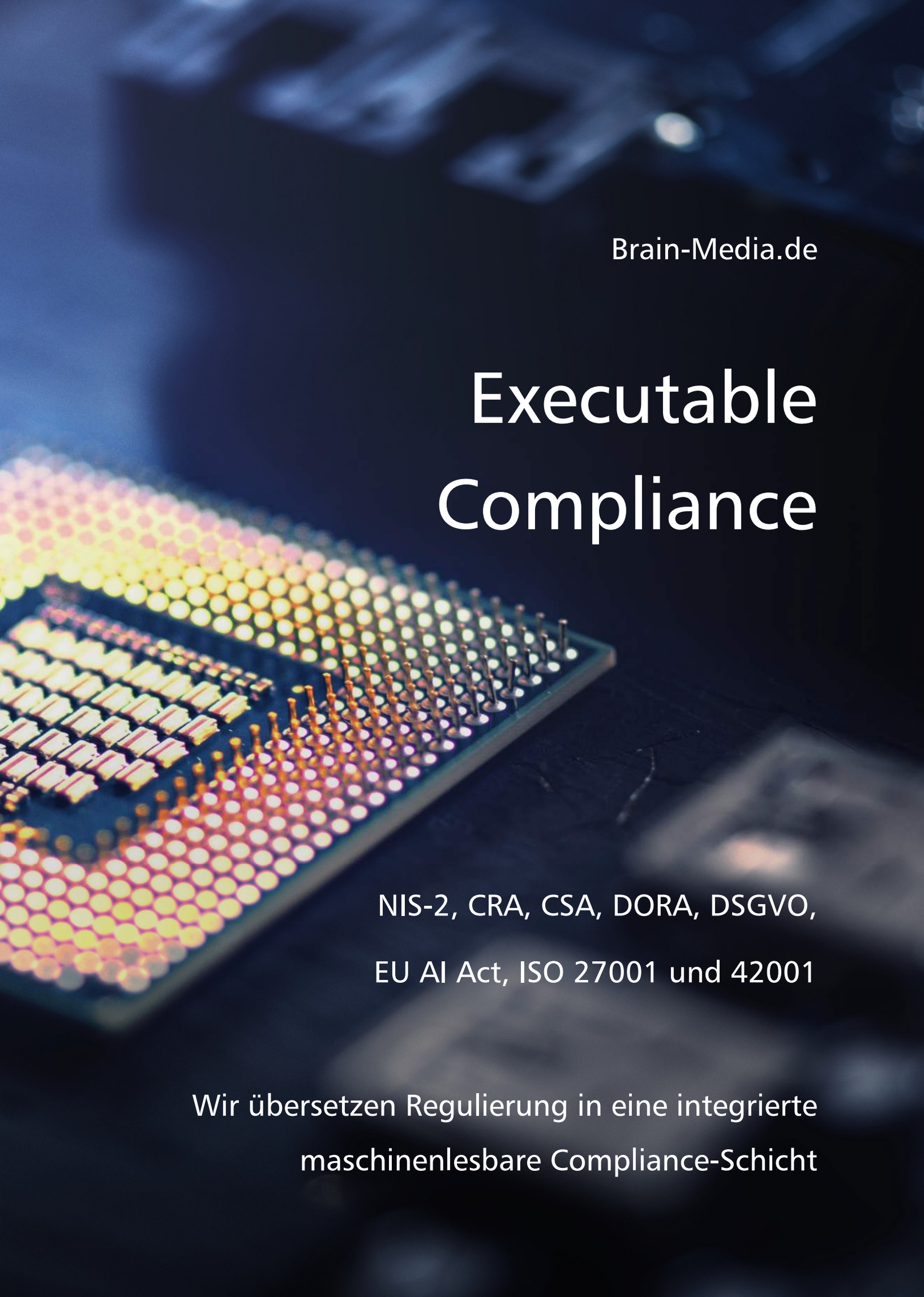


Brain-Media.de

Executable Compliance

NIS-2, CRA, CSA, DORA, DSGVO,

EU AI Act, ISO 27001 und 42001

Wir übersetzen Regulierung in eine integrierte maschinenlesbare Compliance-Schicht

Das Problem

Regulatorische Anforderungen sind kein Wissensproblem.

Sie sind ein Umsetzungsproblem.

NIS-2, CRA, CSA, DORA, DSGVO, EU AI Act, ISO 27001 und ISO 42001 betreffen

tausende Unternehmen in Deutschland –

mit konkreten Fristen, Bußgeldern und Haftungsrisiken.

Die meisten Unternehmen haben das Problem erkannt,

aber die operative Umsetzung stockt.

Typische Vorgehensweise	Die Herausforderung
PDF-Stapel und Word-Dokumente	Unstrukturiert, nicht automatisierbar
Externe Berater und Workshops	Teuer, zeitintensiv, keine nachhaltige Lösung
Manuelle Gap-Analysen	Fehleranfällig, nicht audit-ready
Fragmentierte Tool-Landschaft	Kein einheitliches Datenmodell, inkonsistente Daten, hoher Pflegeaufwand, keine Single Source of Truth

Das Ergebnis

Compliance bleibt ein Projekt, das nie fertig wird – statt eines Systems, das läuft.

Während klassische Ansätze Compliance als „Dokumentationslast“ begreifen, transformiert BAM sie in Infrastruktur-Code. Cross-Controls sorgen dafür, dass Überlappungen gewürdigt werden – und sich der Aufwand signifikant reduziert.

Durch die maschinenlesbare Aufbereitung (JSON) entfällt die manuelle Interpretation von Gesetzestexten durch teure Berater nahezu vollständig.

Die Lösung

Mit BAM überführt Brain-Media.de regulatorische Anforderungen in ein maschinenlesbares Wissensmodell. Jede Anforderung wird in sechs operative Ebenen aufgebrochen:

Ebene	Was es ist	Ihr Nutzen
Requirement	Regulatorische Anforderung (z. B. NIS-2 Art. 21)	Wissen, was gilt – priorisiert und verständlich
Gap-Check	Prüffrage	Wissen, wo Lücken sind – priorisiert und verständlich
Remediation	Behebungsanleitung	Wissen, wie Lücken geschlossen werden – priorisiert und umsetzbar
Risk	Risikobewertung mit Likelihood & Impact	Verstehen, was auf dem Spiel steht
Control	Konkrete Maßnahme mit Umsetzungshinweisen	Wissen, was zu tun ist – direkt umsetzbar
Evidence	Nachweistyp mit editierbarem Template	Auditoren überzeugen – mit einem Klick

BAM ist kein Framework, sondern eine ausführbare Compliance-Infrastruktur.

Während klassische Frameworks Anforderungen beschreiben, stellt BAM die Logik zur operativen Umsetzung und Automatisierung bereit.

