A-1200 Wien, Dresdner Straße 45
E-Mail: kundenservice@forum-media.at

Interner Auditbericht zur Umsetzung des NISG 2026

1. Titel und Zusammenfassung

Berichtstitel: Interner Auditbericht zur Umsetzung der NIS-2-Richtlinie und des NISG 2026

Erstellungsdatum: … [Datum]

Auditzeitraum: … [Startdatum] bis … [Enddatum]

Auditteam: … [Namen der Auditoren, zB Compliance-Manager, IT-Sicherheitsbeauftragter]

Zusammenfassung:

Dieser Bericht dokumentiert die Ergebnisse des internen Audits, das die Umsetzung der Maßnahmen zur Einhaltung der NIS-2-Richtlinie und des NISG 2026 überprüft hat. Das Audit bewertet die Effektivität der implementierten Sicherheitsmaßnahmen, die Einhaltung gesetzlicher Vorgaben und identifiziert Bereiche, die verbessert werden müssen. Insgesamt wurden 10 Maßnahmen überprüft, von denen 7 vollständig implementiert und 3 mit Verbesserungspotenzial identifiziert wurden.

2. Auditziele

- Überprüfung der vollständigen und wirksamen Umsetzung der Maßnahmen gemäß der NIS-2-Richtlinie
- Sicherstellung der Einhaltung der Anforderungen des NISG 2026
- Identifikation von Schwachstellen oder Lücken in der Implementierung
- Bereitstellung eines Maßnahmenplans zur Behebung erkannter Defizite

3. Auditumfang

- Geprüfte Bereiche:
  - Technische Sicherheitsmaßnahmen (MFA, IDPS, Patch-Management, Netzwerksegmentierung)
  - Organisatorische Maßnahmen (Notfallpläne, Vorfallsmanagement, Schulungen für Mitarbeitende und Governance)
  - Lieferkettenmanagement (Verträge und Bewertung)
  - Dokumentation, Selbstdeklaration und Berichterstattung
- Methodik:
  - Interviews mit Schlüsselrollen (zB IT-Administrator, Compliance-Manager)
  - Prüfung der Dokumentation (zB Sicherheitsrichtlinien, Auditprotokolle)
  - Stichprobenbasierte Überprüfung von Systemen und Prozessen

4. Auditbewertung (Ergebnisse)

4.1 Technische Sicherheitsmaßnahmen

Maßnahme	Erfüllung	Auditbewertung	Empfohlene Maßnahmen
Mehrfaktor-Authentifizierung (MFA) für kritische Systeme	Vollständig	MFA wurde für ERP, VPN und E-Mail-Systeme implementiert; keine Schwächen erkannt	Keine weiteren Maßnahmen erforderlich
Patch-Management-System	Teilweise	Patch-Management wurde technisch implementiert, jedoch fehlt ein regelmäßiger Prüfplan	Einführung eines quartalsweisen Prüfplans
Intrusion Detection and Prevention System (IDPS)	Vollständig	IDPS arbeitet zuverlässig und meldet Anomalien	Regelmäßige Testläufe zur Effektivität
Netzwerksegmentierung	Teilweise	Segmentierung abgeschlossen, jedoch fehlt die Dokumentation der internen Netzwerkarchitektur	Erstellung einer vollständigen Dokumentation

4.2 Organisatorische Maßnahmen

Maßnahme	Erfüllung	Auditbewertung	Empfohlene Maßnahmen
Notfallpläne	Vollständig	Notfallpläne sind erstellt und getestet; Simulationen wurden erfolgreich durchgeführt	Weitere jährliche Simulationen einplanen
Vorfallsmanagement	Vollständig	Meldesystem wurde eingerichtet und erfolgreich getestet; Prozesse für 24-Stunden Frühwarnung, 72-Stunden-Meldung und Abschlussbericht sind dokumentiert	Regelmäßige Mitarbeiterschulungen zu Meldeprozessen
Governance- und Mitarbeiterschulungen	Teilweise	Erste Schulungen wurden durchgeführt, jedoch fehlt ein vollständiger Zyklus für Leitungsorgane, Mitarbeitende und Feedbackauswertung	Feedback analysieren, Managementschulungen terminieren und Nachschulungen organisieren

4.3 Lieferkettenmanagement

Maßnahme	Erfüllung	Auditbewertung	Empfohlene Maßnahmen
Überarbeitung der Lieferantenverträge	Teilweise	75 % der Verträge wurden überarbeitet, Rest steht aus	Abschluss der Überarbeitung bis … [Datum]
Lieferantenbewertungssystem	Nicht begonnen	Bewertungssystem ist noch in der Planungsphase	Implementierung bis … [Datum]

4.4 Dokumentation und Berichterstattung

Maßnahme	Erfüllung	Auditbewertung	Empfohlene Maßnahmen
Zentrale Dokumentation und Selbstdeklaration	Teilweise	Dokumentation der Maßnahmen und der Nachweisunterlagen ist unvollständig	Vervollständigung inklusive Registerdaten und Selbstdeklaration bis … [Datum]

5. Identifizierte Schwachstellen

- Patch-Management: fehlender Prüfplan gefährdet langfristige Aktualität der Systeme
- Netzwerksegmentierung: unvollständige Dokumentation der Netzwerkarchitektur
- Mitarbeiterschulungen: Schulungsfeedback wurde nicht ausgewertet und Nachschulungen fehlen
- Lieferkettenmanagement: noch nicht abgeschlossene Überarbeitung der Lieferantenverträge und fehlendes Bewertungssystem
- Dokumentation: Maßnahmen sind nicht vollständig dokumentiert, was die Nachvollziehbarkeit erschwert

6. Verbesserungsmaßnahmen

Schwachstelle	Empfohlene Maßnahme	Verantwortlich	Frist
Fehlender Patch-Management-Prüfplan	Einführung eines regelmäßigen Prüfplans für Patch-Management	IT-Sicherheitsbeauftragter	… [Datum]
Unvollständige Netzwerkdokumentation	Erstellung einer vollständigen Dokumentation der Netzwerksegmentierung	IT-Administrator	… [Datum]
Schulungsfeedback fehlt	Auswertung des Schulungsfeedbacks und Organisation von Nachschulungen	Schulungskoordinator	… [Datum]
Unvollständige Lieferantenverträge	Abschluss der ausstehenden Vertragsüberarbeitungen	Lieferkettenmanager	… [Datum]
Fehlendes Lieferantenbewertungssystem	Implementierung eines Bewertungssystems zur Überprüfung der Lieferantensicherheit	Lieferkettenmanager	… [Datum]
Unvollständige Maßnahmen-Dokumentation	Vervollständigung der zentralen Dokumentation aller Sicherheitsmaßnahmen	Compliance-Manager	… [Datum]

7. Genehmigung

Name	Position	Datum	Unterschrift
… [Auditteamleiter]	Compliance-Manager	… [Datum]	
… [Projektleiter]	Projektleitung	… [Datum]	
… [Geschäftsleitung]	Geschäftsführung	… [Datum]	