NIS2 - KRITIS

CHECKLISTE

Dokumentinformationen	
Organisation	
Verantwortlich	
Prüfzeitraum	
Version	
BSI-Registrierung	

1 Inhaltsverzeichnis

2 Governance & Organisatorische Anforderungen

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Benennung eines CISO / IT-Sicherheitsbeauftragten** Formale Benennung mit ausreichender Qualifikation und Befugnissen. Stellvertreterregelung vorhanden.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**Haftungsübernahme durch Geschäftsführung / Vorstand** Schulungsnachweis der Leitungsebene zu Cybersicherheitspflichten. Protokoll regelmäßiger Lageberichte.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Sicherheitsorganisation mit RACI-Matrix** Organigramm der IS-Organisation, RACI für sicherheitsrelevante Prozesse, Vertretungsregelungen definiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
4	**ISMS nach ISO 27001 oder BSI IT-Grundschutz implementiert** Gültiges Zertifikat oder dokumentierter Umsetzungsstand. Scope-Dokument. Letztes Audit dokumentiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
5	**Informationssicherheitsleitlinie (IS-Policy) aktuell** Policy max. 2 Jahre alt, von Leitungsebene freigegeben, kommuniziert, Quittierung aller MA vorhanden.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

3 Risikomanagement

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Anwendbare Normen und Rechtsgrundlagen identifiziert** ISO/IEC 27005, BSI IT-Grundschutz 200-3, NIS2 Art. 21, KRITIS-DachG §23 als verbindliche Grundlagen dokumentiert und im ISMS verankert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**Normenkonformität regelmäßig überprüft** Abgleich mit aktuellen BSI-Empfehlungen und ENISA-Guidelines. Änderungen an Normen werden nachverfolgt und umgesetzt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Risikomanagement-Rahmenwerk schriftlich definiert** Scope, Ziele, Rollen, Methodik und Verantwortlichkeiten des RM-Rahmenwerks sind dokumentiert und von der Leitungsebene freigegeben.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
4	**Risikodefinition und Bewertungskriterien festgelegt** Einheitliche Definition von Risiko, Schadensklassen, Eintrittswahrscheinlichkeiten und Risikoschwellen organisationsweit verbindlich festgelegt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
5	**Risikomanagementprozess vollständig implementiert** Prozess umfasst alle Phasen: Kontextfestlegung → Risikoidentifikation → Risikobeurteilung → Risikobehandlung → Überwachung → Kommunikation.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
6	**Prozessverantwortliche und Zyklen definiert** Risikoeigner je Risiko benannt. Prozesszyklen (jährlich/anlassbezogen) festgelegt und eingehalten.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
7	**Organisationskontext vollständig erfasst** Interne und externe Einflussfaktoren analysiert (Stakeholder, regulatorisches Umfeld, Sektor, Abhängigkeiten). Schutzbedarfsfeststellung für alle Assets durchgeführt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
8	**Systemgrenzen und Schnittstellen dokumentiert** Kritische Systeme, Prozesse und deren Abhängigkeiten (intern/extern) vollständig erfasst und aktuell gehalten.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

9	**Risikoidentifikation strukturiert und vollständig** Alle relevanten Bedrohungen und Schwachstellen systematisch identifiziert (Threat Intelligence, Audits, Pen-Tests, BSI-Lageberichte).	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
10	**Risikoanalyse und -bewertung dokumentiert** Bewertung nach Eintrittswahrscheinlichkeit × Schadensauswirkung. Risikomatrix angewandt. Alle Risiken im Risikoregister erfasst und priorisiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
11	**Risikobehandlungsoptionen je Risiko festgelegt** Für jedes Risiko: Behandlungsoption (Vermeiden / Vermindern / Übertragen / Akzeptieren) dokumentiert, begründet und genehmigt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
12	**Vollständiger Risikobehandlungsplan** Maßnahmen, Termine und Verantwortliche Konkrete Maßnahmen, Fälligkeit, Budget und Umsetzungsstatus je Risiko. Eskalationsverfahren bei Terminüberschreitung definiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
13	**Kontinuierliche Überwachung der Risiken und Maßnahmen** KPIs für Risikoüberwachung definiert. Regelmäßiges Reporting an die Leitungsebene. Abweichungen werden zeitnah eskaliert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
14	**Risiken bei wesentlichen Änderungen neu bewertet** Change-Management-Prozess löst automatische Risikoneubewertung aus (neue Systeme, Lieferanten, Prozesse, Vorfälle).	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
15	**Risikoregister vollständig, aktuell und revisionssicher** Alle Risiken mit Status, Historie und Behandlungsnachweis dokumentiert. Zugriffsschutz und Versionierung sichergestellt. Aufbewahrungsfristen eingehalten.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
16	**Dokumentation prüfungsreif aufbereitet** Risikoberichte für BSI-Prüfung / §8a-Nachweis vorbereitet. Auditpfad lückenlos nachvollziehbar.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