Audit-Nachweis: Checkliste · Template · JSON/BAM-Export · Compliance-Dashboard

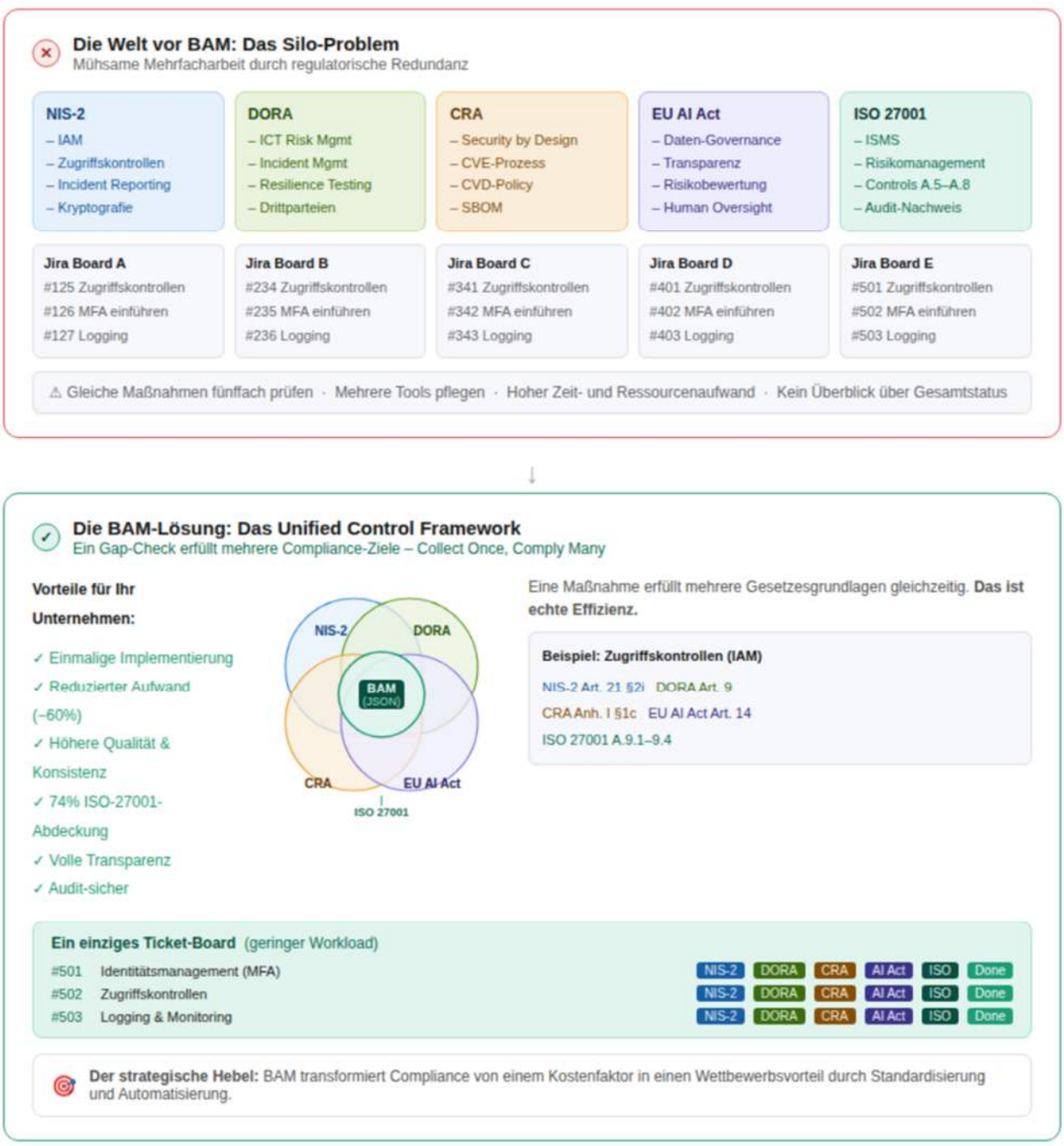
Bereitgestellt als JSON, Markdown und SCORM – direkt nutzbar in GRC-Tools, KI-Systemen und automatisierten Workflows.

JSON-Code-Snippet.

BAM als Unified Control Framework

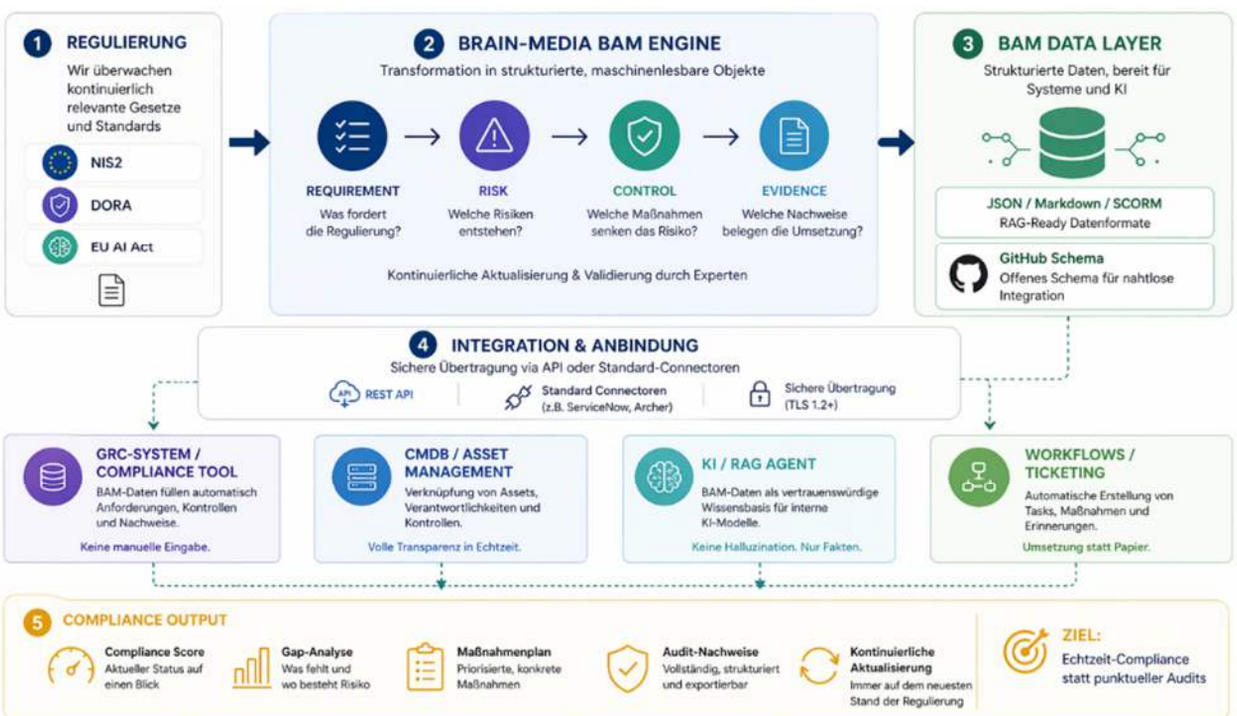
BAM folgt dem Unified Control Framework-Ansatz – geht aber darüber hinaus: Es transformiert statische Anforderungen in ausführbare, integrierbare Compliance-Logik. Für das Unternehmen bedeutet das: Eine einmal implementierte Maßnahme erfüllt automatisch die Anforderungen mehrerer Gesetzesgrundlagen.

