NIS2 checklist for Sections 30 and 32 BSIG

Note
One row per requirement. Enter the status (open / partly / met / not applicable), your evidence, the owner and a due date. Check first whether and at which tier your company falls under NIS2, for example with the free applicability check on complass.eu.

Section 30 (2) BSIG: minimum risk management measures

(a) / no. 1 – Risk analysis and security policies

No.	Requirement	What an audit wants to see	Status	Evidence / note
1	Information security policy approved Art. 21(2)(a) NIS2; Section 30(2) no. 1 BSIG	Policy signed by senior management with objectives, scope and responsibilities; communicated to all employees.		
2	IT and OT asset inventory Art. 21(2)(a) NIS2; Section 30(2) no. 1 BSIG	Processes, systems, OT components, cloud services and service providers recorded with owners; maintenance process defined.		
3	Risk methodology and risk analysis Art. 21(2)(a) NIS2; Section 30(2) no. 1 BSIG	Documented methodology with criteria and acceptance threshold; all-hazards scenarios including physical hazards; updated at least annually.		
4	Risk treatment and risk acceptance Art. 21(2)(a) NIS2; Section 30(2) no. 1 BSIG	Every risk has a treatment decision; residual risks above the threshold are accepted by senior management for a limited period.		
5	Policy framework with document control Art. 21(2)(a) NIS2; Section 30(2) no. 1 BSIG	Topic policies for all minimum measures with version, approval and review interval.		
6	Network segmentation and zone concept Art. 21(2)(a) NIS2; Section 30(2) no. 1 BSIG	Separation of IT, OT, DMZ and guest networks; transitions via controlled firewalls; for OT, e.g. zones and conduits under IEC 62443-3-2.		
7	Network map and firewall rule set Art. 21(2)(a) and (e) NIS2; Section 30(2) nos. 1 and 5 BSIG; Implementing Regulation (EU) 2024/2690, Annex point 6.7	Up-to-date network map for IT, OT and the cloud; only justified connections between zones, services not needed blocked; firewall rules reviewed regularly and after incidents; separate management network.		
8	Remote and service provider access controlled and time-limited Art. 21(2)(a) and (e) NIS2; Section 30(2) nos. 1 and 5 BSIG; Implementing Regulation (EU) 2024/2690, Annex point 6.7.2(d), (g), (h)	All paths from outside recorded (including remote maintenance boxes on machines); approval only on request and for a limited time; central access point with MFA and session logging; approved devices only.		

(b) / no. 2 – Incident handling

No.	Requirement	What an audit wants to see	Status	Evidence / note
9	Incident response process documented Art. 21(2)(b) NIS2; Section 30(2) no. 2 BSIG	Phases, roles, severity levels, escalation to senior management; 24/7 availability regulated.		
10	Logging and detection Art. 21(2)(b) NIS2; Section 30(2) no. 2 BSIG	Central log collection, monitoring (SIEM/MDR), EDR on endpoints; OT network monitoring. Operators of critical facilities: attack detection under Section 31(2) BSIG.		
11	Playbooks for core scenarios Art. 21(2)(b) NIS2; Section 30(2) no. 2 BSIG	Ransomware, compromised account, phishing, attack via remote maintenance/OT, data exfiltration – with OT-specific decisions on shutting down plant.		
12	External support agreed Art. 21(2)(b) NIS2; Section 30(2) no. 2 BSIG	Framework contract with an IR provider, cyber insurance contact details, forensics where needed; call-off route documented.		
13	Reporting process under Section 32 BSIG Art. 21(2)(b) NIS2; Section 30(2) no. 2 BSIG	Criteria for significance, deadlines of 24 h / 72 h / 1 month, templates, access to the BSI portal even during an IT outage.		
14	Follow-up and lessons learned Art. 21(2)(b) NIS2; Section 30(2) no. 2 BSIG	Root cause analysis after every relevant incident; measures feed into the action plan.		
15	Logging concept: sources, retention, time and alerts Art. 21(2)(b) NIS2; Section 30(2) no. 2 BSIG; Implementing Regulation (EU) 2024/2690, Annex point 3.2	Logging concept with a list of log sources (IT, OT, cloud), event types under Annex point 3.2.3 of the Implementing Regulation, retention and integrity protection, time synchronization, alert rules with response times; for operators of critical facilities attack detection systems (Section 31(2) BSIG).		
16	Operate attack detection systems (operators of critical facilities) Section 31(2) BSIG; Section 39(1) BSIG	Mandatory item for operators of critical facilities only: the systems collect and evaluate parameters from ongoing operation continuously and automatically. Assess the degree of implementation according to the BSI guidance and record it for the proof under section 39 BSIG. Recommended for essential entities without a critical facility, not required for important entities.		

