.

Politiken · Richtlinienanweisungen · Risiko · Lieferanten · Fragebögen — erstellt von Compliance-Spezialisten. Ausgerichtet an ISO 27001, NIS2, BSI IT-Grundschutz und DSGVO. Drei Sprachen.



WARUM DAS ZÄHLT

- **Von 80 %+ beim ersten Login genutzt**

Asset-Inventar-Workbook · ISO-27001-Gap-Workbook · Incident Response · KI-Use-Case-Governance.

- **Filter: Framework · Sprache · Typ**

ISO 27001 · NIS2 · BSI Grundschutz · DOCX · XLSX · DOCX · EN · DE · FR — gespeicherte Filter.

- **11 neu in diesem Monat · +4 aktualisiert**

Kuratiert von VamiSec · Download-Statistiken · Versionskontrolle · Kanal für Vorlagenanfragen.

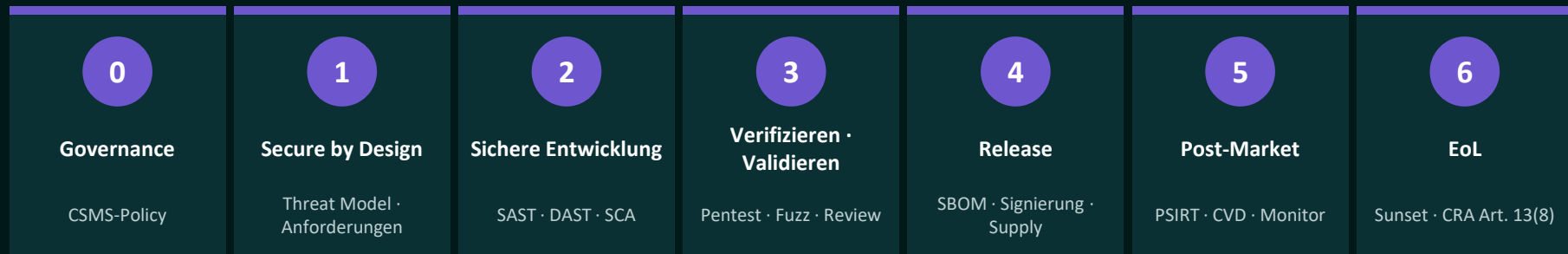
Business Continuity by Design.

BIA-getriebenes Recovery, end-to-end (ISO 22301).

-
- BIA-getriebenes Recovery: MTPD · RTO · RPO
 - BCP- & DR-Pläne · Krisen-War-Room · Tabletop-Kalender
 - ISO-22301-Controls · DORA Kapitel V · NIS2-Meldefristen
 - 42 BIA-Prozesse auf Assets und Risiken gemappt
 - DORA-TLPT-Replay-Tooling integriert

Produkt-Security-Lifecycle — CSMS end-to-end umgesetzt.

IEC 62443 · CRA · ISO 21434 · MDR · SaMD. Sieben Phasen von Secure-by-Design bis End-of-Life — orchestriert von 12 spezialisierten KI-Agenten.



SBOM · xBOM · PSIRT

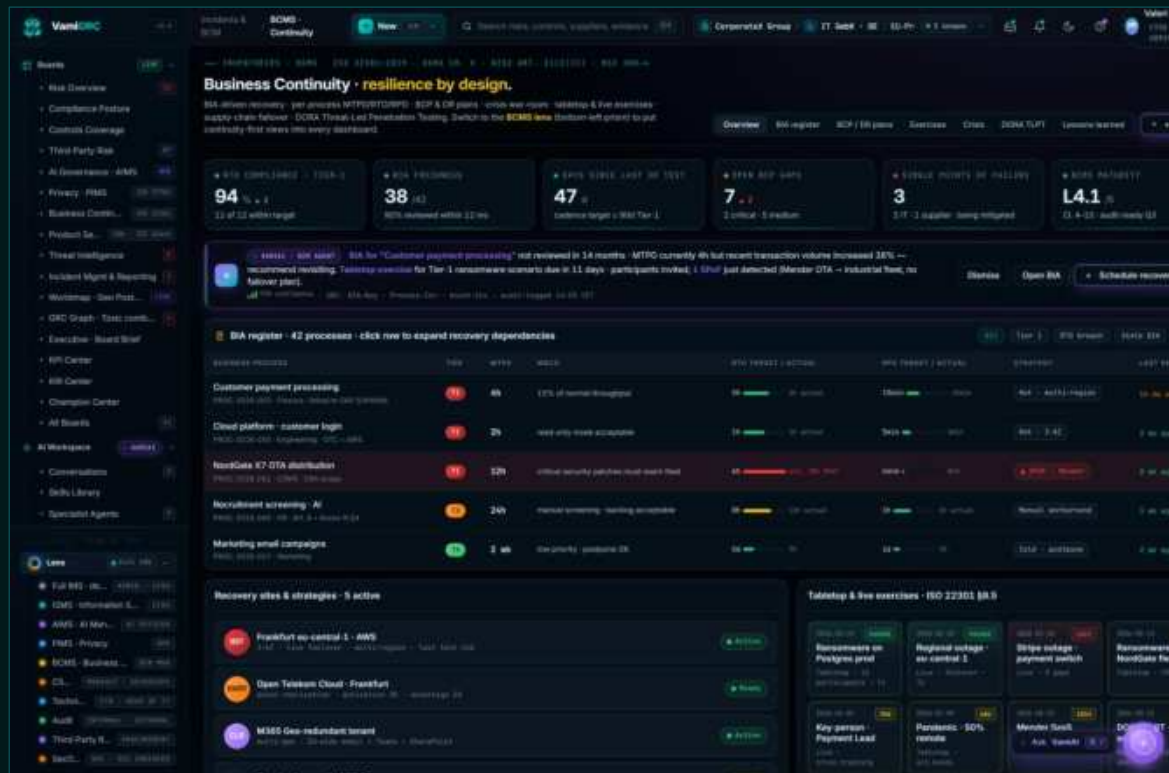
- CycloneDX- & SPDX-Generierung pro Release
- Kontinuierliches Re-Scanning verwundbarer Komponenten
- VEX-Statements für betroffen / nicht betroffen
- PSIRT-Triage · CVSS · CRA-Art.-14-Meldungen
- Coordinated-Vulnerability-Disclosure-Portal

FRAMEWORK-ABDECKUNG · EIN PRODUKT, VIELE PFLICHTEN

IEC 62443	Industrie · OT
EU CRA	Produkte mit digitalen Elementen
ISO 21434	Automotive-Cybersicherheit
MDR · SaMD	Medizinprodukte · IEC 81001-5-1
NIST SSDF	Secure-Software-Development-Framework

BCMS-Lens — ISO 22301 in Bewegung.

Business Continuity als First-Class-Citizen — RTO/RPO über jeden Prozess · Recovery-Standorte · Tabletops ·



Agentische Lieferanten-Intelligenz.

Lieferketten-Sicherheit auf Autopilot — von OSINT und Security Ratings bis zum AVV-Management.

OSINT & Trust Center

Domains, ASM, Security Ratings (BitSight, SecurityScorecard, CybelAngel) — automatische externe Sicht.

Fragebogen-Automatisierung

Eingehende Fragebögen werden per KI mit Ihrem ISMS abgeglichen. Konsistente, nachweisbasierte Antworten in Minuten.

NDA · AVV · Verträge

Lieferantenspezifisches Dokumentenmanagement. DSGVO-Art.-28-Tracking. Ablauf- & Erneuerungsbenachrichtigungen.

Risikobewertungen

Strukturiert nach NIS2 Art. 21(2)(d). Priorisierte Findings, Maßnahmen, auditbereite PDF/Excel-Berichte.