Wir nennen das: Collect Once, Comply Many.



Die BAM-Referenzarchitektur

Die BAM-Referenzarchitektur überführt statische Regulierung in einen dynamischen Datenfluss. Über standardisierte Schnittstellen (REST-API/JSON) wird der Compliance-Layer direkt in Ihre GRC-Systeme und internen KI-Agenten integriert. Statt manueller Dokumentation füttern validierte BAM-Objekte Ihre Systeme mit prüffähigen Anforderungen, Risiken und Controls. Das Ergebnis: Ein kontinuierlicher Compliance-Zyklus, der Automatisierung ermöglicht und Audit-Ready-Status in Echtzeit liefert. BAM fungiert als Compliance Execution Layer zwischen Regulierung und operativen Systemen.

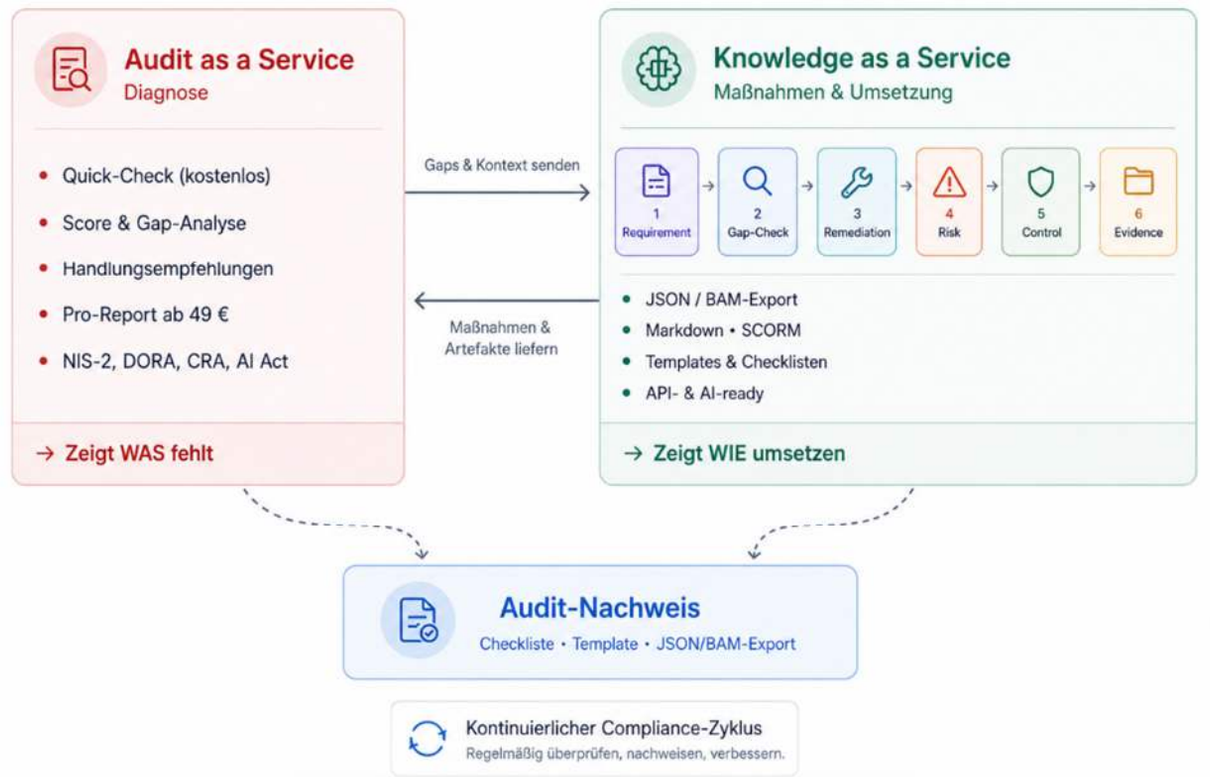


Executive Compliance – von der Regulierung zur automatisierten Umsetzung.

Die Bereitstellung in Markdown und JSON ermöglicht es Unternehmen, ihre internen Large Language Models (LLMs) mit validierten, regulatorischen Fakten zu füttern. Dies reduziert Halluzinationen in der Compliance-KI und schafft eine verlässliche Wissensbasis für automatisierte Antworten.

Das Wechselspiel: KaaS und AaaS

Executable Compliance basiert auf zwei Produkten, die sich gegenseitig verstärken. Keines ist ohne das andere vollständig.



Wechselspiel zwischen Audit as a Service (AaaS) und Knowledge as a Service (KaaS)

Audit as a Service (AaaS) – Diagnose

AaaS liefert den strukturierten Compliance-Status: Score, Gap-Analyse und priorisierte Handlungsempfehlungen für alle acht Frameworks.

Compliance-Stresstest kostenlos – Compliance-Score in wenigen Minuten

Score & Gap-Analyse – Zeigt, **was** fehlt

Handlungsempfehlungen – priorisiert nach Risiko

Knowledge as a Service (KaaS) – Maßnahmen

KaaS liefert ausführbare Remediation-Logik zur Schließung identifizierter Gaps: kontinuierlich aktualisierte Compliance-Inhalte als Abonnement in vier Tarifen.

Requirement → **Gap-Check** → **Remediation** → **Risk** → **Control** → **Evidence**