(c) / no. 3 – Business continuity, backup and crisis management

No.	Requirement	What an audit wants to see	Status	Evidence / note
17	Business impact analysis Art. 21(2)(c) NIS2; Section 30(2) no. 3 BSIG	RTO/RPO for critical processes determined and agreed with process owners.		
18	Emergency and recovery plans Art. 21(2)(c) NIS2; Section 30(2) no. 3 BSIG	Emergency operation and recovery sequence for each critical process, including production plant.		
19	Backup with offline or immutable copy Art. 21(2)(c) NIS2; Section 30(2) no. 3 BSIG	3-2-1 rule, separate administration with MFA, backup of OT projects and configurations.		

No.	Requirement	What an audit wants to see	Status	Evidence / note
20	Regular restore tests Art. 21(2)(c) NIS2; Section 30(2) no. 3 BSIG	Logged restore tests with measured duration compared with the RTO.		
21	Crisis team and crisis communication Art. 21(2)(c) NIS2; Section 30(2) no. 3 BSIG	Composition, alerting, crisis room independent of IT, communication templates.		
22	Crisis and emergency exercises Art. 21(2)(c) NIS2; Section 30(2) no. 3 BSIG	At least annually, with senior management taking part; evaluation documented.		
23	Redundancy and verified integrity of backups (including OT) Art. 21(2)(c) NIS2; Section 30(2) no. 3 BSIG; Implementing Regulation (EU) 2024/2690, Annex point 4.2	At least partial redundancy of systems, sites, staff and communication according to the BIA; complete backups including configuration and cloud data with regular integrity checks; backup and comparison of OT project states and images.		
24	Utilities and protection against environmental threats (UPS, air conditioning, fire, water) Art. 21(2)(c) NIS2; Section 30(2) no. 3 BSIG; Implementing Regulation (EU) 2024/2690, Annex points 13.1 and 13.2	Protection of server rooms, network distribution rooms and control rooms against failure of power, air conditioning and telecommunications, against fire and water; limits, monitoring with alerts, emergency supply contracts, regular tests.		

(d) / no. 4 – Supply chain security

No.	Requirement	What an audit wants to see	Status	Evidence / note
25	Supplier inventory Art. 21(2)(d) NIS2 Directive; § 30(2) no. 4 BSIG	All suppliers and service providers with access to systems/data or critical deliveries recorded.		
26	Criticality rating Art. 21(2)(d) NIS2 Directive; § 30(2) no. 4 BSIG	Classification by access, dependency and replaceability; taking into account specific vulnerabilities and the security practices of suppliers (Art. 21(3) NIS2).		
27	Security requirements and contract clauses Art. 21(2)(d) NIS2 Directive; § 30(2) no. 4 BSIG	Graded minimum requirements, duty to report incidents, right to audit, provisions on subcontractors and patch supply.		
28	Controlled service provider access Art. 21(2)(d) NIS2 Directive; § 30(2) no. 4 BSIG	Remote maintenance only via a central gateway with a personal account, MFA, approval and logging.		
29	Ongoing supplier monitoring Art. 21(2)(d) NIS2 Directive; § 30(2) no. 4 BSIG	Regular reassessment of critical suppliers, monitoring of certificate expiry and incidents, exit strategy.		

(e) / no. 5 – Security in acquisition, development and maintenance; vulnerability management