LIEFERANTEN-ASSESSMENT-WORKFLOW

1

Anlegen oder importieren

2

OSINT & Rating

3

Fragebogen

4

Gap-Analyse

5

AVV / NDA

6

Audit-Bericht

Agentische Lieferanten-Intelligenz.

INVENTORIES · SUPPLIERS · CCM V4.1 / CAIQ / STAR AWARE

Suppliers · cloud-aware by design.

Every supplier mapped to GRC. Cloud providers (IaaS · PaaS · SaaS) automatically routed to **CSA CCM v4.1** (207 controls · 17 domains) · CAIQ · STAR registry ingestion · Shared Security Responsibility tracked per control. Cross-mapped to ISO 27001 / 27017 / 27018 / NIS2 / DORA / BSI C5.

All Cloud only Tier-A Re-assess Export + Add Supplier

TOTAL SUPPLIERS

87

+4 this quarter

CLOUD PROVIDERS

23

11 IaaS · 7 PaaS · 14 SaaS

TIER-A · CRITICAL

9

3 with SSRM gaps

STAR L2+ CERTIFIED

14

~70% re-assess time saved

DPA EXPIRING · 960

3

auto-task created

VAMIAI ASSESS HRS

312_h

vs. 1,560h manual

+ VAMIAI · TPRM AGENT

3 cloud suppliers haven't refreshed their CAIQ in >12 months · 1 STAR L2 attestation expires in 47 days (CloudFactor Ltd.) · auto-drafted re-assessment workflow ready to publish.

Dismiss

Open list

+ Publish Workflow

97% confidence · SRC: STAR Registry · CAIQ-Inv · DPA-Reg · audit-logged 14:47 CET

Filter: AllCloud - IaaSCloud - PaaSCloud - SaaSHardwareConsultingTier-1 CriticalSTAR L2+SSRM gapsDPA expiringNIS2 sub-contractor									
Supplier	Type	Cloud Model		Tier	Star	CCM Coverage	SSRM	DPA	Last Assess
AW AWS Europe SARL Frankfurt - Luxembourg - Tier-1	Cloud Provider	IaaS	PaaS	Tier 1	★ STAR L3	96%	2 SSRM gaps	Active	14d ago
MS Microsoft Azure / M365 Dublin - Tier-1	Cloud Provider	IaaS	PaaS	SaaS	Tier 1	94%	No gaps	Active	22d ago
AN Anthropic San Francisco - LLM provider - Tier-2	Cloud Provider	AI Vendor	SaaS	Tier 2	★ STAR L1	81%	5 SSRM gaps	Active	31d ago
OT Open Telekom Cloud Frankfurt - sovereign EU - Tier-1	Cloud Provider	IaaS	PaaS	Tier 1	★ STAR L3	98%	No gaps	Active	8d ago
CF CloudFactor Ltd. London - DLP / DSPM - Tier-2	Cloud Provider	SaaS		Tier 2	★ STAR L1	72%	8 SSRM gaps	Expires 47d	387d ago
VS VendorCV Ltd. Tallinn - Skill marketplace - Tier-3	Cloud Provider	SaaS		Tier 3	★ None	42%	14 SSRM gaps	Missing	Never

Automatisierte Lieferanten- Assessments.

Lieferketten-Sicherheit auf
Autopilot — von OSINT,
Fragebögen, CSA-STAR-DB und
Security Ratings bis zum AVV-
Management.

Supplier detail - AWS Europe SARL

CLOUD-WARE



AWS Europe SARL

SUP-2026-0007 - Frankfurt - Luxembourg HQ

Tier 1

STAR L3

CLOUD PROVIDER

Supplier ID

SUP-2026-0007

LEI

LEI-EXAMPLE-AWS-EU

Owner

E. Müller (CEO Office)

Criticality

94 / 100

Inherent risk

High - 18

Residual risk

Medium - 9

Contract

2024-01-15 - 2027-12-31

DPA - Art. 28

Active - v3 (2026-01)

Sub-processors

14 - last sync 8h

Linked assets

142 - 78 Iaas - 64 Paas

Adequacy decision

EU-US DPF - valid

SPoF

Yes - region-eu-central-1

CLOUD SERVICE MODEL - CSA CCM APPLICABILITY

IaaS

Infrastructure as a Service

PaaS

Platform as a Service

SaaS

Software as a Service

Hyb

Hybrid

VaniAI auto-detected based on contracted services - 142 assets cascade SSPM ownership from this selection.

+ Questionnaire Router - auto-selected

Tier 1 + STAR L3 - Ingest existing CAIQ from STAR registry, no re-questionnaire needed. ~70% effort saved.

CAIQ v4.1 - 351 q - Last refresh: 8d ago - Source: STAR Registry

Open CAIQ

Re-ingest

CCM v4.1 CLOUD POSTURE - 37 DOMAINS - 287 CONTROLS



SHARED SECURITY RESPONSIBILITY - PER-CONTROL OWNERSHIP

CSP AWS CSC IIS SHARED-INREP SSP-CAP

CONTROL ID	TITLE	DOMAIN	SSPM (IaaS)	SSPM (PaaS)	STATUS	EVIDENCE
AGA-01	Audit & Assurance Policy and Procedures	AGA	SHARED-INREP	SHARED-INREP	Yes	CAIQ AGA-01.1
CEK-03	Encryption Algorithm Strength & Lifetime	CEK	CSP	CSP	Yes	FIPS 140-3 attest.
CEK-13	Key Management Lifecycle (rotation, custody)	CEK	CSC	CSC	Yes	Internal KMS policy
DSP-05	Data Classification	DSP	CSC	CSC	Partial	3/4 systems
STA-05	Supply Chain Data Security Assessment	STA	SSP-CAP	SSP-CAP	No	Awaiting CSP disclosures
IVS-08	Network Architecture - Segmentation	IVS	CSC	SHARED-INREP	Yes	VPC design v4

Showing 6 of 207 controls - Open full CCM v4.1 matrix -

CR213-FRAMEWORK COVERAGE - AUTO-MAPPED FROM ICH

ISO 27001:2022	Full	ISO 27017	Full	ISO 27018	Full	ISO 27032 Art. 21(2)(d)	Partial	BSA Ch. V	Full
BSI CS	Full	SOC 2 TSC	Full	PCI DSS 4.0	Partial	EU AI Act Art. 28b	No		

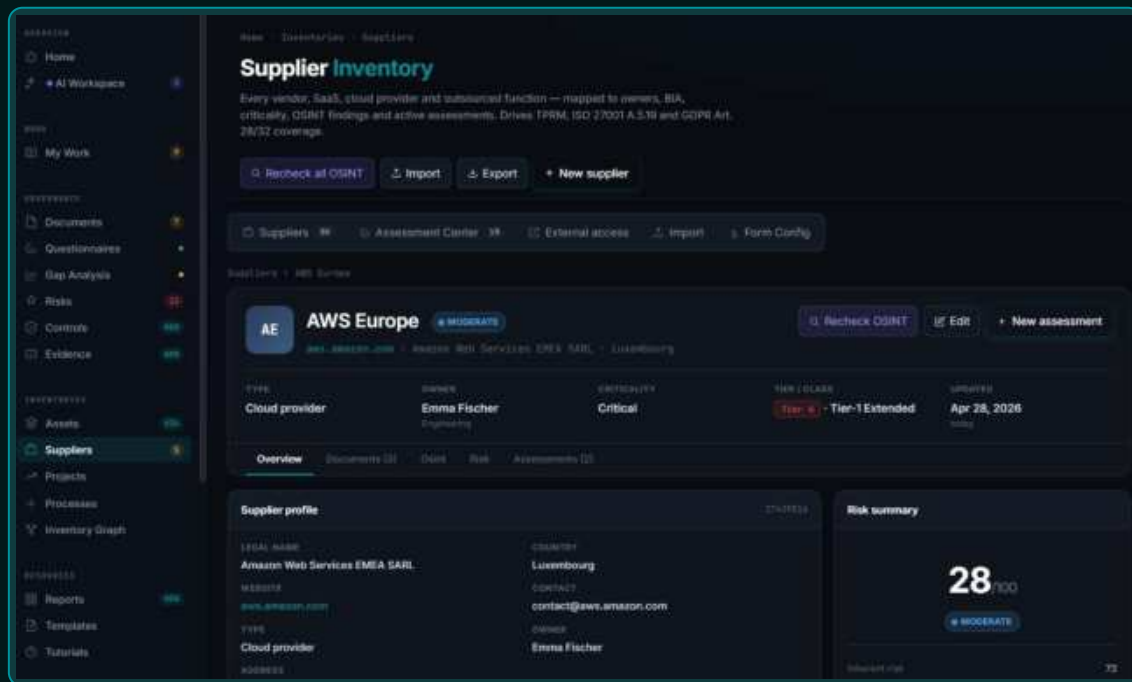
Software-Third-Party-Risiko — xBOM-nativ.

