					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P33					Dokumenttitel: **– Richtlinie zur Audit- und Compliance-Überwachung**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 9.2, 9.3, 10	
ISO/IEC 27002:2022	Maßnahmen 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
EU-DSGVO	Artikel 24, 32, 33	
EU NIS2	Artikel 21(2)(g), 27	
EU DORA	Artikel 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Zweck

1.1 Zweck dieser Richtlinie ist es, das Audit- und Compliance-Überwachungsprogramm der Organisation festzulegen und zu steuern, um:

1.1.1 die Wirksamkeit von Sicherheits- und Datenschutzkontrollen zu validieren,

1.1.2 die Konformität mit anwendbaren Standards, gesetzlichen Anforderungen und vertraglichen Verpflichtungen sicherzustellen,

1.1.3 Nichtkonformitäten, Ineffizienzen und Compliance-Risiken frühzeitig zu erkennen,

1.1.4 die kontinuierliche Verbesserung sowie die Bereitschaft für Zertifizierungen, Assessments und regulatorische Prüfungen zu unterstützen.

1.2 Diese Richtlinie stärkt die Integrität und den Reifegrad des Informationssicherheitsmanagementsystems (ISMS), indem sie strukturierte, risikoorientierte und nachweisgestützte Audit- und Überwachungspraktiken verankert.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle internen Geschäftsbereiche, Funktionen und Abteilungen,

2.1.2 physische Standorte, Cloud-Umgebungen, SaaS-Plattformen und ausgelagerte Dienstleistungen,

2.1.3 Informationssysteme, Anwendungen, Infrastrukturen und Datenbestände, die durch das ISMS geregelt werden,

2.1.4 Mitarbeitende, Auftragnehmer sowie Dritte mit Audit- oder Compliance-Verpflichtungen.

2.2 Diese Richtlinie umfasst:

2.2.1 interne Audits,

2.2.2 externe Audits/Zertifizierungsaudits,

2.2.3 die technische Compliance-Überwachung,

2.2.4 Lieferanten- und Drittaudits,

2.2.5 Korrektur- und Vorbeugemaßnahmen (CAPA),

2.2.6 Kennzahlen, Dashboards und Berichtsprozesse.

2.3 Sie gilt für alle relevanten Rahmenwerke, denen die Organisation unterliegt, einschließlich ISO/IEC 27001, DSGVO, NIS2, DORA und SOC 2.

3. Ziele

3.1 Die Angemessenheit und Wirksamkeit der implementierten Kontrollen, Richtlinien und Verfahren im gesamten ISMS und in den zugehörigen Umgebungen zu überprüfen.

3.2 Mängel, Nichtkonformitäten oder Compliance-Lücken zu identifizieren und zu beheben, bevor sie zu Sicherheitsvorfällen oder Verstößen eskalieren.

3.3 Eine dauerhafte Bereitschaft für interne Governance-Überprüfungen, externe Audits und unabhängige Zertifizierungen sicherzustellen.

3.4 Belastbare Nachweise und Prüfpfade zur Unterstützung regulatorischer Anfragen, rechtlicher Verfahren oder von Kunden angeforderter Nachweise bereitzustellen.

3.5 Auditergebnisse in das übergreifende Risikomanagement, die Sicherheitskennzahlen und die kontinuierliche Verbesserung der Organisation zu integrieren.

4. Rollen und Verantwortlichkeiten

4.1 Leitung Interne Revision / Compliance Manager

4.1.1 Plant, terminiert und führt interne Audits auf Basis der Risikopriorität durch.

4.1.2 Pflegt das Audit-Repository, koordiniert Auditaktivitäten und verfolgt Korrekturmaßnahmen nach.

4.2 Chief Information Security Officer (CISO)

4.2.1 Stellt sicher, dass der Audit-Geltungsbereich alle relevanten ISMS-Elemente und Maßnahmen aus Anhang A umfasst.

4.2.2 Überwacht die Verifizierung von CAPA und integriert Auditergebnisse in das Sicherheitsprogramm.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1 Diese Richtlinie muss mindestens jährlich durch den Compliance Manager und den CISO überprüft werden oder früher als Reaktion auf:

9.1.1 Änderungen regulatorischer, vertraglicher oder zertifizierungsbezogener Rahmenwerke,

9.1.2 wesentliche Audit-Feststellungen oder wiederholte Kontrollausfälle,

9.1.3 organisatorische Umstrukturierungen oder Änderungen am GRC-System,

9.1.4 Empfehlungen externer Auditoren oder Rückmeldungen von Aufsichtsbehörden.

9.2 Im Rahmen der Überprüfung ist Folgendes zu bewerten:

9.2.1 Methodik und Häufigkeit der Auditplanung,

9.2.2 Änderungen des ISMS-Geltungsbereichs oder der Infrastruktur,

9.2.3 Aktualisierungen des Kontrollkatalogs oder des Rechtsregisters,

9.2.4 Konsistenz und Qualität von Auditnachweisen und CAPA-Prozessen.

9.3 Alle Änderungen an dieser Richtlinie müssen:

9.3.1 in einem versionskontrollierten Repository dokumentiert werden,

9.3.2 durch die Geschäftsleitung genehmigt werden,

9.3.3 an sämtliches betroffenes Personal kommuniziert und in aktualisierte Verfahren sowie Sensibilisierungsprogramme integriert werden.