No.	Requirement	What an audit wants to see	Status	Evidence / note
30	Security requirements in procurement Art. 21(2)(e) NIS2; Section 30(2) no. 5 BSIG	Requirements catalog for IT and OT procurement (e.g. MFA capability, logging, support period, hardening, IEC 62443-4-2 for components).		
31	Secure development Art. 21(2)(e) NIS2; Section 30(2) no. 5 BSIG	Policy for in-house software and control programs: reviews, environment separation, dependency checks, secrets management.		
32	Change and configuration management Art. 21(2)(e) NIS2; Section 30(2) no. 5 BSIG	Changes with risk assessment, testing, approval and a rollback plan; hardening standards for systems.		
33	Vulnerability management with deadlines Art. 21(2)(e) NIS2; Section 30(2) no. 5 BSIG	Sources (vendors, CERT-Bund, ICS advisories), assessment by criticality and exposure, defined remediation deadlines.		
34	Compensation for systems that cannot be patched Art. 21(2)(e) NIS2; Section 30(2) no. 5 BSIG	List of EoL and unpatchable OT systems with documented compensating measures.		
35	Vulnerability disclosure Art. 21(2)(e) NIS2; Section 30(2) no. 5 BSIG	Published contact channel (e.g. security.txt) and a procedure for coordinated vulnerability disclosure.		
36	Hardening, secure configuration and protection against malware Art. 21(2)(e) NIS2; Section 30(2) no. 5 BSIG; Implementing Regulation (EU) 2024/2690, Annex points 6.3 and 6.9	Hardening baselines per system type (CIS, BSI or vendor, protection levels for PLCs), applied on installation, regular comparison of target and actual state; EDR or application allowlisting against malware and unauthorized software.		

(f) / no. 6 – Assessment of effectiveness

No.	Requirement	What an audit wants to see	Status	Evidence / note
37	Measurement concept and metrics Art. 21(2)(f) NIS2; Section 30(2) no. 6 BSIG	Eight to twelve metrics with targets, owners and measurement interval.		
38	Technical testing Art. 21(2)(f) NIS2; Section 30(2) no. 6 BSIG	Vulnerability scans, penetration tests (coordinated for OT), configuration reviews.		
39	Internal audits Art. 21(2)(f) NIS2; Section 30(2) no. 6 BSIG	Annual risk-based audit of the minimum measures by independent auditors.		
40	Reporting to senior management Art. 21(2)(f) NIS2; Section 30(2) no. 6 BSIG	Regular reports on metrics, audit results and progress on measures.		
41	Management review and corrective actions Art. 21(2)(f) NIS2; Section 30(2) no. 6 BSIG	Annual review with resolutions; deviations lead to measures in the action plan.		

(g) / no. 7 – Cyber hygiene and training

No.	Requirement	What an audit wants to see	Status	Evidence / note
42	Baseline cyber hygiene rules implemented Art. 21(2)(g) NIS2; Section 30(2) no. 7 BSIG	Patching, changing default passwords, no local admin rights, email and endpoint protection, removable media rules.		
43	Basic training for all employees Art. 21(2)(g) NIS2; Section 30(2) no. 7 BSIG	Mandatory at onboarding and annually; including external personnel with system access.		
44	Target group training Art. 21(2)(g) NIS2; Section 30(2) no. 7 BSIG	Admins, OT staff, procurement, HR, accounting/assistants with specific content.		
45	Senior management training Art. 21(2)(g) NIS2; Section 30(2) no. 7 BSIG	Regular participation by all members under Section 38(3) BSIG, with evidence.		
46	Awareness and simulations Art. 21(2)(g) NIS2; Section 30(2) no. 7 BSIG	Phishing simulations and campaigns; measure impact via reporting and click rates.		

(h) / no. 8 – Cryptography and encryption

No.	Requirement	What an audit wants to see	Status	Evidence / note
47	Cryptography policy Art. 21(2)(h) NIS2; Section 30(2) no. 8 BSIG	Areas of use, permitted methods (guided by BSI TR-02102), responsibilities, exception process.		
48	Encryption of data in transit Art. 21(2)(h) NIS2; Section 30(2) no. 8 BSIG	TLS 1.2+/1.3 for web services and interfaces, encrypted VPN and remote maintenance connections, email transport encryption.		
49	Encryption of data at rest Art. 21(2)(h) NIS2; Section 30(2) no. 8 BSIG	Disk encryption on mobile devices, encrypted backups and cloud storage with secure key custody.		
50	Key and certificate management Art. 21(2)(h) NIS2; Section 30(2) no. 8 BSIG	Certificate inventory, expiry monitoring, secure key storage, rotation and revocation.		
51	Replacement of outdated methods Art. 21(2)(h) NIS2; Section 30(2) no. 8 BSIG	SSL, TLS 1.0/1.1, SHA-1 and weak cipher suites identified and replaced, or compensated for with justification (especially in OT).		