JSON / BAM-Export – direkt integrierbar in GRC-Tools und KI-Systeme

Markdown, SCORM, Templates – alle Formate enthalten

API- & AI-ready – zeigt, **wie** umzusetzen ist

Der kontinuierliche Zyklus

AaaS identifiziert Gaps

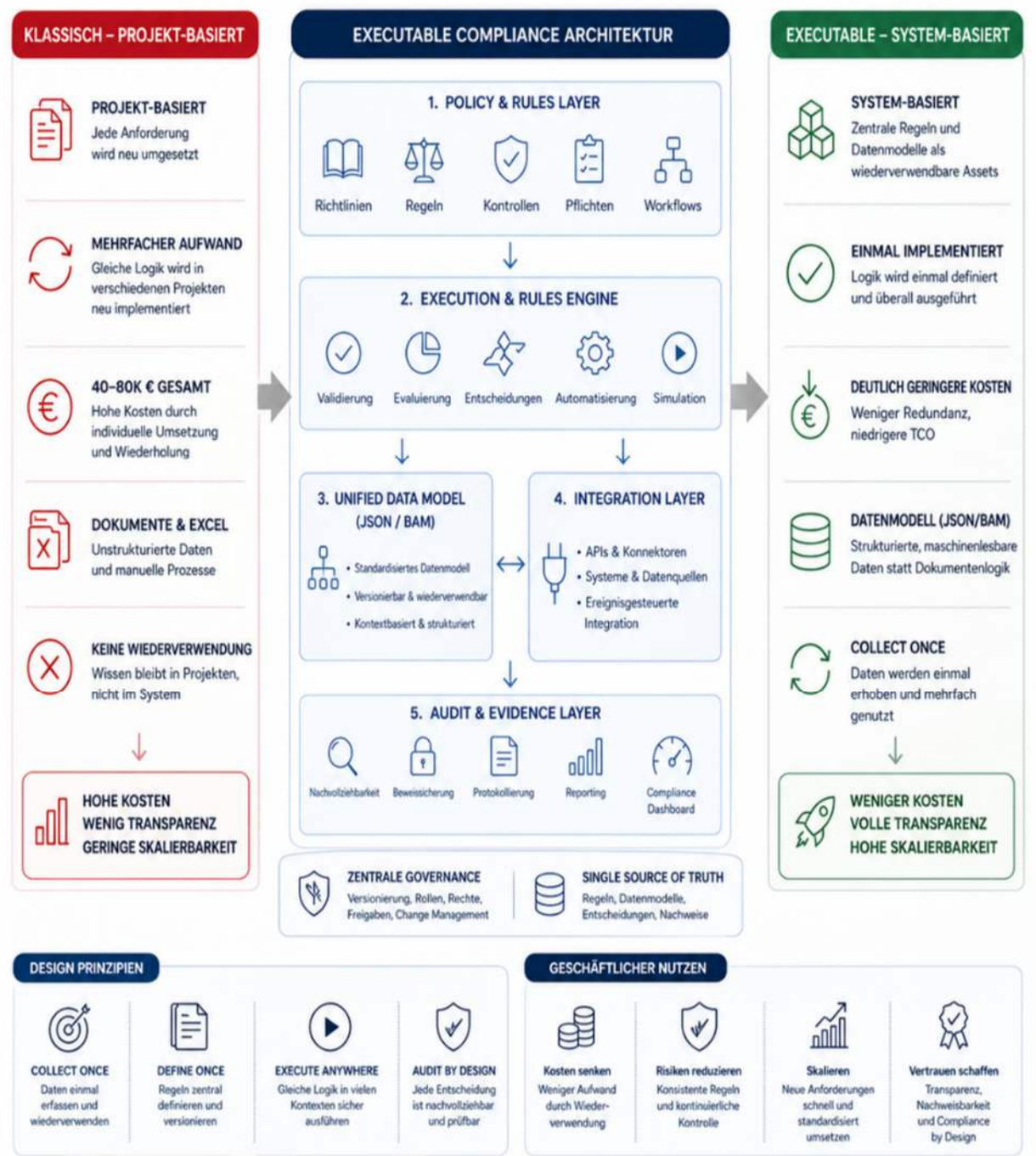
→ KaaS liefert Remediation

→ AaaS validiert

→ ein auditfähiger, kontinuierlicher **Compliance-Zyklus**.

Klassische, projektbezogene vs. datenmodellgetriebenen Ansatz

Während der klassische, projektbasierte Ansatz durch unstrukturierte Daten in Excel und redundante, manuelle Prozesse zu hohen Kosten und geringer Skalierbarkeit führt, verschiebt die Executable-Compliance-Architektur den Fokus auf ein zentrales, wiederverwendbares Datenmodell, das durch das Prinzip „Collect Once, Comply Many“ volle Transparenz und eine signifikante Reduktion des Aufwands ermöglicht.



Ein System – vier Modelltarife

Plan	Preis/Jahr in EUR	Nutzer	Zielgruppe
Personal	99	1	IT-Leiter, Freiberufler, KMU
Professional	249	bis 5	IT-Teams, Compliance-Abteilungen, Berater
Business	499	bis 20	Mittelstand, IT-Dienstleister, MSSP
Enterprise	ab 999	unbegr.	Konzerne, KRITIS, Berater mit Kundenprojekten

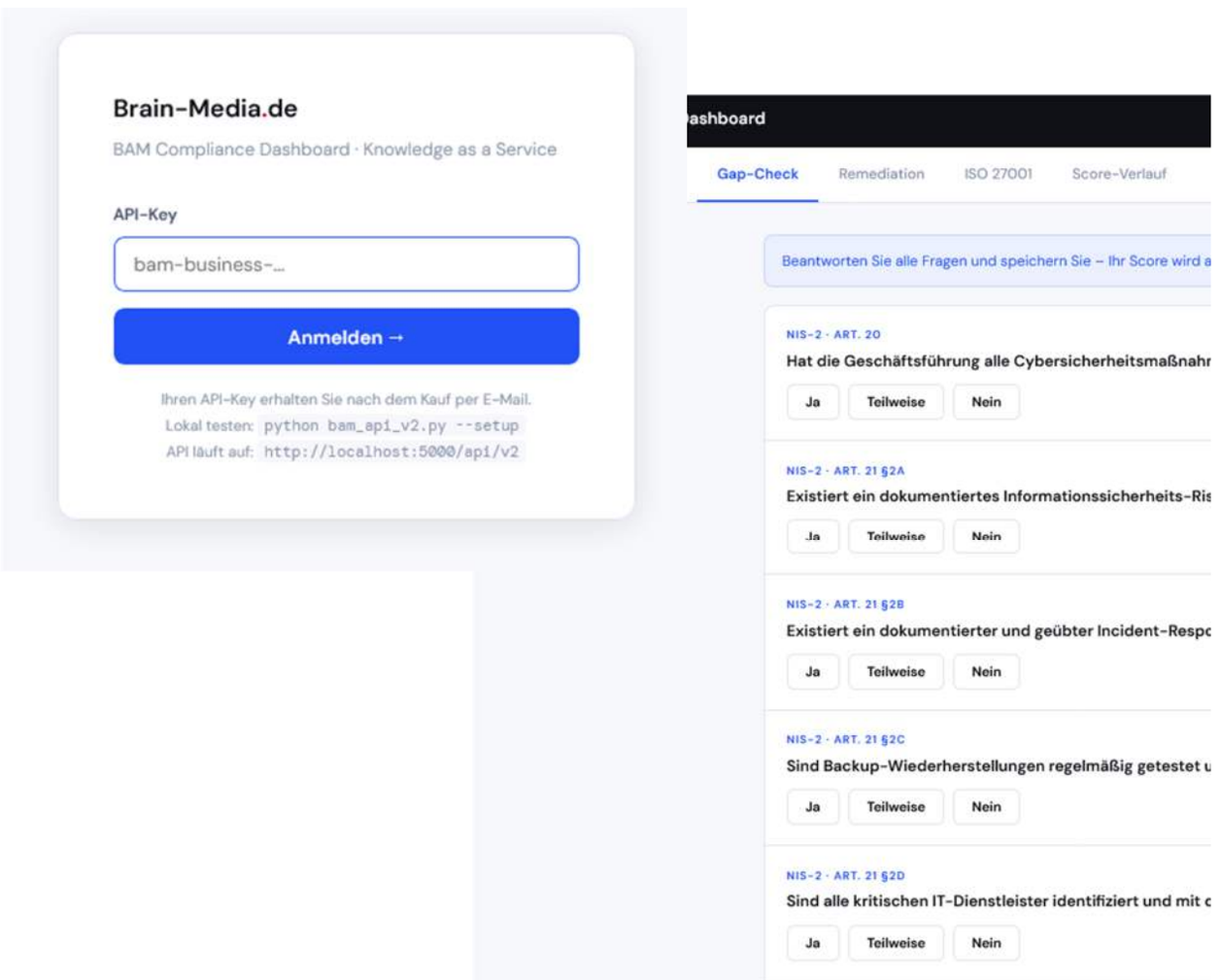
Für wen ist Executable Compliance?