4 Drittdienstleister & Lieferkettensicherheit

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Anwendbare Normen für Lieferkettensicherheit identifiziert** ISO/IEC 27036, BSI C5, KRITIS-DachG §24, NIS2 Art. 21(2)(d) als verbindliche Grundlagen dokumentiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**Drittdienstleister vollständig definiert und abgegrenzt** Klare Definition welche Lieferanten, Subunternehmer und Partner als „Drittdienstleister" im Sinne von NIS2/KRITIS gelten. Abgrenzung zu internen Einheiten dokumentiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Vollständiges Lieferantenregister mit Kritikalitätseinstufung** Alle Drittdienstleister erfasst. Klassifizierung nach Kritikalität (kritisch / wesentlich / Standard) auf Basis des Schutzbedarfs der erbrachten Leistung. Mind. jährliche Überprüfung.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
4	**Abhängigkeiten und Lieferketten vollständig kartiert** Alle relevanten Lieferketten inkl. Sub-Subunternehmer erfasst. Konzentrationsrisiken (Single Points of Failure) identifiziert und bewertet.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
5	**Informationsflüsse und Datenweitergabe an Dritte dokumentiert** Welche Daten (inkl. Klassifizierung) werden an welche Drittdienstleister weitergegeben? Datenschutz-AVV und Vertraulichkeitsvereinbarungen vorhanden.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
6	**Konzentrationsrisiken bewertet und Alternativlieferanten geprüft** Multi-Sourcing-Strategie oder Contingency-Plan für kritische Lieferanten vorhanden.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
7	**Sicherheitsanforderungen vertraglich verankert** Mindestanforderungen in allen Verträgen mit kritischen Lieferanten: Sicherheitsnachweise (ISO 27001/TISAX/BSI C5), Auditrechte, Incident-Meldepflichten (24h), Unterauftragnehmerpflichten, Exit-Klauseln.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
8	**Regelmäßige Sicherheits-Assessments kritischer Lieferanten** Dokumentierter Assessment-Prozess (Fragebogen, Audit, Zertifikatsprüfung).	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen	

	Eskalationsprozess bei Nicht-Erfüllung. Nachverfolgung offener Findings.		☐ N/A	
9	**Prozess für Sicherheitsvorfälle bei Lieferanten definiert** Eskalationswege und Kommunikationsprotokoll festgelegt. IRP berücksichtigt Lieferantenvorfälle. Isolierungsmaßnahmen dokumentiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
10	**Onboarding- und Offboarding-Prozess für Drittdienstleister** Sicherheitsprüfung vor Vertragsschluss (Due Diligence). Geordneter Offboarding-Prozess inkl. Datenlöschung, Zugriffsentzug und Wissenstransfer.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
11	**Sicherheitsanforderungen vertraglich verankert** Mindestanforderungen in allen Verträgen mit kritischen Lieferanten: Sicherheitsnachweise (ISO 27001/TISAX/BSI C5), Auditrechte, Incident-Meldepflichten (24h), Unterauftragnehmerpflichten, Exit-Klauseln.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
12	**Regelmäßige Sicherheits-Assessments kritischer Lieferanten** Dokumentierter Assessment-Prozess (Fragebogen, Audit, Zertifikatsprüfung). Eskalationsprozess bei Nicht-Erfüllung. Nachverfolgung offener Findings.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
13	**Prozess für Sicherheitsvorfälle bei Lieferanten definiert** Eskalationswege und Kommunikationsprotokoll festgelegt. IRP berücksichtigt Lieferantenvorfälle. Isolierungsmaßnahmen dokumentiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
14	**Onboarding- und Offboarding-Prozess für Drittdienstleister** Sicherheitsprüfung vor Vertragsschluss (Due Diligence). Geordneter Offboarding-Prozess inkl. Datenlöschung, Zugriffsentzug und Wissenstransfer.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

