NIS2-Checkliste

sosafe

Zweck:

Arbeits- und Nachweisgrundlage für eine prüfbare NIS2-Umsetzung.

Organisation:

Standort/Scope:

Verantwortlich:

Version/Datum:

Anwendung

Markieren Sie pro Punkt den Fortschritt. Nutzen Sie dafür die Spalten **Offen**, **In Arbeit**, **Umgesetzt** und **Geprüft**.

Nachweise: Legen Sie pro Punkt mindestens ein prüfbares Artefakt ab (Policy, Prozessbeschreibung, Protokoll, Report, Ticket-Nachweis).

A) Governance & Verantwortlichkeiten

sosafe

Nr.	Checklistenpunkt	Mindestanforderung	Typische Nachweise/ Artefakte	Offen	In Arbeit	Umgesetzt	Geprüft	Owner	Zieltermin
1	Scope & Verantwortlichkeiten festlegen	Rollen, Geltungsbereich, Reporting und Eskalation dokumentieren	RACI, Scope-Dokument, Eskalationsmatrix						
2	Risikoanalyse durchführen	Methode, Bewertung, Priorisierung und Ausnahmen festlegen	Risiko-Register, Bewertungsmethodik, Management-Freigaben						
3	Sicherheitsrichtlinien etablieren	Policies definieren, freigeben und regelmäßig überprüfen	Policy-Set, Review-Protokolle, Versionshistorie						

B) Awareness & Human Risk Management

Nr.	Checklistenpunkt	Mindestanforderung	Typische Nachweise/ Artefakte	Offen	In Arbeit	Umgesetzt	Geprüft	Owner	Zieltermin
4	Schulungsprogramme umsetzen	Trainings für Leitungsorgane und Mitarbeitende planen und durchführen	Trainingsplan, Teilnahme- und Ergebnisausweise						
5	Awareness wirksam steuern	Wirksamkeit messen, verbessern und berichten	Phishing-Reports, KPIs, Management-Reporting						

C) Technische Maßnahmen & Basisschutz

sosafe

Nr.	Checklistenpunkt	Mindestanforderung	Typische Nachweise/ Artefakte	Offen	In Arbeit	Umgesetzt	Geprüft	Owner	Zieltermin
6	Asset-Inventar pflegen	Systeme, Dienste und Schutzbedarf dokumentieren	Asset-Liste, Schutzbedarfsbewertung						
7	Zugriffskontrollen umsetzen	Rollen, Rechte und JML-Prozesse definieren	IAM-Konzept, Rezertifizierungen						
8	Starke Authentifizierung einsetzen	MFA für kritische Systeme und Admin-Zugänge	MFA-Rollout, Konfigurationsnachweise						
9	Schwachstellen managen	Erkennen, priorisieren und beheben	Scan-Reports, Patch-Protokolle						
10	Verschlüsselung einsetzen	Daten und Kommunikation angemessen schützen	Kryptorichtlinie, Key-Management						

D) Vorfälle & Meldewege

sosafe

Nr.	Checklistenpunkt	Mindestanforderung	Typische Nachweise/ Artefakte	Offen	In Arbeit	Umgesetzt	Geprüft	Owner	Zieltermin
11	Incident-Response etablieren	Prozesse, Rollen und Übungen definieren	IR-Plan, Übungsprotokolle						
12	Meldepflichten umsetzen	Fristen, Freigaben und Dokumentation regeln	Melde-Runbook, Vorfall-Timeline						

E) Resilienz & Wirksamkeitsnachweise

Nr.	Checklistenpunkt	Mindestanforderung	Typische Nachweise/ Artefakte	Offen	In Arbeit	Umgesetzt	Geprüft	Owner	Zieltermin
13	Backup & Wiederherstellung	Backup-Strategie testen und dokumentieren	Restore-Tests, Protokolle						
14	Business Continuity sicherstellen	BCM- und DR-Pläne pflegen und üben	BCM-Dokumente, Übungsberichte						
15	Wirksamkeit prüfen	Audits und Tests durchführen	Auditberichte, Maßnahmen-Tracking						

F) Lieferkette & Dienstleistersteuerung

sosafe

Nr.	Checklistenpunkt	Mindestanforderung	Typische Nachweise/ Artefakte	Offen	In Arbeit	Umgesetzt	Geprüft	Owner	Zieltermin
16	Lieferantenrisiken steuern	Kritische Dienstleister identifizieren und bewerten	Supplier-Register, Risikoanalysen						
17	Anforderungen vertraglich regeln	Sicherheitsanforderungen festschreiben	Verträge, Auditklauseln						
18	Secure SDLC absichern	Sichere Beschaffung, Entwicklung und Wartung	Nachweise, Ausnahmeprozesse