Zielgruppe	Ihr Nutzen	Einstieg
IT-Leiter & Compliance-Verantwortliche Mittelstand 50–500 MA	Audit-ready ohne externe Berater. Klare Anforderungen, direkt umsetzbar.	Personal oder Professional
CISOs & GRC-Architekten Enterprise & Konzerne	JSON/BAM zur Integration in GRC-Tools und KI-Assistenten.	Business oder Enterprise
IT-Dienstleister & MSSPs Berater mit Kundenprojekten	Strukturierte Inhalte für eigene Kundenprojekte. White-Label möglich.	Enterprise oder Personal

MSSPs und Berater nutzen BAM als White-Label-Infrastruktur. Statt für jeden Kunden das Rad neu zu erfinden, beziehen sie den standardisierten Datenstrom von Brain-Media und konzentrieren sich auf die hochpreisige Implementierung.

BAM in der Praxis

BAM basiert auf einem klassischen Web-Stack. In den Business- und Enterprise-Varianten erfolgt der Zugriff auf die Datenbank über einen API-Key, den die Kunden beim Erwerb erhalten. Über die API ist auch die nahtlose Integration in die eigene Infrastruktur möglich. Über das webbasierte Dashboard sind alle relevanten Funktionen wie beispielsweise die Gap-Analyse verfügbar.



Durch die webbasierte Bereitstellung transformiert Brain-Media statisches Compliance-Wissen in eine Cloud-native Ressource, die über das BAM-Portal und standardisierte API-Schnittstellen jederzeit abrufbar ist und den nahtlosen Import strukturierter Rohdaten in Ihre digitale Infrastruktur ermöglicht.

Die technischen Details

BAM ist in verschiedenen Tarifen mit unterschiedlichen Features verfügbar – von der Einzelplatzvariante bis zur White-Label-Lösung. Für jede Anforderung die passende Variante.

FEATURE	ENTERPRISE
INHALTE & PORTAL	
Regulatorische Inhalte (NIS-2, CRA, CSA, DORA, DSGVO, EU AI Act, ISO 27001, ISO 42001)	vollständig
Kontinuierliche Inhalts-Updates	✓
Audio-Content	✓
Downloads & Templates	✓
Living Documents	✓
Editierbare Checklisten & Tabellen	✓
Quiz-Module (vollständig)	✓
Markdown-Export	✓
SCORM / LMS-Integration	✓
Nutzeranzahl	unbegrenzt
INFRASTRUKTUR & SICHERHEIT	
Dedizierte, gekapselte Instanz	✓
Nicht erreichbar aus dem Internet	✓
Keine geteilte Datenbank / kein Multi-Tenancy	✓
Datenbank verschlüsselt (at rest)	✓
VPN-gesicherter Zugriff	✓
Serverstandorte Deutschland (Saarbrücken & Frankfurt)	🇩🇪
DSGVO-konform · SSL-verschlüsselt	✓
BAM – OPERATIVE COMPLIANCE-SCHICHT	
Gap-Check – aktive Lückenerkennung NEU	✓
Remediation – Schritt-für-Schritt-Behebung NEU	✓
JSON / BAM-Export für GRC-Tools & KI	✓
REST API-Zugang (optional)	+ 150 €/Monat
Compliance-Dashboard mit Score & Gap-Analyse	✓
ISO 27001 & ISO 42001 Cross-Mapping NEU	✓
ENTERPRISE-OPTIONEN	
Zusätzliche Standorte	ab 25 €/Monat
White-Label für eigene Kundenprojekte	auf Anfrage
Individuelle Anpassungen	✓
Prioritäts-Support	✓
SLA	auf Anfrage
Setup (einmalig)	ab 999 € netto
Basis / Monat (1 Standort)	ab 249 € netto
	Jetzt anfragen

Alle Preise zzgl. MwSt. · Jahresvertrag: 10% Rabatt · Individuelles Angebot auf Anfrage

Compliance als Wettbewerbsvorteil

Executable Compliance schafft messbaren Mehrwert – weit über regulatorische Pflichterfüllung hinaus

BUSINESS CASE 1

Vertrauen & Marktposition

Wer regulatorische Anforderungen jederzeit nachweisen kann, gewinnt Ausschreibungen schneller, überzeugt Kunden in der Due Diligence und stärkt seine Position in Lieferketten. Audit-Readiness wird vom Audit-Vorbereitungs-Stress zur permanenten, sichtbaren Stärke.

VERTRIEBSVORTEIL

BUSINESS CASE 2

Operational Excellence

Standardisierte, automatisierte Kontrollprozesse eliminieren Medienbrüche und manuelle Abstimmungsschleifen. Compliance-konforme Entscheidungen werden in Echtzeit getroffen – schneller, konsistenter und mit messbarer Fehlerreduktion.

EFFIZIENZGEWINN

BUSINESS CASE3

Sales-Beschleunigung

Kürzere Due-Diligence-Zeiten, schnelleres Kunden-Onboarding, weniger Rückfragen im Vergabeverfahren. Wenn Compliance keine Bremse mehr ist, sondern ein abrufbarer Nachweis, verkürzen sich Sales-Zyklen messbar.

UMSATZWIRKUNG

BUSINESS CASE 4

KI-Enabling

BAM-Daten im JSON/Markdown-Format sind nativ RAG-fähig: Sie füttern interne Large Language Models mit validierten, regulatorischen Fakten – kaum Halluzinationen. Compliance-Infrastruktur wird zur KI-Datenbasis und ermöglicht verlässliche KI-Assistenten für Compliance, Risiko und Audit.

