BM

Brain-Media.de
COMPLIANCE SOLUTIONS

Executable Compliance

Regulierung in eine integrierte, maschinenlesbare Compliance-Schicht übersetzen.

NIS-2 · CRA · CSA · DORA · DSGVO
EU AI Act · ISO 27001 · ISO 42001

WHITEPAPER

Version 2.0 · 2026
BAM v4 · 8 EU-Frameworks

DAS PROBLEM

The Compliance Gap

Regulatorische Anforderungen sind kein Wissensproblem. Sie sind ein Umsetzungsproblem. NIS-2, DORA, CRA, EU AI Act und DSGVO betreffen tausende Unternehmen – mit konkreten Fristen, Bußgeldern und Haftungsrisiken.

TYPISCHE VORGEHENSWEISE	WARUM SIE SCHEITERT
PDF-Stapel & Word-Dokumente	Unstrukturiert, nicht automatisierbar, kein einheitliches Datenmodell.
Externe Berater & Workshops	Teuer, zeitintensiv, kein nachhaltiges Wissen im Haus.
Manuelle Gap-Analysen	Fehleranfällig, subjektiv, nicht reproduzierbar.
Fragmentierte Tool-Landschaft	Inkonsistente Daten, hoher Pflegeaufwand, keine Single Source of Truth.

70% des gesamten Compliance-Aufwands entfällt auf manuelle Tätigkeiten – Abstimmungen, Dokumentation, Nacharbeit. Dieser Anteil lässt sich durch strukturierte Automatisierung erheblich reduzieren.

Das Ergebnis: Compliance bleibt ein Projekt, das nie fertig wird. **BAM überführt sie in dauerhaft laufende Infrastruktur.**

DIE LÖSUNG

From Regulation to Execution

BAM bricht jede regulatorische Anforderung in sechs operative Ebenen herunter. Maschinenlesbar. Einmal aufsetzen – alle Frameworks erfüllen.

	EBENE	WAS ES IST	IHR NUTZEN
01	**Requirement**	Regulatorische Anforderung – z. B. NIS-2 Art. 21 – priorisiert und strukturiert erfasst.	Wissen, was gilt
02	**Gap-Check**	Prüffrage zur Identifikation offener Lücken – nach Bußgeldrisiko priorisiert.	Wissen, wo Lücken sind
03	**Remediation**	Schritt-für-Schritt-Behebungsanleitung – direkt umsetzbar, keine Interpretation.	Wissen, wie beheben
04	**Risk**	Risikobewertung mit Likelihood & Impact – quantifiziert, nachvollziehbar dokumentiert.	Verstehen, was auf dem Spiel steht
05	**Control**	Konkrete Maßnahme mit Umsetzungshinweisen – cross-framework, einmal implementiert.	Wissen, was zu tun ist
06	**Evidence**	Nachweistyp mit editierbarem Template – auditfähig, sofort verwendbar.	Auditoren überzeugen

BAM ist kein Framework. BAM ist ausführbare Compliance-Infrastruktur – als **JSON, Markdown und SCORM** direkt nutzbar in GRC-Tools, KI-Systemen und automatisierten Workflows.

DAS PRINZIP

Collect Once.
Comply Many.

Eine einzige Maßnahme erfüllt gleichzeitig NIS-2, DORA, CRA, EU AI Act, DSGVO, ISO 27001, ISO 42001 und den Cyber Solidarity Act. BAM erkennt die Überlappung automatisch.

SCHRITT 1
Collect Once
Anforderungen, Kontrollen und Evidenzen einmal strukturiert erfassen.

→ SCHRITT 2
Einheitliches Datenmodell
BAM kartiert Überlappungen zwischen allen 8 Frameworks automatisch.

→ SCHRITT 3
Comply Many
Wiederverwendung in Frameworks, Prozessen und Nachweisen – ohne Mehraufwand.

WAS SICH VERÄNDERT	EFFEKT
Manueller Aufwand durch Cross-Controls	-60%
Datenkonsistenz über alle Frameworks	+80%
Geschwindigkeit bei neuen Frameworks	2-3×
Compliance-Kosten durch Effizienz	-30%

8 EU-Frameworks in einem einzigen Datenmodell. **Einmal erfassen. Überall compliant.** NIS-2, CRA, CSA, DORA, DSGVO, EU AI Act, ISO 27001, ISO 42001.

Single Source of Truth für alle Compliance-Daten. Konsistent. Skalierbar. Automatisch aktualisiert bei Regulierungsänderungen.

DIAGNOSE

Audit as a Service (AaaS)

AaaS zeigt, was fehlt – strukturiert, objektiv und priorisiert. Kein Login. Kein Berater. Ergebnis in unter 20 Minuten.

