PROFESSIONAL RESOURCES

NIS2 Governance. Auf einen Blick.

Von der gesetzlichen Anforderung zur steuerbaren Umsetzung und belastbaren Nachweisführung.

301	69	10	6
abgeleitete Anforderungen	Toolkit-Dokumente	Handlungsfelder	Umsetzungssäulen

HANDLUNGSFELD	MANAGEMENTAUFTRAG	GOVERNANCE- UND UMSETZUNGSOBJEKTE	OPERATIVER REGELKREIS	NACHWEISE UND STEUERUNG
01 Governance & Geschäftsleitung §§ 30, 38 BSIG	Pflichten billigen, Verantwortlichkeiten festlegen, Umsetzung überwachen und regelmäßig entscheiden.	Governance-Richtlinie; Rollen- und Eskalationsstandard; Beschluss- und Management-Review-Verfahren.	Auftrag → Entscheidung → Freigabe → Überwachung → Management Review	Beschlüsse, Freigaben, Protokolle, Statusberichte, Eskalationen
02 Risiko & Verhältnismäßigkeit § 30 Abs. 1-2 BSIG	Geltungsbereich, Risiken und angemessene Maßnahmen risikobasiert festlegen; Restrisiken entscheiden.	Risikomanagementrichtlinie; Bewertungsstandard; Behandlungsverfahren; Risiko- und Maßnahmenregister.	Identifizieren → bewerten → behandeln → verfolgen → neu bewerten	Risikoregister, Maßnahmenplan, Verhältnismäßigkeit, Restrisikofreigaben
03 Vorfälle & gesetzliche Meldungen § 30 Abs. 2 Nr. 2, § 32 BSIG	Erkennung, Klassifizierung, Behandlung, Wiederherstellung und gesetzliche Meldefristen beherrschbar machen.	Incident-Verfahren; Meldeverfahren und Vorlagen; Vorfall-, Melde- und Lessons-Learned-Register.	Erkennen → einstufen → eindämmen → melden → wiederherstellen → lernen	Zeitlinie, Entscheidungen, Meldungen, Abschlussbericht, Verbesserungsmaßnahmen
04 BCM, Krise & Datensicherung § 30 Abs. 2 Nr. 3 BSIG	Kritische Leistungen, Wiederanlaufziele, Krisenorganisation und belastbare Wiederherstellung festlegen.	BIA-/BCM-/DR-Konzept; Notfall- und Krisenplan; Testverfahren; Backup- und Restore-Register.	BIA → planen → sichern → üben → wiederherstellen → verbessern	BIA, Testprotokolle, Restore-Nachweise, Kontaktreviews, Korrekturen
05 Lieferkette & Dienstleister § 30 Abs. 2 Nr. 4 BSIG	Abhängigkeiten erkennen, Lieferanten klassifizieren, Anforderungen vertraglich sichern und überwachen.	Due-Diligence- und Monitoringverfahren; Vertragsklauseln; Lieferanten- und Abhängigkeitsregister.	Klassifizieren → prüfen → vereinbaren → überwachen → eskalieren / beenden	Risikoprüfungen, Verträge, Leistungsnachweise, Audits, Offboarding-Belege
06 Assets, Identitäten & Personal § 30 Abs. 2 Nr. 9 BSIG	Assets und Eigentümer kennen; Zugriffe minimieren; privilegierte Rechte und kritische Rollen kontrollieren.	Asset- und Zugriffsstandards; Rezertifizierungs- und JML-Verfahren; Inventare und Berechtigungsregister.	Inventarisieren → zuordnen → berechtigen → prüfen → entziehen	Inventare, Genehmigungen, Reviews, Privilegiennachweise, Austrittsbestätigungen
07 Beschaffung, Änderung & Schwachstellen § 30 Abs. 2 Nr. 5 BSIG	Sicherheit vor Erwerb und Änderung verbindlich prüfen; Schwachstellen priorisiert bis zum Abschluss steuern.	Entwicklungs- und Änderungsstandard; Abnahmeverfahren; Release-, Konfigurations- und Schwachstellenregister.	Anfordern → prüfen → ändern / freigeben → erkennen → priorisieren → beheben	Sicherheitsanforderungen, Abnahmen, Changes, Triage und Behebungsnachweise
08 Technischer Schutz & Monitoring § 30 Abs. 1-2 BSIG	Mindeststandards, Ausnahmen und Wirksamkeit für Netz, Endgeräte, Protokollierung, Kryptographie und MFA steuern.	Netz-/Endpoint-Standards; Loggingverfahren; Kryptographie- und Schlüsselstandard; MFA- und Kommunikationsstandard.	Härten → authentifizieren → verschlüsseln → überwachen → reagieren	Regelreviews, Konfigurationsprüfungen, Logreviews, Schlüssel- und MFA-Nachweise
09 Schulung, Wirksamkeit & Verbesserung § 30 Abs. 2 Nr. 6-7 BSIG	Kompetenz aufbauen, Maßnahmen regelmäßig prüfen und erkannte Unwirksamkeiten verbindlich korrigieren.	Schulungsverfahren; Wirksamkeits- und Kennzahlenstandard; Auditverfahren; Feststellungsregister.	Schulen → messen → prüfen → feststellen → korrigieren → berichten	Teilnahmen, Kennzahlen, Prüfungen, Korrekturen, Managementberichte
10 Registrierung, Behörden & Nachweise §§ 33-35, 39 BSIG	Registrierung, Erreichbarkeit, behördliche Kommunikation sowie besondere KRITIS-Pflichten sicherstellen.	Registrierungsakten; Behördenverfahren; Dokumenten- und Nachweisregister; bedingte KRITIS-Unterlagen.	Registrieren → erreichbar sein → übermitteln → beantworten → beheben → archivieren	Bestätigungen, Behördenakte, Nachweispakete, Mängel- und Abschlussbelege

DURCHGÄNGIGE GOVERNANCE-ARCHITEKTUR

Anforderungen und Maßnahmen bleiben wechselseitig bis zu Rechtsbezug, Umsetzung und Wirksamkeitsnachweis zuordenbar.

Rechtsbezug — Verantwortung — Dokument — Prozess — Nachweis — Wirksamkeit

Einordnung

Die Map dient der allgemeinen Orientierung. Anwendbarkeit, Angemessenheit und Wirksamkeit sind organisationsspezifisch zu prüfen. Sie ersetzt keine Rechtsberatung, Prüfung oder Konformitätsbestätigung.

Vollständige Umsetzungsarchitektur

cyberlligency.com/resources/nis2-governance-map/

NIS2 Governance Toolkit