KI-GRUNDLAGE

BUSINESS CASE 5

Haftungsminimierung

Lückenlose Audit-Trails und Echtzeit-Dokumentation aller Kontrollmaßnahmen reduzieren das persönliche Haftungsrisiko der Geschäftsführung konkret und nachweisbar. Abweichungen werden im Entstehungsmoment erkannt – nicht erst beim nächsten Audit. Auch Cyber-Versicherungsprämien können durch nachweisbare Kontrollreife sinken.

GF-ABSICHERUNG

Von der Pflicht zum strategischen Hebel

Unternehmen, die Compliance als System implementieren, schaffen in allen fünf Dimensionen gleichzeitig Wert – ohne Mehraufwand, denn eine Maßnahme erfüllt mehrere Frameworks. Das ist Executive Compliance: Compliance, die nicht nur läuft, sondern Wettbewerbsvorteile erzeugt.

Regulatorischer Kalender & Einstieg

Was gilt wann – und wie starten Sie in unter 30 Tagen

FRAMEWORK	INKRAFTTRETEN / FRIST	STATUS	KERNPFLICHT	BUSSGELD-RAHMEN
DSGVO	In Kraft seit Mai 2018	Aktiv Fällig	Verarbeitungsverzeichnis, Rechtsgrundlagen, Datenschutz-Grundsätze	bis 20 Mio. € oder 4 % Umsatz
NIS-2	5. Dezember 2025, NIS2UmsuCG	Aktiv Fällig	Governance, IAM, Incident Reporting, Lieferkette	bis 10 Mio. € oder 2 % Umsatz
DORA	Gilt seit Januar 2025	Aktiv	Finanzsektor, IKT-Risikomanagement, Resilience Testing, Drittparteien	bis 5 Mio. € oder 1 % Tagesumsatz
EU AI Act	Verbote: Feb. 2025, GPAI: Aug. 2025, Hochrisiko: Aug. 2026	Stufenweise	KI-Inventar, Risikoklassifizierung, Transparenz, Oversight	bis 35 Mio. € oder 7 % Umsatz
CRA	In Kraft Nov. 2024, Anwendung ab Dez. 2027	Übergangsfrist	Security by Design, CVE-Prozess, SDL, technische Doku	bis 15 Mio. € oder 2,5 % Umsatz
ISO 27001	Version 2022 seit Okt. 2022, Übergang bis Okt. 2025	Update fällig	ISMS, 93 Controls (neue Struktur), SoA, PDCA	Freiwillig / Marktanforderung
ISO 42001	Standard seit Dez. 2023	Empfohlen	KI-Management-System, Lifecycle, Transparenz	Freiwillig / Marktanforderung
Cyber Solidarity Act	Inkrafttreten 2025/26	In Vorbereitung	BSI-CERT-Registrierung, EU-CSIRT-Anbindung	bis 5 Mio. € oder 1 % Umsatz

In 3 Schritten zur Audit-Rediness

Der BAM-Einstieg – strukturiert, risikoarm, mit messbarem Ergebnis ab Tag 1

1

Quick-Check

Kostenloser Compliance-Stresstest auf brainmedia.de. Compliance-Score für alle 8 Frameworks in wenigen Minuten. Zeigt, wo Sie stehen – Ohne Vorabinvestition.

Kostenlos I Online

2

Gap-Analyse

Pro-Report ab 49 € mit priorisierten Lücken, Bußgeldrisiken und konkreten Handlungsempfehlungen. Audit-ready in einem Dokument.

49 EUR I 2 Std.

3

Remediation (KaaS)

Schritt-für-Schritt-Anleitungen, editierbare Vorlagen, JSON/BAM-Export und kontinuierliche Updates – direkt nutzbar in Ihrem GRC-Tool oder KI.

Ab 99 EUR/Jahr

✓

Audit-Ready

Kontinuierlicher Compliance-Zyklus. Automatisch aktualisiert bei Regulierungsänderungen. Keine manuelle Nacharbeit.

Dauerhaft I Automatisch

Executive Summary

Tausende Unternehmen stehen vor der Umsetzung von NIS-2, CRA, CSA, DORA, DSGVO, EU AI Act, ISO 27001 und ISO 42001.

Das Problem: Regulatorik existiert bisher nur als statischer Text, nicht als System. Wir lösen dies mit dem **Brain-Media Audit Model (BAM)**. BAM überführt Anforderungen in ein maschinenlesbares **Unified Control Framework (UCF)** nach dem Prinzip: **Collect Once, Comply Many.** Das Schema erweitert die Theorie um aktive Praxis:

Requirement → Gap-Check → Remediation → Risk → Control → Evidence

Als JSON, Markdown oder SCORM fließen die Daten direkt in Ihre GRC-Tools oder KIs. **AaaS** identifiziert Lücken durch automatisierte Checks; **KaaS** liefert die Lösung (Remediation) zur Behebung.

Das **Ergebnis**: Ein harmonisierter Compliance-Datenstrom, der Redundanzen eliminiert und den Aufwand durch Cross Controls signifikant reduziert.

Keine Interpretation. Kein Berater. Compliance als System.

BAM reduziert nicht nur den Aufwand, sondern minimiert durch den kontinuierlichen Datenabgleich das **Haftungsrisiko der Geschäftsführung**.

Starten Sie jetzt Ihren kostenlosen Compliance-Stresstest auf Brain-Media.de und erhalten Sie zeitnah Ihren Compliance-Score. Identifizieren Sie Ihre Gaps, bevor es der Auditor tut.

Brain-Media.de · Executable Compliance

BAM Compliance Report

Saar Industrie GmbH · Mai 2026 | BAM v4 · 8 Frameworks · 64 Objekte · Vertraulich

NIS-2	CRA	EU AI ACT	ISO 27001
61%	74%	55%	63%
Handlungsbedarf	Weitgehend konform	Handlungsbedarf	In Umsetzung

DSGVO	ISO 42001	CYBER SOLIDARITY ACT	DORA
48%	40%	70%	—
Kritische Lücken	Handlungsbedarf	Handlungsbedarf	Nicht anwendbar

58%	6	3	8	3	46–75 PT
Gesamt-Score	Offene Gaps	Kritisch (Sofort)	Frameworks	Konform	Aufwand

Gesamt-Compliance-Score: 58% – Handlungsbedarf in NIS-2, EU AI Act und DSGVO.
Drei kritische Lücken erfordern sofortige Maßnahmen: GF-Governance (NIS-2), KI-Inventar (EU AI Act), DSGVO-Grundsätze.
DORA ist für Saar Industrie GmbH als Industrieunternehmen **nicht anwendbar** – wird bei Scope-Änderung geprüft.
BAM v4 deckt alle 8 relevanten EU-Compliance-Frameworks ab. Empfohlener Gesamtaufwand: 46–75 Personentage. Zeitrahmen: 6–9 Monate.