87 aktive Lieferanten · 412 CycloneDX 1.6 eingelesen · 6 Lieferanten-Sub-Agenten auf Streife · STAR-Registry-Sync.



Lieferanten-Inventar — jeder Anbieter abgebildet, bewertet und nachverfolgt.

Jeder Anbieter (SaaS, Cloud-Provider und ausgelagerte Funktion — gemappt auf Owner, BIA, Kritikalität, OSINT-Findings und aktive Assessments. Treibt TPRM, ISO 27001 A.5.19 und DSGVO Art. 28/32.



WARUM DAS ZÄHLT

● 360°-Sicht je Lieferant

AWS Europe · Kritisch · Tier-A · Cloud-Provider
— Owner, Land, Kontakt, Adresse, Klassifikation.

● Risiko-Score sichtbar

28/100 · Moderat · inhärent vs. Rest — OSINT
per Klick neu prüfen.

● Reiter: Dokumente · OSINT · Risiko

Reiteransicht jeder Lieferanteninteraktion —
vergangene Assessments und Findings stets
zugänglich.

KI-Fragebogen-Review — Minuten statt Tage.

Eingehende oder ausgehende Sicherheitsfragebögen, KI-vorbeantwortet aus Ihrem ISMS — mit Status, Kommentar, Quelldateien, Framework-Referenz und Scope pro Zeile. Bearbeiten, überschreiben, sperren.

WARUM DAS ZÄHLT

- **KI-erstellt, dort bearbeitet, wo nötig**

„Fertigstellung 91%.“ bearbeitet von Sara Mendes — ursprüngliche KI-Antwort mit Audit-Trail erhalten.

- **Quelldateien pro Zeile zitiert**

ISMS-POL-v4.2 · ASSET-REG · DLP-CFG — jede Aussage referenziert die Quelle zurück.

- **Statusverteilung live**

Ja 61 % · Teilweise 25 % · Nein 11 % · n. z. — Vollständigkeit %, Scope und externe IDs auf einen Blick.

#	REQUIREMENT	STATUS	COMMENT	SOURCE FILES	EXTERNAL ID	SCOPE
1	Does the organisation maintain an approved Information Security Policy?	YES	ISMS Policy v4.2 approved 2020-03-11 by CISO. Annual review scheduled.	ISMS-POL-v4.2	A.5.1	Global
2	Is there an inventory of information, associated assets, and ownership?	YES	Asset register maintained in VantivGRC; 426 assets, ownership coverage 98%.	ASSET-REG-2024-03-19	A.5.2	Global
3	Do all personnel receive security awareness training annually?	PARTIALLY EDITED	AI answer: "Completion 81%." Edited by Sara Mendes: "Completion 91% as of Apr 1; remaining 9% have until May 15 per HR plan."	HR-TRAIN-2024-03-19	A.5.3	Global
4	Is information classified according to sensitivity and handled accordingly?	YES	4-tier classification scheme. DLP enforced for Confidential+. Quarterly spot-checks.	DATA-CLASS-v3.1-DLP-CFG	A.5.4	Global
5	Are data leakage prevention measures implemented for sensitive data?	PARTIALLY	DLP active on endpoints and mail; cloud storage DLP rollout at 68% of tenants.	DLP-RULE-REPORT	A.5.5	Global
6	Are systems monitored for anomalous behaviour and security events?	YES	SIEM covers 100% of production; 24x7 SOC; MTTR 4m 15s (Q1).	SOC-RT-2024-03-19	A.5.6	Global
7	Is the use of AI components governed by explicit policy and risk review?	YES	AI Use Policy v1.3; mandatory risk assessment before production; 14 projects reviewed.	AI-POL-v1.3-WA-REG	A.5.7	Global
8	Is secure software development practiced, including SSDL and code review?	PARTIALLY EDITED	AI answer: "SSDLC documented." Edited by Alex Lj: "SSDLC documented; code review mandatory for prod repos; SAST	SSDLC-STR-2024-03-19	A.5.8	Global

CSA · Cloud Controls Matrix v4.1 · Live-Walkthrough.

VamiAI parst jede Frage, fragt Ihr Dokumentenmanagement ab, wählt den korrekten Status, zitiert die Quelle — in Sekunden. 200+ Fragen = 2 Tage → <5 Min.

vamigrapp — CCM-v4.1 · Audit & Assurance · 6 Fragen					VamiAI · BEANTWORTET		
ID	FRAGE	STATUS	CONF.	NACHWEIS			
A&A-01.1	Sind Audit- und Assurance-Policies etabliert, dokumentiert, freigegeben und gepflegt?	VOLL	98 %	→ ISMS-POL-001 · §4.2			
A&A-01.2	Werden Policies mindestens jährlich oder bei wesentlichen Änderungen geprüft und aktualisiert?	VOLL	95 %	→ Mgmt-Review-2024-Q4			
A&A-02.1	Werden mindestens jährlich unabhängige Audit-Assessments durchgeführt?	VOLL	99 %	→ ISO-27001-Zert · TÜV Süd			
A&A-05.1	Ist ein Audit-Management-Prozess für Planung, Risikoanalyse und Behebung definiert?	TEILWEISE	91 %	→ Audit-Proc-002 · Excel			
A&A-06.1	Existiert ein risikobasierter Korrekturmaßnahmenplan und wird er auf Audit-Findings angewendet?	GEPLANT	87 %	→ Roadmap-2025-Q1 · ETA März			
A&A-04.1	Wird Compliance gegen alle relevanten Standards, Regulierungen und vertraglichen Anforderungen verifiziert?	VOLL	96 %	→ Legal-Reg-2024 · DSGVO/NIS2			
ERGEBNIS · CCM A&A · 6 von 6 beantwortet · bereit zur Prüfung durch Compliance-Officer							
4 VOLL		1 TEILWEISE		1 GEPLANT		0 LÜCKE	

VamiGRC kennt alle Ihre Policies und Verfahrensanweisungen

KI-generiertes HTML · mehrsprachig (DE · EN · FR) · tiefe WordPress-Integration · auditbereite Compliance-Pakete auf Knopfdruck.

COMPLIANCE FOUNDATION · POLICIES AND DOCUMENTS · AI-GENERATED · APPROVAL-MANAGED

Policies, procedures, evidence — authored with VamiAI, signed by humans.

12 document types (Policy · Guideline · Concept · Procedure · Work Instruction · Record · Evidence · Report · Protocol · SoA · DPIA · Threat Model). 4-step generation pipeline · approval workflow · eSignatures · version compare · linked controls. 186 templates by IMS domain (ISMS · AIMS · PIMS · CSMS · BCMS) cross-mapped to ISO 27001/42001/22301/27701 · GDPR · NIS2 · AI Act · DORA.