LEISTUNG	WAS SIE ERHALTEN
Quick Check	Kostenloser Compliance-Stresstest. Score für alle 8 Frameworks – ohne Registrierung.
Gap-Analyse	Vollständige Lückenliste nach Bußgeldrisiko priorisiert. Handlungsbedarf sofort erkennbar und quantifiziert.
Priorisierung	Welche Gaps sofort, welche mittelfristig – in Personentagen geschätzt, nach Risiko sortiert.
Pro-Report	Audit-ready Dokument mit Handlungsempfehlungen – direkt verwendbar für Geschäftsführung und Auditor.

20 min bis zum vollständigen Compliance-Score über alle 8 EU-Frameworks. Kostenlos. Ohne Login. Ohne Vorabinvestition. **Kein Berater braucht weniger Zeit für eine erste Einschätzung.**

Prüfung ist kein Ereignis. AaaS macht Audit-Readiness zum Dauerzustand – **nicht zur Vorbereitung.**

UMSETZUNG

Knowledge as a Service (KaaS)

KaaS liefert ausführbare Remediation-Logik zur Schließung identifizierter Gaps – kontinuierlich aktualisiert, direkt in GRC-Tools und KI-Systeme integrierbar.

KOMPONENTE	INHALT	FORMAT
Remediation	Schritt-für-Schritt-Anleitungen zur Umsetzung – priorisiert, umsetzbar, cross-framework.	Markdown · HTML
Controls	Konkrete Maßnahmen mit Umsetzungshinweisen – einmal implementiert, mehrfach wirksam.	JSON · BAM
Evidence-Templates	Editierbare Nachweisvorlagen – auditfähig, sofort verwendbar für alle 8 Frameworks.	DOCX · PDF
Export & API	Maschinenlesbare Rohdaten für GRC-Tools und KI-Agenten. RAG-fähig, keine Halluzinationen.	REST · SCORM

100+ Fachtitel hat Dr. Holger Reibold im Bereich IT-Sicherheit und Compliance veröffentlicht. Das BAM-Modell entstand aus realen Audit-Projekten – **nicht aus einem Lehrbuch.**

Zentrales Compliance-Wissen. Strukturiert. Aktuell. **Direkt aus dem System in Ihre Infrastruktur.**

TECHNISCHE ARCHITEKTUR

Der Execution Layer

BAM fungiert als Compliance Execution Layer zwischen Regulierung und Ihren operativen Systemen. Ein Datenmodell. End-to-End durch alle Compliance-Prozesse.

SCHICHT	FUNKTION	SCHNITTSTELLE
Regulierung	NIS-2, DORA, CRA, EU AI Act, DSGVO, ISO 27001, ISO 42001, CSA – kontinuierlich überwacht und validiert.	Gesetze · Normen
BAM Engine	Transformation in maschinenlesbare Objekte: Requirement → Risk → Control → Evidence. Kontinuierliche Expertenaktualisierung.	JSON · Markdown · SCORM
Integration Layer	API-First, Webhooks, Konnektoren für GRC, ITSM, SIEM, ERP. Sichere Übertragung via TLS 1.2+.	REST-API · Webhooks
Automation & AI	Smart Mapping, regelbasierte Automatisierung. RAG-fähige Daten für interne LLMs – validierte Fakten, keine Halluzinationen.	RAG · KI-Agenten
Compliance Output	Score, Gap-Analyse, Maßnahmenplan, Audit-Nachweise – in Echtzeit, automatisch aktualisiert.	Dashboard · Report

DE Serverstandorte Saarbrücken & Frankfurt. Dedizierte Instanz pro Kunde. Kein Multi-Tenant. **DSGVO-konform. VPN-Zugang. Verschlüsselt at rest.**

Compliance-Infrastruktur, die in Ihre Systeme hineinwächst.

VERGLEICH

Classical vs. Executable Compliance

Der Unterschied ist nicht technisch. Er ist strukturell.

KLASSISCHER ANSATZ	EXECUTABLE COMPLIANCE
Dokumente und Policies in Silos	Integrierte Struktur in einem System
Manuelle Umsetzung und Nachverfolgung	Automatisierte Workflows
Excel-Listen und E-Mail-Nachweise	Strukturierte Echtzeit-Evidenzen
Reaktiv auf Audits und Prüfungen	Proaktiv durch Monitoring
Hoher manueller Aufwand, Medienbrüche	End-to-End digital, durchgängig
Unklare Verantwortlichkeiten	Klare Rollen und Rechte
Schwer skalierbar, fehleranfällig	Skalierbar, konsistent, auditfest
Unsicherheit über Compliance-Status	Transparenz jederzeit

6–9 Monate bis zur Audit-Readiness im klassischen Ansatz – durch redundante Umsetzung, manuelle Abstimmung und fehlende Integration. **BAM reduziert diesen Zeitraum strukturell.**

Der Unterschied entsteht nicht durch bessere Werkzeuge. Er entsteht durch ein anderes Prinzip.