1. Score-Übersicht nach Framework

Framework	Score	Status	Anmerkung
NIS-2	61%	Handlungsbedarf	IAM und Governance priorisieren
DORA	—	Nicht anwendbar	Nur für Finanzunternehmen (Banken, Versicherungen, Wertpapierfirmen)
CRA	74%	Weitgehend konform	SDL-Prozess formalisieren
EU AI Act	55%	Handlungsbedarf	KI-Inventar sofort erstellen
DSGVO	48%	Kritische Lücken	VVT und Grundsätze-Dokumentation fehlen
ISO 27001	63%	In Umsetzung	ISMS-Aufbau nach 2022er Standard
ISO 42001	40%	Handlungsbedarf	KI-Management-System aufbauen
Cyber Solidarity Act	70%	Handlungsbedarf	BSI-CERT-Anbindung fehlt

ℹ️ **DORA (Digital Operational Resilience Act):** Diese Verordnung gilt ausschließlich für Finanzunternehmen (Kreditinstitute, Versicherungen, Wertpapierfirmen u.a.) gemäß Art. 2 DORA. Für Saar Industrie GmbH als Industrieunternehmen ist DORA nicht anwendbar. Bei Änderung des Geschäftsmodells oder bei Einführung von Finanzdienstleistungen ist eine erneute Prüfung erforderlich.

2. Offene Gaps – nach Risiko priorisiert

BAM-ID	Framework	Kategorie	Priorität	Risiko	Bußgeldrisiko
NIS2-021i-IAM	NIS-2	Verwendung von Lösungen zur Kontrolle des Zugangs – Ide…	**SOFORT**	9/9	bis 10 Mio. EUR
CRA-001-SECURITY-BY-DESIGN	CRA	Produkte mit digitalen Elementen müssen unter Berücksic…	**HOCH**	7/9	bis 15 Mio. EUR
AIACT-001-INVENTUR	EU AI Act	Betreiber müssen alle eingesetzten KI-Systeme kennen un…	**SOFORT**	8/9	bis 35 Mio. EUR
DSGVO-005-GRUNDSAETZE	DSGVO	Personenbezogene Daten müssen rechtmäßig, nach Treu und…	**SOFORT**	8/9	bis 20 Mio. EUR
ISO27-005-ISMS	ISO 27001	Aufbau, Implementierung, Betrieb und kontinuierliche Ve…	**HOCH**	7/9	–
CSA-001-CERT-ANBINDUNG	Cyber Solidarity Act	Teilnahme am EU-Cyber-Solidaritätsmechanismus durch Reg…	**HOCH**	7/9	bis 5 Mio. EUR

3. Gap-Analyse – Detailbeschreibungen

NIS2-021i-IAM | NIS-2 · Art. 21 §2i | **SOFORT · Risiko: 9/9**

ANFORDERUNG

Verwendung von Lösungen zur Kontrolle des Zugangs – Identity and Access Management.

PRÜFFRAGE

Ist das Minimalprinzip (Least Privilege) für alle Benutzer- und Admin-Konten implementiert und werden Zugriffsrechte mindestens jährlich überprüft?

Bußgeldrisiko	Aufwand	Frist	ISO 27001:2022
bis 10 Mio. EUR	**10–20 PT**	**kurzfristig**	**5.15, 5.16, 5.18, 5.3 … (ISO 27001:2022)**

REMEDIATION: IAM NACH MINIMALPRINZIP MIT REGELMÄSSIGEM ACCESS REVIEW EINRICHTEN

1. Alle Benutzer- und Service-Konten inventarisieren
2. Zugriffsrechte auf Minimum reduzieren (Least Privilege)
3. Privilegierte Konten (Admin) separieren und mit PAM schützen
4. Halbjährliche Access-Rezertifizierung für alle Konten einführen

📖 NIS-2 Survival Kit – Kap. 12 – Identity & Access Management

CRA-001-SECURITY-BY-DESIGN | CRA · Anh. I §1 | **HOCH · Risiko: 7/9**

ANFORDERUNG

Produkte mit digitalen Elementen müssen unter Berücksichtigung von Security by Design entwickelt werden – kein bekannter ausnutzbarer Exploit bei Markteinführung.

PRÜFFRAGE

Ist Security by Design im Entwicklungsprozess verankert – mit Bedrohungsmodellierung, Security Reviews und Secure Coding Guidelines?

Bußgeldrisiko	Aufwand	Frist	ISO 27001:2022
bis 15 Mio. EUR	**10–20 PT**	**mittelfristig**	**5.8, 8.25, 8.26, 8.27 … (ISO 27001:2022)**

REMEDIATION: SECURE DEVELOPMENT LIFECYCLE (SDL) IMPLEMENTIEREN

1. Bedrohungsmodellierung (Threat Modeling) für alle neuen Features einführen
2. Secure Coding Guidelines erstellen und entwicklerverbindlich machen
3. Security-Code-Reviews als verpflichtenden Schritt im PR-Prozess verankern
4. SAST/DAST-Tools in CI/CD-Pipeline integrieren

📖 Cyber Resilience Act in der Praxis – Kap. 5 – Security by Design

AIACT-001-INVENTUR | EU AI Act · Art. 3 + Art. 26 | **SOFORT · Risiko: 8/9**

ANFORDERUNG

Betreiber müssen alle eingesetzten KI-Systeme kennen und dokumentieren – einschließlich SaaS-Dienste, APIs und Shadow AI (nicht genehmigter KI-Einsatz durch Mitarbeiter).

PRÜFFRAGE

Existiert ein vollständiges, aktuelles KI-Inventar das alle eingesetzten KI-Systeme erfasst – inkl. SaaS, APIs, eingebettete KI und Shadow AI?

Bußgeldrisiko	Aufwand	Frist	ISO 27001:2022
bis 35 Mio. EUR	**1–2 PT**	**sofort**	**5.10, 5.23, 5.9 (ISO 27001:2022)**

REMEDIATION: VOLLSTÄNDIGES KI-INVENTAR INKL. SHADOW AI AUFBAUEN

1. IT-Asset-Inventar nach KI-Funktionalitäten durchsuchen
2. Mitarbeiterbefragung zu genutzten KI-Tools (Copilot, ChatGPT, etc.)
3. SaaS-Verträge auf KI-Funktionalitäten prüfen
4. Shadow-AI-Richtlinie einführen und KI-Nutzungsrichtlinie kommunizieren
5. Quartalsweises Inventar-Update-Verfahren etablieren

📖 EU AI Act in der Praxis – Kap. 1 – Inventur, Shadow AI und Rollenrealität

DSGVO-005-GRUNDSAETZE | DSGVO · Art. 5 | **SOFORT · Risiko: 8/9**

ANFORDERUNG

Personenbezogene Daten müssen rechtmäßig, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Grundsätze: Zweckbindung, Datensparsamkeit, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit.

PRÜFFRAGE

Sind alle Verarbeitungstätigkeiten auf Rechtmäßigkeit, Zweckbindung und Datensparsamkeit geprüft und dokumentiert?