Library

Templates · 186

Approval queue · 23

Review calendar

Evidence generator

Acknowledgements

+ Generate Document

TOTAL DOCUMENTS

418

312 policies · 68 SOPs · 38 records

VAMIAI DRAFTED

142 ▲ 18

all human-approved before publish

IN REVIEW · QUEUE

23

9 mine · 14 others

REVIEW OVERDUE

5 ▲ 2

annual cycle SLA breach

ACKNOWLEDGED

94 %

staff training rate

AVG GENERATION

8 .2 min

vs. 8 hours manual draft

VAMIAI · DOC GEN AGENT

BCM Policy v3.0 auto-drafted for ISO 22301 audit · 18 chapters · grounded in your BIA register + risk register + recovery sites · cited 47 internal sources + ISO 22301:2019 Cl. 4-10. Awaiting BCM Manager approval (Diana Ruiz).

96% confidence · SRC · BIA-Reg · Risk-Inv · Recovery-Sites · audit-logged 14:55 CET

Dismiss

Compare with v2.4

+ Open in editor

+ AI Generation Wizard · 4 steps · ~8 min

Cancel

+ Continue

1 Pick template

BCM Policy · ISO 22301

2 TOC refinement

18 chapters · 2 added

3 Generate sections

streaming · ch. 12 of 18

4 Approve · sign · publish

awaiting · D. Ruiz

Template browser · 186 ready · framework-mapped

All

ISMS · 45

BCMS · 14

PIMS · 18

AIMS · 12

CSMS · 11

ISMS

Policy

Information Security Policy

ISO 27001 §5.2 · 14 chapters · roles · scope · linked to 93 Annex A controls.

3.2 KB · EN · DE · FR · used 87+

BCMS

Policy

Business Continuity Policy · ISO 22301

Cl. 5.2 + 6.2 · 18 chapters incl. governance, scope, BIA framework, exercise schedule.

4.1 KB · EN · DE · used 16+

BCMS

Procedure

BIA · Business Impact Analysis

Per-process worksheet · MTPD · MBCO · RTO · RPO · dependencies · criticality tier · approver chain.

2.4 KB · EN · DE · used 42+

BCMS

SOP

BCP · Business Continuity Plan

BCMS

SOP

Disaster Recovery Plan · ICT

BCMS

Record

Tabletop Exercise Report

Trust Center · Compliance-Pakete für Ihr IMS.

KI-generiert. Mehrsprachig (DE · EN · FR). Quelldaten ändern sich → Narrative werden neu erzeugt → Pakete neu ausgestellt → Trust Center neu veröffentlicht — ohne dass jemand ein Word-Dokument anfasst.

The screenshot displays the VamiSec Trust Center interface, which is a dashboard for managing compliance packages. The main header reads "Trust Center · your compliance posture, audit-ready in minutes." Below this, there's a section with four key metrics: "LIVE PACKAGES" (6), "ACTIVE CERTIFICATES" (2), "EXPIRING" (2), and "PUBLIC VIEWS" (12,402). A navigation bar at the top right includes tabs for "Overview", "Packages", "Documents", "Channels", and "Requests".

On the left, a German-language overlay titled "Trust Center" is visible, with the subtitle "Unser Bekenntnis zu Informationssicherheit und Datenschutz". It mentions "Höchste Standards in Informationssicherheit und Datenschutz." Below this, it says "Sicherheits & Compliance bei VamiSec" and "Transparenz ist die Grundlage für Vertrauen. Hier finden Sie alle Informationen zu unseren Zertifizierungen, Managementsystemen und Sicherheitsrichtlinien." It lists several standards: ISO 27001, ISO 42001, DSGVO, AI Act, CRA, and NIS2, each with a brief description of the certification or system.

The main content area shows a list of compliance packages. The first package is "ISO 27001 - Information Security", which is a "pre-built" package. It includes a "Score maturity" section (0.0 to 1.0) and a "Generate narrative" button. The second package is "ISO 42001 - AI Management System", which is a "pre-built" package. It includes a "Visualize" button and a "Link evidence" button. The third package is "NIS2 - Essential entity", which is a "pre-built" package. It includes a "Publish" button and a "Link evidence" button.

At the bottom, there's a section for "pre-built" packages, which includes "ISO 27001 - Information Security", "ISO 42001 - AI Management System", "NIS2 - Essential entity", "DORA - ICT Risk & Resilience", and "GDPR - Privacy Compliance". Each package has a "pre-built" label and a "Link evidence" button.

The URL <https://vamisec.com/de/trust-center> is displayed at the bottom left. The text "Oh" is visible at the bottom center.

Dort, wo Ihre Teams bereits arbeiten.

• ROADMAP

Volle Funktionsparität in Teams, Slack, E-Mail, Mobile, Browser und API.

Microsoft Teams

@VamiAI in Kanälen · Adaptive Cards ·
Meeting-Intel

Slack

/vami-Befehle · Block Kit · Incident-War-
Rooms

E-Mail

Mandantenadresse · weitergeleitete RFIs ·
Dokumenten-Intake

Mobile (iOS/Android)

Voice-First · Push-Freigaben · Offline-
Entwürfe

Browser-Erweiterung

Kontext auf jeder Seite · Regulator- &
Anbieter-Websites

API · Webhooks · MCP

Jede Funktion programmatisch · KI-zu-KI-
Interoperabilität

Compliance im Fluss des Geschäfts — nicht erst, wenn jemand das GRC-Tool öffnet.

Wählen Sie Ihr LLM. Bewahren Sie Ihre Souveränität.

• ROADMAP

Default: Claude. Alternative: OpenAI/Azure. Souverän: Open Telekom Cloud. Oder BYOL — bringen Sie Ihr eigenes.

DEFAULT

Anthropic Claude

Beste Reasoning-Qualität.
EU-Region verfügbar.

MODELLE

Opus 4 • Sonnet 4 • Haiku 4

ALTERNATIVE

OpenAI / Azure OpenAI

MS-Stack-Organisationen.
Azure Private Endpoints.

MODELLE

GPT-4o • o3 • o4-mini

SOUVERÄN



DE Nur Deutschland.
KRITIS / NIS2 / DORA.

MODELLE

Llama 3.1 • Mistral •
Mixtral

BYOL

Bringen Sie Ihr eigenes LLM

On-Prem (vLLM, Ollama),
Bedrock, Vertex AI.

MODELLE

Jede OpenAI-kompatible API

Mandantenkonfiguration • Modellebene pro Use Case • Auto-Routing • Graceful Fallback.

Lens-Picker — zehn rollenbasierte Sichten.

CISO · DSB · KI-Beauftragter · BCM · Einkauf · Auditor · SecOps. Gleiche Daten. Andere Realität.



03

KPI · Aufgaben · Incidents

KPI Engine · My Work · Incidents · BCM

KPI-Engine, Dashboards & Management Review.

80+ KPIs über 5 IMS-Domänen · 14 interaktive Dashboards · strukturierte ISO-9.3-Management-Reviews · Action-to-Task-Pipeline.