4.1 Lieferkettensicherheit: PDCA-Zyklus

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Plan: Anforderungen und Ziele für Lieferantensicherheit definiert** Sicherheitsziele, Mindeststandards und Bewertungskriterien für alle Lieferantenkategorien festgelegt und dokumentiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**Do: Maßnahmen implementiert und Lieferanten bewertet** Vertragsklauseln umgesetzt, Assessments durchgeführt, Monitoring aktiv. Schulungen für lieferantenbezogene Prozesse durchgeführt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Check: Wirksamkeit der Lieferantensicherheit überprüft** KPIs definiert (z.B. Anteil compliant gebundener Lieferanten, offene Findings, Vorfallsquote). Regelmäßiges Reporting.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
4	**Act: Verbesserungsmaßnahmen eingeleitet** Lessons Learned aus Vorfällen und Audits fließen in die Vertragsgestaltung und den Assessmentprozess zurück. Kontinuierliche Verbesserung nachweisbar.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

5 Business Continuity Management (BCM)

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Business Impact Analyse (BIA) aktuell und vollständig** BIA für alle kritischen Geschäftsprozesse. MTPD, RTO und RPO definiert und abgestimmt. BIA max. 2 Jahre alt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**Business Continuity Pläne (BCP) für kritische Prozesse** Detaillierte BCPs mit Handlungsanweisungen, Verantwortlichen, Ressourcen und Aktivierungskriterien. Mind. jährl. Review.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Disaster Recovery Plan (DRP) inkl. Backup-Strategie** DRP mit Wiederherstellungsreihenfolge, RTO/RPO je System. Backup-Konzept (3-2-1-Regel), Offsite, regelmäßige Restore-Tests.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
4	**Regelmäßige BCM-Tests und Übungen mit Dokumentation** Mind. jährliche Übungen (Tabletop, Simulation, Volltest). Übungsberichte mit Findings und Lessons Learned.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
5	**Notfallkommunikationsplan mit aktuellen Kontaktlisten** Kontaktlisten (intern/extern, Lieferanten, Behörden, BSI) aktuell. Out-of-band-Kommunikation möglich.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

6 Incident Management

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Anwendbare Normen für Incident Management identifiziert** ISO/IEC 27035, BSI IT-Grundschutz DER.2.1, NIS2 Art. 23, KRITIS-DachG §35 als verbindliche Grundlagen dokumentiert und im ISMS verankert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**„Erheblicher Vorfall" im Sinne von NIS2 Art. 23** definiert Klare, dokumentierte Kriterien wann ein Sicherheitsvorfall als „erheblich" gilt (Auswirkung auf Dienstverfügbarkeit, Datenverlust, betroffene Personen, finanzielle Schäden). Klassifizierungsschema vorhanden.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Abgrenzung Incident / Event / Problem dokumentiert** Eindeutige Definitionen und Abgrenzungen vorhanden. Triage-Prozess für eingehende Meldungen definiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
4	**Klassifizierungsschema vorhanden** Klar definierte und dokumentierte Kriterien wann ein Sicherheitsvorfall als „erheblich" gilt (Auswirkung auf Dienstverfügbarkeit, Datenverlust, betroffene Personen, finanzielle Schäden).	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
5	**Abgrenzung Incident / Event / Problem dokumentiert** Eindeutige Definitionen und Abgrenzungen vorhanden. Triage-Prozess für eingehende Meldungen definiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
6	**Threat Intelligence als Input genutzt** BSI-Warnmeldungen systematisch ausgewertet und in die Incident-Erkennung eingespeist.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