Bußgeldrisiko	Aufwand	Frist	ISO 27001:2022
bis 20 Mio. EUR	**hoch**	**mittelfristig**	**5.1, 5.12, 5.34 (ISO 27001:2022)**

REMEDIATION: VOLLSTÄNDIGEN COMPLIANCE-REVIEW ALLER VERARBEITUNGSTÄTIGKEITEN DURCHFÜHREN

1. Alle Verarbeitungstätigkeiten (VVT) inventarisieren und dokumentieren
2. Rechtsgrundlage nach Art. 6 je Verarbeitung prüfen und dokumentieren
3. Lösch- und Speicherbegrenzungskonzept je Datenkategorie erstellen
4. Jährlichen Datenschutz-Review-Zyklus etablieren

📖 DSGVO Praxishandbuch – Kap. 2 – Die Grundsätze des Art. 5

ISO27-005-ISMS | ISO 27001 · Kap. 4-6 (ISMS-Aufbau) | **HOCH · Risiko: 7/9**

ANFORDERUNG

Aufbau, Implementierung, Betrieb und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems (ISMS) entsprechend den Anforderungen der ISO/IEC 27001:2022.

PRÜFFRAGE

Ist ein formales ISMS nach ISO 27001 implementiert – mit dokumentiertem Scope, Risikobeurteilung, Statement of Applicability (SoA) und Leitungsbekenntnis?

Bußgeldrisiko	Aufwand	Frist	ISO 27001:2022
–	**hoch**	**langfristig**	**5.1, 5.2, 6.1 (ISO 27001:2022)**

REMEDIATION: VOLLSTÄNDIGES ISMS NACH ISO 27001:2022 AUFBAUEN

1. ISMS-Scope und Kontext der Organisation definieren
2. Risikobeurteilungsmethodik nach ISO 27001 Kap. 6.1.2 festlegen
3. Statement of Applicability (SoA) für alle 93 Annex-A-Controls erstellen
4. PDCA-Zyklus mit jährlichem Managementbewertungs- und internem Audit-Prozess einrichten
5. Zertifizierungsaudit mit akkreditiertem Zertifizierer planen

📖 ISO 27001 Praxisleitfaden – Kap. 2 – ISMS aufbauen: Schritt für Schritt

CSA-001-CERT-ANBINDUNG | Cyber Solidarity Act · Art. 15 + Art. 18 | **HOCH · Risiko: 7/9**

ANFORDERUNG

Teilnahme am EU-Cyber-Solidaritätsmechanismus durch Registrierung beim nationalen CERT (BSI) und Anbindung an das europäische CSIRT-Netzwerk. Ermöglicht Zugang zu EU-Solidaritätshilfe bei grenzüberschreitenden Angriffen.

PRÜFFRAGE

Ist die Organisation beim BSI-CERT und dem EU-CSIRT-Netzwerk registriert und können Vorfälle gemeldet und Solidaritätshilfe angefordert werden?

Bußgeldrisiko	Aufwand	Frist	ISO 27001:2022
bis 5 Mio. EUR	**mittel**	**kurzfristig**	**5.5, 5.24, 6.8 (ISO 27001:2022)**

REMEDIATION: CERT-REGISTRIERUNG UND EU-CSIRT-ANBINDUNG FÜR SOLIDARITÄTSMECHANISMUS EINRICHTEN

1. BSI-Registrierung prüfen und ggf. erneuern
2. EU-CSIRT-Netzwerk-Onboarding über nationale Behörde initiieren
3. Kommunikationskanäle und Kontaktdaten für CERT-Eskalation dokumentieren
4. Internes Eskalationshandbuch für CERT-Kommunikation erstellen
5. Jährlichen Test der CERT-Kommunikationskanäle durchführen

📖 Cyber Solidarity Act Praxisleitfaden – Kap. 3 – CERT-Anbindung und Solidaritätsmechanismus

4. Empfohlener Maßnahmenplan

#	Maßnahme	Framework	Aufwand	Frist	Priorität
1	Least-Privilege-IAM mit halbjährl. Access Review	NIS-2	10–20 PT	kurzfristig	**SOFORT**
2	SDL mit Threat Modeling & Secure Coding Guidelines	CRA	10–20 PT	mittelfristig	**HOCH**
3	Vollständiges KI-Inventar inkl. Shadow AI	EU AI Act	1–2 PT	sofort	**SOFORT**
4	Vollst. VVT mit Rechtsgrundlagen & Löschkonzept	DSGVO	hoch	mittelfristig	**SOFORT**
5	Vollständiges ISMS mit Scope, SoA, PDCA	ISO 27001	hoch	langfristig	**HOCH**
6	BSI-CERT-Registrierung + EU-CSIRT-Anbindung	Cyber Solidarity Act	mittel	kurzfristig	**HOCH**
Gesamt			**46–75 PT**	**6–9 Monate**	

5. Nächste Schritte – Sofortmaßnahmen

1. GF-Sitzung: Cybersicherheitsrichtlinie beschließen und Leitungsverantwortung formalisieren (NIS-2)

2. KI-Inventar starten: Alle eingesetzten KI-Systeme inkl. Shadow-AI erfassen (EU AI Act) – Quick-Win in 1–2 PT

3. DSGVO-Grundsätze-Dokumentation erstellen: VVT inventarisieren, Rechtsgrundlagen prüfen (DSGVO)

DORA: Nicht anwendbar für Industrieunternehmen – bei Scope-Änderung (Finanzdienstleistungen) erneut prüfen.

Ihr Abo enthält alle Ressourcen – BAM v4 mit 8 Frameworks

✓ Remediation-Anleitungen, editierbare Vorlagen und JSON/BAM-Export für alle 6 offenen Gaps

✓ Compliance-Dashboard mit Score-Verlauf und Echtzeit-Aktualisierung

✓ Cross-Controls: eine Maßnahme erfüllt gleichzeitig NIS-2, ISO 27001 und DSGVO

✓ Automatisch aktualisiert bei Regulierungsänderungen – kein manueller Aufwand

Executable Compliance.

Regulierung als System.

Compliance, die läuft.

Brain-Media.de ist Herausgeber des Brain-Media Audit Models (BAM) und Anbieter von Executable Compliance als integrierter Infrastruktur. Gegründet in Saarbrücken, entwickeln wir maschinenlesbare Compliance-Lösungen für Unternehmen, die regulatorische Anforderungen nicht nur erfüllen, sondern als strategischen Wettbewerbsvorteil nutzen möchten. BAM deckt alle relevanten EU-Compliance-Frameworks ab – von NIS-2 über den EU AI Act bis ISO 27001 – und wird kontinuierlich durch Experten aktualisiert.

Kontakt

Brain-Media.de

Dr. Holger Reibold

Hubert-Müller-Str. 52c

66113 Saarbrücken

info@brain-media.de

www.brain-media.de

+49 681 91005698