MANAGEMENT REVIEW · ISO 9.3

INPUTS (gemäß ISO 9.3.2)

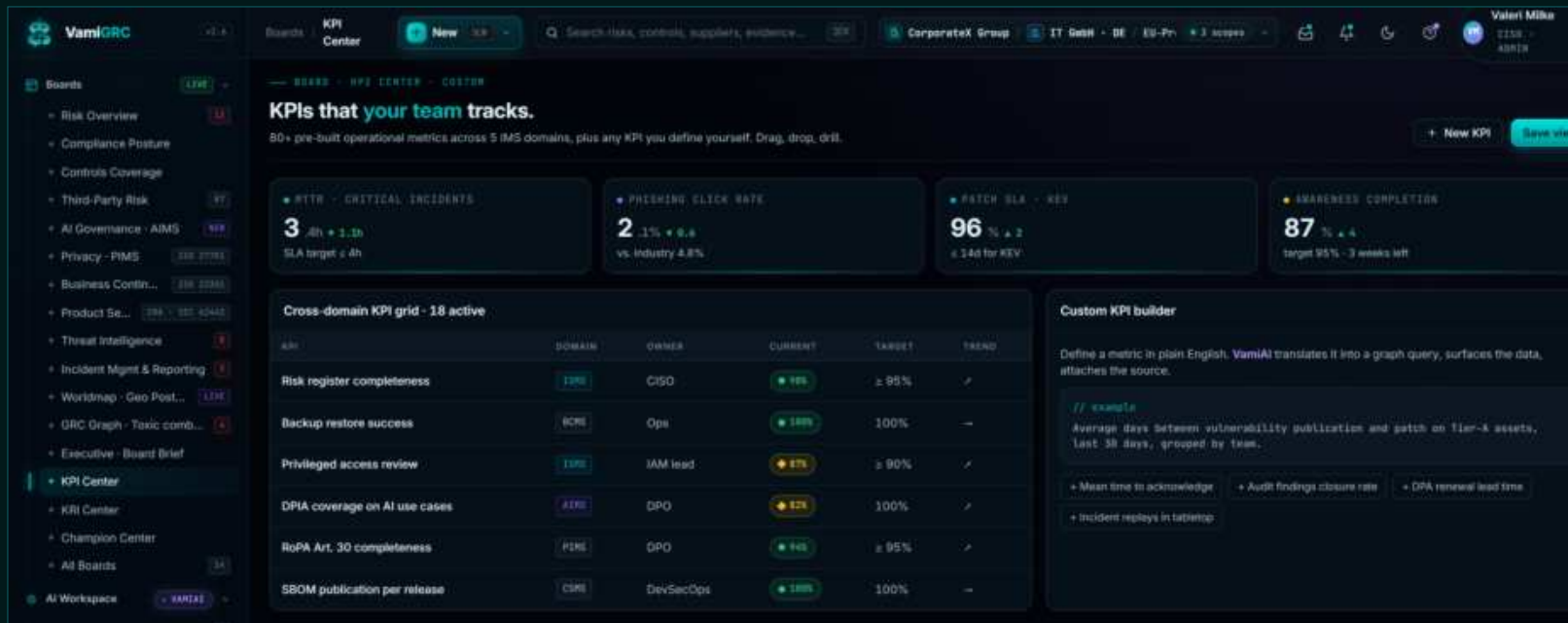
- ▶ Auditergebnisse · Finding-Trend
- ▶ Änderungen im Risikoregister · Top-Risiken
- ▶ Kundenfeedback · Beschwerden
- ▶ Prozessleistung · KPIs
- ▶ Ressourcenangemessenheit · Verbesserung

OUTPUTS (gemäß ISO 9.3.3)

- Verbesserungsentscheidungen · CAPA
- Ressourcenbedarf · Investitionsplan
- Maßnahmen-Datensätze → Aufgaben (Auto-Pipe)

KPI Center — Metriken in natürlicher Sprache.

Definieren Sie eine Metrik in natürlicher Sprache. VamiAI übersetzt sie in eine Graph-Abfrage und hängt die Quelle an.



Task Management & Agentic Automation.

Mensch- + KI-Aufgaben in einer Engine. Vier Autonomie-Stufen. IMS-Jahreskalender steuert wiederkehrende Arbeit. Multi-Source-Erstellung. Jira & ServiceNow synchronisiert.

L0 Manuell

Nur Mensch-Aufgabe. Agent wird nicht tätig.

L1 Vorschlagen

Agent schlägt vor · Mensch entscheidet über die Anwendung.

L2 Ausführen · Freigeben

Agent erledigt die Arbeit · Mensch gibt vor dem Commit frei.

L3 Autonom

Agent führt innerhalb von Guardrails aus · Audit-protokolliert.

IMS - JAHRESKALENDER · WIEDERKEHRENDE AUFGABEN

Vorgeladen über ISMS · AIMS · PIMS · CSMS · BCMS.

- Governance · Policy-Reviews · MR-Zyklen
- Compliance · Rechtsregister · Pflichten
- Risiko · Register-Review · Behandlungsstatus
- BCM · BIA · BCP · DR-Testfenster
- Lieferanten · Re-Assessments · AVV-Verlängerungen
- IAM · Access-Reviews · Joiner-Leaver
- Audit · intern · Management Review

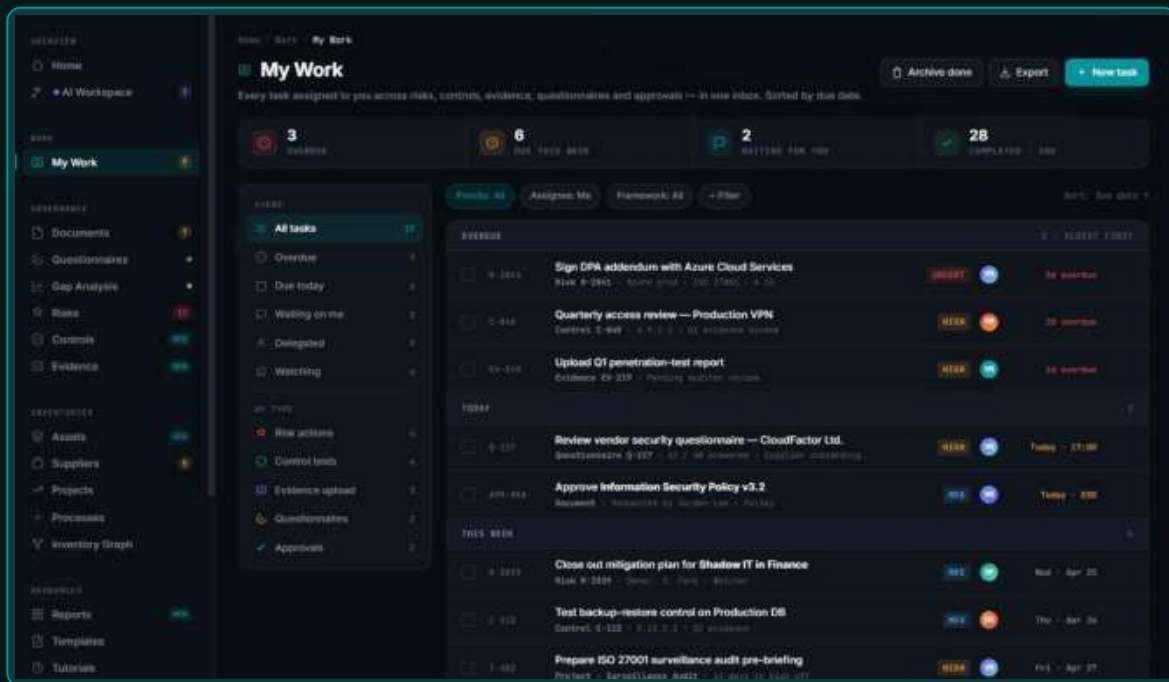
AUFGABEN-ERSTELLUNG AUS MEHREREN QUELLEN

Jedes Modul schiebt Arbeit in die gemeinsame Queue.

- ▶ Audit-Findings · Ergebnisse der Gap-Analyse
- ▶ Risikobehandlung · Incident Response
- ▶ Lieferanten-Assessments · Vertragsverlängerungen
- ▶ Schwachstellenbehebung · Least-Privilege-Findings
- ▶ → Jira / ServiceNow · Last-Write-Wins

My Work — jede Zuweisung in einer Inbox.