6.1 Incident Prozess

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Phase 1 Vorbereitung: IRP dokumentiert und erprobt** Incident-Response-Plan mit Eskalationsstufen, Rollen (Incident Commander, Kommunikator, Techniker), Playbooks für Hauptszenarien (Ransomware, DDoS, Datenleck, Insider). Regelmäßige Übungen.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**Phase 2 Erkennung & Analyse: Triage-Prozess definiert** Strukturierte Erstbewertung (Klassifizierung, Schweregrad, betroffene Systeme). Beweissicherung ab erster Minute. Eskalationsentscheidung dokumentiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Phase 3 Eindämmung: Isolierungsmaßnahmen vordefiniert** Playbooks für Sofortmaßnahmen (Netzwerktrennung, Account-Sperrung, Backup-Aktivierung) vorhanden und erprobt. Entscheidungskompetenzen klar geregelt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
4	**Phase 4 Beseitigung & Wiederherstellung: DRP verzahnt** Disaster Recovery Plan greift nahtlos. Wiederherstellungsreihenfolge dokumentiert. Rückkehr zum Normalbetrieb nachvollziehbar protokolliert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
5	**Phase 5 Meldepflichten: NIS2 3-Stufen-Meldung umgesetzt** Frühwarnung, Detailbericht, Abschlussbericht nach vollständiger Untersuchung. Templates vorhanden, Verantwortlicher benannt, BSI-Kontakt hinterlegt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
6	**Phase 6 Nachbereitung: Lessons Learned dokumentiert** Root Cause Analysis nach jedem erheblichen Vorfall. Findings in Risikoregister und IRP überführt. Reporting an Leitungsebene. Maßnahmen nachverfolgt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

7 Technische Sicherheitsmaßnahmen

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Multi-Faktor-Authentifizierung (MFA) für privilegierte Zugriffe** MFA für Admin-Konten, Remote-Zugriff, Cloud-Dienste erzwungen. Ausnahmen dokumentiert und genehmigt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**Privileged Access Management (PAM) implementiert** PAM-Lösung für Admin-Konten. Least-Privilege-Prinzip. Just-in-Time-Zugänge. Session-Recording. Regelmäßiger Access Review.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Netzwerksegmentierung kritischer Systeme / OT-IT-Trennung** Kritische Systeme in separaten Segmenten. OT/IT-Netztrennung. Firewall-Regelwerke dokumentiert und regelmäßig reviewed.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
4	**Vulnerability Management & Patch-Prozess mit definierten SLAs** Regelmäßige Scans (mind. monatlich). Patch-SLAs: Kritisch ≤7d, hoch ≤30d, Mittel ≤90d. Kompensationsmaßnahmen dokumentiert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
5	**Verschlüsselung sensibler Daten (at rest & in transit)** Datenverschlüsselung at rest und in transit (TLS 1.2+). Schlüsselmanagement dokumentiert. Krypto-Verfahren aktuell (BSI TR-02102).	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	

8 Registrierung, Compliance & Nachweisführung

Nr.-	Prüfpunkt & Beschreibung	Nachweis / Fundstelle	Status	Bemerkung
1	**Registrierung beim BSI als KRITIS-Betreiber / NIS2-Einrichtung** Organisation beim BSI registriert. Bestätigung vorhanden. SPOC (Single Point of Contact) benannt und hinterlegt.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
2	**Nachweise §8a BSIG / NIS2-Compliance-Bericht vorbereitet** Compliance-Nachweise für 2-Jahres-Prüfung zusammengestellt. Qualifizierter Prüfer identifiziert.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	
3	**Awareness-Schulungen für alle Mitarbeiter und Rollen** Jährliche Pflicht-Schulungen (alle MA). Rollenspezifische Schulungen (IT, Management, BCM-Team). Phishing-Simulationen.	[Dokument / Datum / Ansprechpartner]	☐ erfüllt ☐ Teilw. ☐ offen ☐ N/A	