9.4 Die Validierung nach der Überprüfung muss bestätigen, dass aktualisierte Anforderungen im Audit-Repository, in Werkzeugen zur Compliance-Überwachung und in internen Monitoring-Dashboards berücksichtigt sind.

10. Verknüpfte Richtlinien und Bezüge

10.1 Diese Richtlinie ist mit den folgenden zugehörigen Organisationsrichtlinien abgestimmt:

10.1.1 P1 – Informationssicherheitsrichtlinie: Definiert das ISMS und legt die Rechenschaftspflicht für Einhaltung und kontinuierliche Verbesserung fest.

10.1.2 P5 – Änderungsmanagement-Richtlinie: Stellt sicher, dass Änderungen an Infrastruktur und Konfigurationen mit Auswirkungen auf Kontrollumgebungen für Audits transparent sind.

10.1.3 P6 – Risikomanagement-Richtlinie: Integriert Auditergebnisse in die unternehmensweite Risikobewertung und Risikobehandlung.

10.1.4 P14 – Richtlinie zur Datenaufbewahrung und Entsorgung: Regelt die Aufbewahrung von Auditnachweisen, Protokollen und Compliance-Aufzeichnungen.

10.1.5 P18 – Richtlinie zu kryptografischen Kontrollen: Unterstützt die sichere Speicherung und Übertragung sensibler Auditdaten.

10.1.6 P26 – Richtlinie zur Lieferanten- und Drittparteiensicherheit: Umfasst Auditrechte, Nachweisdokumentation und die Überwachung der Compliance von Lieferanten.

10.1.7 P30 – Incident-Response-Richtlinie (P30): Richtet Audits von Verfahren zum Umgang mit Informationssicherheitsvorfällen an den Sicherstellungszielen des ISMS aus.

10.1.8 P32 – Richtlinie zur Aufrechterhaltung des Geschäftsbetriebs und Disaster Recovery: Verlangt die Verifizierung von Kontinuitätstests und der Einhaltung des DRP während der Auditzyklen.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an globalen Standards und rechtlichen Anforderungen für Audits und die kontinuierliche Validierung der Compliance ausgerichtet.

11.2 ISO/IEC 27001:

11.2.1 Klausel 9.2 – Internes Audit: Verlangt regelmäßige, risikobasierte Audits des ISMS zur Bewertung von Wirksamkeit und Konformität.

11.2.2 Klausel 9.3 – Managementbewertung: Auditergebnisse müssen in die strategische Überprüfung und Verbesserung einfließen.

11.2.3 Klausel 10.1 – Nichtkonformität und Korrekturmaßnahme: Audit-Feststellungen müssen durch dokumentierte CAPA-Verfahren behandelt werden.

11.3 ISO/IEC 27002:2022 – Maßnahmen 5.35–5.37:

11.3.1 Maßnahmen aus Anhang A 5.35–5.37: Umfassen unabhängige Überprüfung, Einhaltung rechtlicher und vertraglicher Anforderungen sowie Audit-Protokollierung.

11.3.2 Geben Umsetzungshinweise für die Planung, Durchführung und Verbesserung von Audit- und Compliance-Programmen.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Kontrollbewertungen: Verlangt die regelmäßige Überprüfung implementierter Sicherheitskontrollen.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): Unterstützt die Nachverfolgung und Behebung von Audit-Feststellungen.

11.4.3 CA-7 – Kontinuierliche Überwachung: Unterstützt proaktive, automatisierte Compliance-Bewertungen.

11.5 EU-DSGVO (2016/679):

11.5.1 Artikel 24 und 32: Fordern Nachweise über die Implementierung und Wirksamkeit von Sicherheitskontrollen durch geeignete Governance-Strukturen.

11.5.2 Artikel 33: Unterstützt die Notwendigkeit validierter Prüfpfade bei der Reaktion auf Datenschutzverletzungen und Meldungen.

11.6 EU-NIS2-Richtlinie (2022/2555):

11.6.1 Artikel 21(2)(g): Verlangt die Auditierung von Richtlinien und Verfahren als Teil der Mindestmaßnahmen für das Management von Cybersicherheitsrisiken.

11.6.2 Artikel 27: Nationale Behörden können Audits für wesentliche und wichtige Einrichtungen durchführen oder verlangen.

11.7 EU DORA (2022/2554):

11.7.1 Artikel 10(2)(e): Unternehmen müssen interne und externe Audits der Verfahren zum Management von IKT-Risiken durchführen.

11.7.2 Artikel 25 – Audit-Anforderungen: Verlangt regelmäßige Audits durch interne oder unabhängige externe Auditoren mit regulatorischer Einsichtsmöglichkeit.

11.8 COBIT 2019:

11.8.1 MEA01 – Überwachen, Evaluieren und Beurteilen von Leistung und Konformität: Stellt sicher, dass die Kontrollwirksamkeit verifiziert und an Governance-Gremien berichtet wird.

11.8.2 MEA03 – Überwachen, Evaluieren und Beurteilen der Einhaltung: Verlangt die Ausrichtung organisatorischer Praktiken an rechtlichen, vertraglichen und normenbasierten Anforderungen.