Jede Ihnen zugewiesene Aufgabe über Risiken, Controls, Nachweise, Fragebögen und Freigaben hinweg — sortiert nach Fälligkeit, segmentiert nach Typ und Priorität. Mensch- und KI-Aufgaben teilen dieselbe Engine.



WARUM DAS ZÄHLT

● Drei Prioritäts-Lanes · live

3 überfällig · 6 fällig diese Woche · 2 wartend · 28 in den letzten 30 Tagen abgeschlossen.

● Modulübergreifende Vereinheitlichung

Risiko-Aktionen · Control-Tests · Nachweis-Uploads · Fragebögen · Freigaben — in einer Queue.

● Gefilterte Ansichten · Smart Sort

Priorität · Bearbeiter · Framework · Typ · Fälligkeit — gespeichert oder ad-hoc, exportierbar als CSV.

Incident Management · 6 Module + KI-Layer.

Wenn etwas bricht, läuft die Uhr. NIS2 24 h · DSGVO 72 h · DORA · CRA Art. 14 · AI Act — jede Uhr startet automatisch. 15+ Playbooks · 3 Eskalationsstufen · KI-unterstützt.

NIS2 · 24 h

DORA

DSGVO · 72 h

CRA Art. 14

AI Act

01 IncidentEngine

CRUD · Lifecycle · State Machine · Audit-Log. Single Source of Truth von der Erkennung bis zum Abschluss.

REST API · Webhook

02 EscalationEngine

Regelbasierte Auto-Eskalation · On-Call-Rotation · SLA-Tracking. 3 Stufen mit Override-Pfaden.

Event-getrieben

03 PlaybookEngine

15+ vorgefertigte Playbooks: Ransomware · Data Exfil · DDoS · Lieferanten-Breach · KI-Missbrauch. KI erzeugt individuelle bei Bedarf.

REST API · KI-generiert

04 RegulatoryEngine

Erkennt Meldepflichten automatisch über NIS2 · DORA · CRA · AI Act · DSGVO. Verwaltet Fristen. BSI-API-Export.

REST API · BSI-API

05 NotificationEngine

Kunden- / Partner-Benachrichtigungen über mehrere Kanäle. Pflichten werden aus den vertraglichen Anforderungen gezogen. SLA-getrackt.

E-Mail · Portal · ServiceNow

06 TabletopEngine

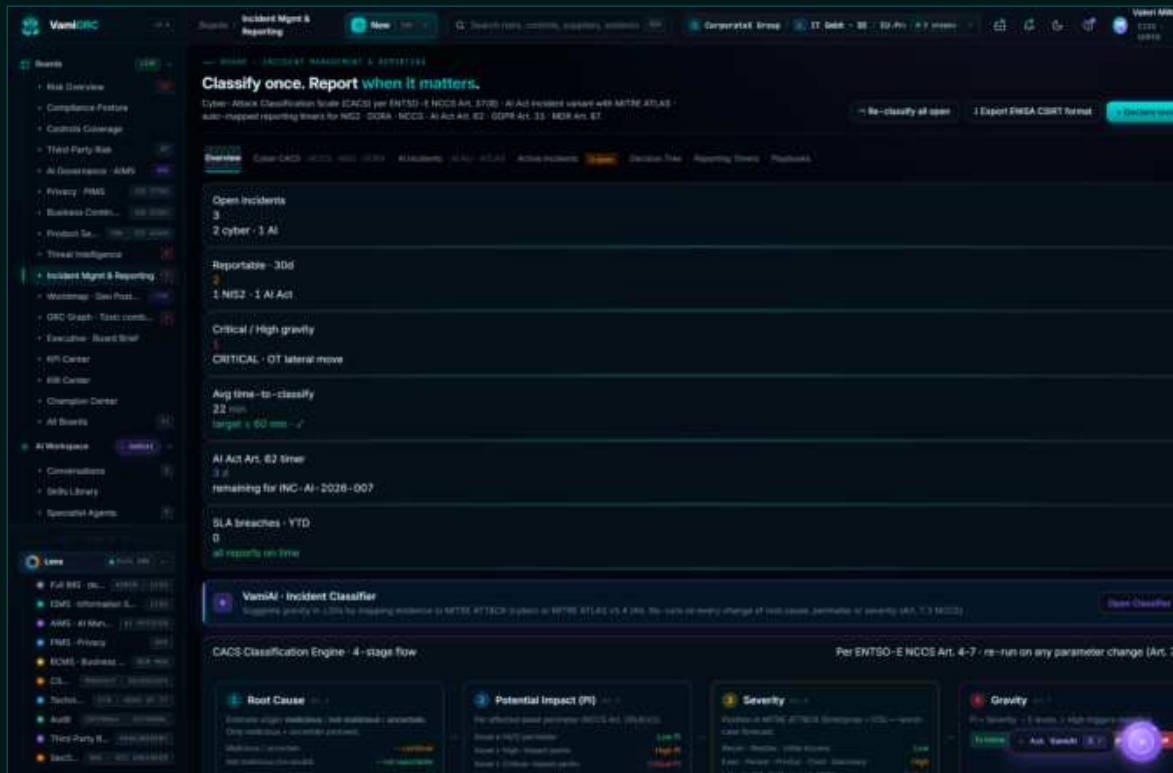
Tabletop-Übungen planen, durchführen und dokumentieren. Auto-Evaluation gegen Playbook-Konformität. ISO 22301 §8.5 Nachweis.

REST API

Eine Incident Engine · eine BCM Engine · eine DRP Engine · ein Graph. Einmal testen → ISO 22301, NIS2 BCM und DORA erfüllen.

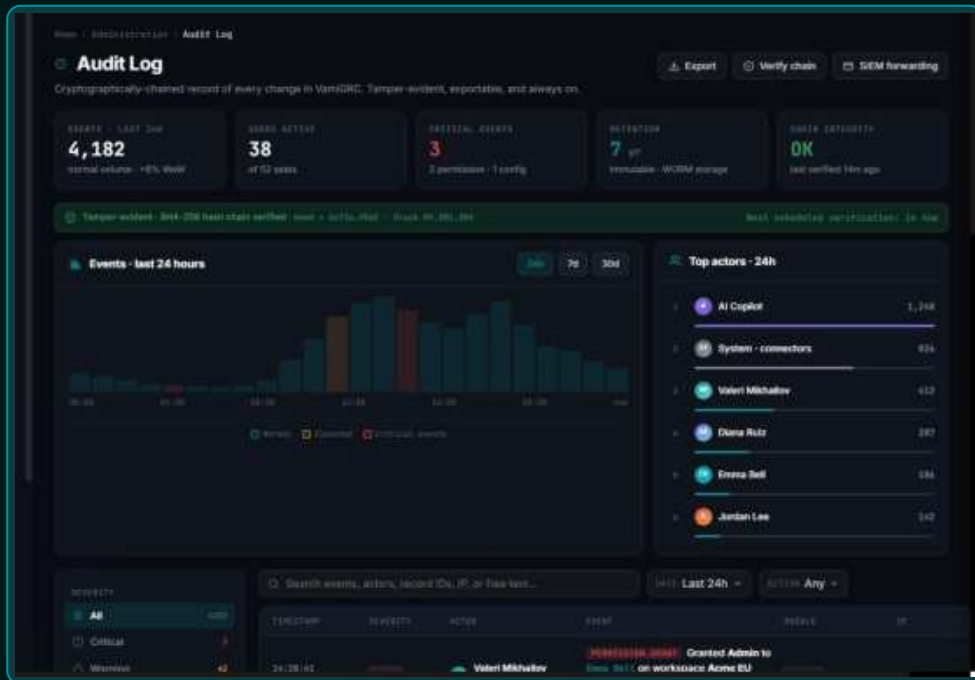
CACS-basiertes Incident Management und Reporting.