MUSTER-AUSWERTUNG · BEISPIELUNTERNEHMEN

BAM Compliance Report

Automatisiert generiert. Audit-ready. Das folgende Beispiel zeigt den Output für ein mittelständisches Industrieunternehmen mit 8 relevanten EU-Frameworks.

FRAMEWORK	SCORE	HANDLUNGSBEDARF	PRIORITÄT
NIS-2	61%	IAM und Governance-Dokumentation priorisieren	Hoch
CRA	74%	SDL-Prozess formalisieren und dokumentieren	Mittel
EU AI Act	55%	KI-Inventar inkl. Shadow AI sofort aufbauen	Sofort
DSGVO	48%	VVT und Grundsätze-Dokumentation fehlen	Sofort
ISO 27001	63%	ISMS-Aufbau nach 2022er Standard abschließen	Hoch
ISO 42001	40%	KI-Management-System strukturiert aufbauen	Hoch
CSA	70%	BSI-CERT-Registrierung und EU-CSIRT-Anbindung	Hoch
DORA	–	Nicht anwendbar – gilt ausschließlich für Finanzunternehmen	N/A

Gesamt-Score: **58% · Ziel: ≥ 80%.** Ihr Score in unter 20 Minuten – kostenlos auf brain-media.de.

MASSNAHMENPLAN

Remediation Plan

Priorisierte Maßnahmen zur Schließung kritischer Gaps – cross-framework, direkt aus dem KaaS-Abo umsetzbar.

	MASSNAHME	AUFWAND	FRIST	FRAMEWORK
1	**Incident Response Process aufbauen**	12–20 PT	Sofort	NIS-2 · ISO 27001
2	**KI-Inventar inkl. Shadow AI aufbauen**	1–2 PT	Sofort	EU AI Act
3	**VVT mit Rechtsgrundlagen erstellen**	hoch	Mittelfristig	DSGVO
4	**Third-Party Risk Management etablieren**	10–16 PT	Mittelfristig	DORA · ISO 27001
5	**ISMS nach ISO 27001:2022 aufbauen**	hoch	Langfristig	ISO 27001
6	**BSI-CERT-Registrierung einrichten**	mittel	Kurzfristig	CSA

46–75 PT Gesamtaufwand über alle 6 Maßnahmen. 6–9 Monate bis zur vollständigen Audit-Readiness. **Eine Maßnahme erfüllt dabei mehrere Frameworks gleichzeitig.**

Redundanz ist kein Aufwand mehr. Sie ist ein Effizienzhebel.

BUSINESS CASE

Compliance als Wettbewerbsvorteil

Executable Compliance schafft messbaren Mehrwert jenseits regulatorischer Pflichterfüllung – in fünf Dimensionen gleichzeitig.

DIMENSION	WAS SICH STRUKTURELL VERÄNDERT	WIRKUNG
Marktposition	Wer Anforderungen jederzeit nachweisen kann, gewinnt Ausschreibungen schneller und besteht Due-Diligence-Prüfungen ohne Vorbereitung.	Vertriebsvorteil
Operational Excellence	Automatisierte Kontrollprozesse eliminieren Medienbrüche. Compliance-konforme Entscheidungen werden in Echtzeit getroffen.	Effizienzgewinn
Sales-Beschleunigung	Kürzere Due-Diligence-Zeiten, schnelleres Kunden-Onboarding, weniger Rückfragen im Vergabeverfahren.	Umsatzwirkung
KI-Enabling	BAM-Daten im JSON/Markdown-Format sind nativ RAG-fähig. Compliance-Infrastruktur wird zur validierten KI-Datenbasis.	KI-Grundlage
Haftungsminimierung	Lückenlose Audit-Trails und Echtzeit-Dokumentation reduzieren das persönliche Haftungsrisiko der Geschäftsführung nachweisbar.	GF-Absicherung

seit 2003 entwickelt und publiziert Dr. Holger Reibold im Bereich IT-Sicherheit und Compliance. Das BAM-Modell entstand aus realen Audit-Projekten. **100+ Fachtitel. 8 EU-Frameworks.**

Compliance, die als System implementiert ist, schafft in allen fünf Dimensionen gleichzeitig Wert – ohne Mehraufwand.

BM

Brain-Media.de

COMPLIANCE SOLUTIONS

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.

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.**

01 - ASSESS

Quick Check

Kostenloser Stresstest. Score in unter 20 Minuten. Kein Login.

02 - ANALYZE

Gap-Report

Priorisierte Lücken, Bußgeldrisiken, Handlungsempfehlungen.

03 - EXECUTE

KaaS

Anleitungen, Templates, JSON/BAM-Export, kontinuierliche Updates.

brain-media.de

Dr. Holger Reibold · Hubert-Müller-Str. 52c · 66113 Saarbrücken

info@brain-media.de · +49 681 91005698

GitHub: BrainMediaDe/brain-media-audit-model