Offene Incidents werden automatisch auf NIS2 · DORA · NCCS · AI Act · DSGVO · MDR · CRA gemappt. Ein Timer-Panel. Alle Uhren.



Immutable Audit Log — manipulationssicher, immer aktiv.

Kryptografisch verkettete Aufzeichnung jeder Änderung in VamiGRC. SHA-256-Hash-Chain · WORM-Speicher · 7 Jahre Aufbewahrung · SIEM-Forwarding · regulatorisch geeigneter Export.



WARUM DAS ZÄHLT

● Chain-Integrität: OK

Zuletzt vor 14 Min. verifiziert · Block #4.281.204
· nächste geplante Verifizierung in 46 Min.

● 4.182 Events / 24 h · normal

+6 % WoW · 3 kritische Events · 38 aktive Nutzer
— Anomalieerkennung standardmäßig an.

● Top-Akteure · Top-Module

KI-Copilot · System-Konnektoren · benannte Nutzer — jedes Event mit Zeitstempel, Schweregrad, IP.

Security & Trust — gebaut für regulierte Branchen.

Deutsche Cloud · Zero-Trust-Isolation · Auditierbarkeit · Zertifizierte Expertise.

Deutsche Cloud · Open Telekom Cloud



- ▶ Daten ausschließlich in deutschen Rechenzentren
- ▶ DSGVO Art. 44+ — keine Drittlandtransfers
- ▶ Infrastruktur von T-Systems / Deutsche Telekom
- ▶ ISO-27001-zertifizierter Cloud-Anbieter

Tenant-Isolation & Zero Trust

- ▶ Strikte Datentrennung zwischen Mandanten
- ▶ Keycloak-JWT-Validierung & Rollendurchsetzung
- ▶ Kein mandantenübergreifender Zugriff by Design
- ▶ Dedizierte Namespaces für Dokumente & Indizes

Compliance & Auditierbarkeit

- ▶ Vollständiger, unveränderlicher Audit-Trail
- ▶ Nachweisbasierte Antworten mit Quellenangaben
- ▶ Exportierbare Berichte & signierte Downloads
- ▶ DSGVO-Art.-32-Logging-Richtlinien

Zertifizierungen & Expertise

- ▶ ISO 27001- & ISO 42001-Lead-Auditoren
- ▶ AI-Act-konformer Systembetrieb
- ▶ BSIG-§8a-Kompetenz
- ▶ EU AI Act — KI-System mit begrenztem Risiko

VamiGRC vs. traditionelle GRC-Tools — ein struktureller Unterschied.

Kein Features-Vergleich, ein Kategorienwechsel.

Capability	Traditionelle GRC-Tools	VamiGRC
KI-native Automatisierung	<i>Nein / nur assistierend</i>	✓ Vollständig agentisch
Multi-Framework in einem System	<i>Selten; oft Add-on</i>	✓ ISMS · AIMS · PIMS · CSMS · BCMS
Risikoregister auf einen Prompt	<i>Nein — manuell</i>	✓ Vollautomatisiert in Minuten
Agentisches Lieferanten-Assessment	<i>Nein</i>	✓ OSINT + Fragebogen auf Autopilot
Deutsche Cloud / DSGVO-konform	<i>Oft US-basiert</i>	✓ Open Telekom Cloud, deutsche Rechenzentren
Nachweisbasierte KI-Antworten	<i>Nein</i>	✓ Gestützt auf Ihre ISMS-Dokumente
Lens-Funktion (rollenoptimiert)	<i>Nein</i>	✓ 9 rollenspezifische Workspaces
Preis-Leistung im Mittelstand	<i>Oft >50.000 €/Jahr</i>	✓ Skalierbar ab Mittelstand aufwärts

VamiGRC × Claude-Ökosystem.

• ROADMAP

Das GRC-Rückgrat für jeden Claude-Nutzer im Unternehmen — kein Kontextwechsel, keine eigenen Konnektor-Entwicklungen.

1

VamiGRC ALS MCP-SERVER

Externe Claude-Instanzen lesen/schreiben in VamiGRC — in Chrome, Code, Desktop, Excel, Cowork.

2

VamiGRC ALS MCP-CLIENT

Interne VamiAI-Agenten nutzen externe MCP-Server — Wiz, GitHub, Microsoft, SAP, BSI.

3

Claude-native UX-Patterns

Skills, Slash-Befehle, Tool Use, Artifacts — dieselbe Experience wie in jedem anderen Claude-Workflow.

7 CLAUDE-OBERFLÄCHEN • EIN VERTEILTES KI-FABRIC

C

Claude.ai

Web · Desktop · Mobile

C

Chrome

Agentisches Browser-
Plugin

C

Claude Code

Terminal-Coding-Agent

C

Excel

Spreadsheet-Agent

C

Cowork

Desktop-Datei-/E-Mail-
Agent

C

API

Programmatisch &
Batch

C

Skills

Wiederverwendbare
Anweisungen

Browser-Plugin + Skills-Bibliothek — Claude lernt GRC.

• ROADMAP

Aus jedem Tool erfassen · einmal installieren, GRC-Capability überall.

BROWSER-PLUGIN · ERFASSEN VON ÜBERALL

SAP LeanIX → 47 VamiGRC-Assets gemappt

Wiz Findings → 8 kritische Risiken in 11 s

BSI Advisory → Rechtsregister + Impact

Microsoft Trust → Lieferant + 2 Zertifizierungen

ServiceNow → Incident + NIS2-/DSGVO-Aufgaben

SKILLS-BIBLIOTHEK · IM GESAMTEN CLAUDE-ÖKOSYSTEM INSTALLIERBAR

vamigrc-risk-analysis

vamigrc-audit-finding

vamigrc-regulation-
classifier

vamigrc-control-mapper

vamigrc-pentest-
interpreter

vamigrc-incident-
classifier

vamigrc-vendor-
questionnaire

vamigrc-evidence-
packager

MCP-nativ bedeutet: Jedes neue Tool im Claude-Ökosystem wird integrierbar — ohne eigene Entwicklung.

TEIL II

GRC as a Service.

Umfassende IT-Security- und Compliance-Sicherheit mit VamiGRC.

Wir lizenzieren Ihnen nicht nur die Plattform — wir betreiben sie für Sie.

Virtual CISO · kontinuierliches Monitoring · Audit-Vorbereitung · Incident Response · Managed-Pentest-Zyklen · Beantwortung von Kunden-Due-Diligences — mit VamiGRC als Betriebssystem.

Compliance is an ongoing management responsibility —
regulatory and contractual requirements evolve continuously.

REGULATIONS & FRAMEWORKS



NIS2



DORA



EU AI Act



CRA



ISO/IEC 27001



ISO/IEC 42001



ISO 22301



CSMS-Standards

GRC as a Service

Powered by VamiGRC
AI-native GRC Solution



1 Gap Analysis &
Baseline Assessment



2 Roadmap &
Prioritization



3 Implementation Support &
Evidence Management



4 Continuous Monitoring,
Reporting &
Improvement

ADDITIONAL SERVICES



External CISO



External AI /
AI Officer



Policy &
Process Design



Risk Assessments &
Technical Measures

MANAGEMENT BENEFITS



Continuous
Compliance



Clear Management
Transparency



Reduced
Audit Effort



Scalable for
New Regulations



Audit-Ready
at Any Time

Compliance is not completed once — it is continuously managed.

Modular Expert Roles for GRC as a Service

vCISO, vAI Officer, vDPO and vCSIRT/vPSIRT for Governance, Compliance, Data Protection and Incident Readiness

• Powered by VamiGRC – AI-native GRC Solution •



vCISO

- ✓ Security Strategy & Governance
- ✓ ISMS Management & Risk Management
- ✓ Management Reporting & Board Sparring
- ✓ Coordination of Measures & Service Providers



vAI Officer

- ✓ AI Governance & EU AI Act
- ✓ Use Case Classification & Gap Analyses
- ✓ Secure AI Usage & Control Framework
- ✓ Policies, Role Model & Evidence



vDPO

- ✓ Data Protection Governance & GDPR
- ✓ TOMs, Records of Processing & DPIA
- ✓ Data Subject Rights & Incident Support
- ✓ Advisory, Training & Data Processing Agreements



vCSIRT / vPSIRT

- ✓ Incident Readiness & Playbooks
- ✓ Triage, Coordination & Crisis Support
- ✓ Vulnerability Disclosure & Product Security
- ✓ Lessons Learned & CAPA Management

Shared Delivery Elements



Governance & Policies



Risk & Action Management



Evidence Management in VamiGRC



Reporting, KPIs & Steering



Audit & Assurance Readiness



Modular and scalable



Close to management



Audit-oriented

Flexible engagement model – as an interim function, co-managed service or strategic support.

04

Business · Roadmap · Trust

GRCaaS · Partner · ROI · Roadmap

Drei Delivery-Modelle. Eine Plattform. Dieselben Daten.

Von der Self-Service-Lizenz bis zum Fully-Managed — Ihr Engagement, Ihre Kadenz, Ihr Scope.

TIER 1

Plattform

Self-Service

VamiGRC SaaS. Ihr Team betreibt. Wir liefern Updates, Support, Schulungen.

- ▶ Multi-Tenant-SaaS
- ▶ Standard-SLAs
- ▶ Onboarding in 4 Wochen
- ▶ Ideal für: interne GRC-Teams

TIER 2

Co-Managed

Hybridbetrieb

Ihr Team + unsere Experten teilen sich die Plattform. Wir übernehmen, wofür Ihnen die Zeit fehlt.

- ▶ Geteilter Workspace
- ▶ Quartalsweise Business Reviews
- ▶ Benannter Delivery-Lead
- ▶ Ideal für: schlanke Security-Teams

TIER 3

Fully Managed

GRC-as-a-Service

VamiSec betreibt Ihr IT-Security- & Compliance-Programm Ende-zu-Ende auf VamiGRC.

- ▶ Dedizierter vCISO
- ▶ Alle 6 Service-Säulen
- ▶ Monatliches Vorstands-Reporting
- ▶ Ideal für: KMU · reguliert · KRITIS

Partnerprogramm — betreiben Sie VamiGRC für Ihre Kunden.

Drei Partnerstufen für Beratungen, MSSPs und Systemintegratoren. Wir liefern Plattform und Methodik. Sie besitzen die Kundenbeziehung.

TIER 1

Referral

Lead-Sharing

Senden Sie qualifizierte Leads an VamiSec. Erhalten Sie eine Referral-Gebühr bei abgeschlossenen Deals. Co-Marketing-Materialien inklusive.

- ▶ Gebrandetes Co-Marketing-Kit
- ▶ Referral-Gebühr bei Abschluss
- ▶ Quartalsweise Enablement-Sessions
- ▶ Ideal für: GRC-Beratungen

TIER 2

Implementierung

Co-Delivery

Zertifizierte VamiGRC-Berater auf Ihrer Bench. Gemeinsame Lieferung von Audits, Gap-Analysen, ISMS-Rollouts. Geteilte Marge.

- ▶ Bench mit zertifizierten Beratern
- ▶ Gemeinsames Delivery-Modell
- ▶ Umsatzbeteiligung bei Services
- ▶ Ideal für: Boutique-Auditfirmen

TIER 3

MSSP

Run-as-Your-Service

Tenant pro Kunde. Ihr Service, unser Rückgrat. Komplettes VamiGRC-Fabric.

- ▶ Isolierter Mandant pro Kunde
- ▶ Voller Zugriff auf das VamiGRC-Fabric
- ▶ vCISO-Backbone optional
- ▶ Ideal für: MSSPs · große Integratoren

Messbarer ROI. Sofort realisierbar.

Harte Zahlen aus den vier Bereichen, in denen GRC traditionell Zeit und Qualität verliert.

80–95%

Reduktion der manuellen
Compliance-Arbeit

Echtzeit

Time-to-Report
vs. 2–5 Tage manuell

>95 %

Konsistenz bei
Sicherheitsfragebögen

ISMS-Teams & CISOs

- ▶ Keine manuellen Gap-Analysen mehr
- ▶ Fragebögen in Minuten statt Tagen
- ▶ Audit-Vorbereitung automatisiert

Management & Vorstand

- ▶ Priorisierte Risiken auf Knopfdruck
- ▶ Compliance-Dashboard in Echtzeit
- ▶ Executive Reporting automatisiert

Fachbereiche

- ▶ ISMS-Fragen eigenständig beantwortet
- ▶ Kein Warten auf den CISO für Policy-Infos
- ▶ Awareness ohne Schulungs-Overhead

Lieferantenmanagement

- ▶ Assessments auf Autopilot
- ▶ AVV / NDA digital verwaltet
- ▶ Lieferketten-Sicherheit im großen Maßstab

Von Zahlen zu Ergebnissen — ein Reality-Check für den Mittelstand.

Personen · 1.200 Mitarbeitende · 87 Lieferanten · 23 KI-Use-Cases · NIS2 im Scope · TISAX-zertifiziert.

14→2

FTE-Wochen → Tage
NIS2-Audit-Vorbereitung

87

Lieferanten neu bewertet
5 Tage statt 6 Monate

340 k €

Jährliche FTE-Einsparung
vs. manuelle Baseline

4×

Audit-Zyklen / Jahr
ohne Personalaufbau

Audit-Vorbereitung

- ▶ 14 FTE-Wochen → 2 FTE-Tage
- ▶ NIS2 + ISO 27001 + TISAX in einem Durchgang
- ▶ Auditor-Portal · Live-Nachweise

Lieferanten-Onboarding

- ▶ OSINT-Scan · Fragebogen · AVV
- ▶ 3 Stunden pro Lieferant (vorher 2 Wochen)
- ▶ AVV-Ablauf automatisch nachverfolgt

Beantwortung Kunden-DD

- ▶ CAIQ/SIG in 4 Stunden beantwortet
- ▶ >95 % Antwortkonsistenz
- ▶ Gebrandetes Trust Center automatisch veröffentlicht

Risikoregister

- ▶ 1.200 Mitarbeitende an 1 Tag erfasst
- ▶ ISO 31000- + 27005-konform
- ▶ Mitigationsplan automatisch erzeugt

Schluss mit Swivel-

Chairing.

Beginnen Sie GRC zu automatisieren – von

Ihr Ansprechpartner für intelligente GRC-Architektur

Wir freuen uns auf eine erfolgreiche Zusammenarbeit



Valeri Milke
CEO

- 15 Jahre Erfahrung in IT-Sicherheit & Compliance, CISO, Application Security, Pentesting, ISMS und Incident Response & Forensik
- Lead Auditor (ISO/IEC 27001 & ISO/IEC 42001)
- **BSI IT-Grundschutz-Praktiker**
- **Experte für NIS2, DORA, CRA und AI Act**
- **Datenschutzbeauftragter (IHK)**
- KI-Beauftragter gemäß EU AI Act



+49 155 6096 2044



valeri.milke@vamisec.com



<https://www.linkedin.com/in/valeri-milke/>

Die VamiSec GmbH vereint über 15 Jahre Erfahrung in IT-Sicherheit und Compliance mit dem Anspruch, maßgeschneiderte Lösungen zu entwickeln, die Werte schützen und Innovation fördern. 150 erfolgreich abgeschlossene Projekte und über 70 Kunden



VamiSec GmbH, Bornheimer Straße
127, 53119 Bonn



Termin buchen



<https://www.vamisec.com/>