(i) / no. 9 – Personnel security, access control and asset management

No.	Requirement	What an audit wants to see	Status	Evidence / note
52	Security in the HR process Art. 21(2)(i) NIS2; Section 30(2) no. 9 BSIG	Screening before hiring for sensitive roles, confidentiality undertaking, regulated leaving with return of items and removal of access.		

No.	Requirement	What an audit wants to see	Status	Evidence / note
53	Access control concept and role model Art. 21(2)(i) NIS2; Section 30(2) no. 9 BSIG	Least privilege, role-based rights, request and approval process.		
54	Privileged Accounts Art. 21(2)(i) NIS2; Section 30(2) no. 9 BSIG	Separate admin accounts, tiering/PAM, sealed emergency accounts, recertification every six months.		
55	Joiner-mover-leaver process Art. 21(2)(i) NIS2; Section 30(2) no. 9 BSIG	Automated link to the HR system; service provider accounts limited in time.		
56	Physical Access Control Art. 21(2)(i) NIS2; Section 30(2) no. 9 BSIG	Access to server rooms, control rooms, control cabinets and network distribution points regulated and logged.		
57	Asset management as an ongoing process Art. 21(2)(i) NIS2; Section 30(2) no. 9 BSIG	Onboarding, classification, owners, lifecycle and secure decommissioning of ICT systems and products.		
58	Complete inventory with classification and software inventory Art. 21(2)(i) NIS2; Section 30(2) no. 9 BSIG; Implementing Regulation (EU) 2024/2690, Annex points 12.1 and 12.4	Services and supporting systems, mandatory data per asset (including version, zone, owners, end of support), classification levels, software inventory with SBOM for critical products, traceable changes.		
59	Secure erasure, disposal, removable media and return Art. 21(2)(i) NIS2; Section 30(2) no. 9 BSIG; Implementing Regulation (EU) 2024/2690, Annex points 12.2, 12.3 and 12.5	Verifiable erasure or destruction before disposal and repair (including OT memory cards), rules for removable media, return or blocking of devices when someone leaves.		

(j) / no. 10 – MFA, secured communication and emergency communication

No.	Requirement	What an audit wants to see	Status	Evidence / note
60	MFA for remote access Art. 21(2)(j) NIS2; Section 30(2) no. 10 BSIG	VPN, remote desktop, remote maintenance portals – including service provider access into OT (MFA at the gateway/jump server).		
61	MFA for cloud, email and privileged accounts Art. 21(2)(j) NIS2; Section 30(2) no. 10 BSIG	Prefer phishing-resistant methods (FIDO2, smart card); disable legacy sign-in.		
62	MFA for all users Art. 21(2)(j) NIS2; Section 30(2) no. 10 BSIG	Full-coverage MFA or continuous authentication with documented exceptions.		
63	Secured voice, video and text communication Art. 21(2)(j) NIS2; Section 30(2) no. 10 BSIG	Approved tools with encryption and regulated administration; rules for private messengers.		
64	Emergency communication system Art. 21(2)(j) NIS2; Section 30(2) no. 10 BSIG	Out-of-band channel for the crisis team, independent of corporate IT, tested regularly.		

Section 32 BSIG: reporting duties for significant security incidents

Assessing significance: when is an incident reportable?

No.	Requirement	What an audit wants to see	Status	Evidence / note
65	Company-specific criteria for significant incidents are defined Section 2 BSIG; Art. 23(3) NIS2			
66	Responsibility for assessment and the reporting decision (including deputies, 24/7) is regulated § 32(1) BSIG			
67	The time of becoming aware is documented in the incident log § 32(1) BSIG			
68	“Not reportable” assessments are documented with reasons § 30(1) BSIG (German BSI Act)			
69	The status of clarifications has been checked and documented: ordinance under Section 56(4) BSIG (not issued so far), Implementing Regulation (EU) 2024/2690 Art. 3–14 (where the type of entity is covered) and current BSI guidance on the reporting obligation Section 2 no. 11 BSIG; Section 56(4) BSIG; Art. 3–14 Implementing Regulation (EU) 2024/2690			

Implementing reporting deadlines and content

No.	Requirement	What an audit wants to see	Status	Evidence / note
70	A reporting plan with the stages 24 h / 72 h / intermediate report / one month is documented Section 32(1) BSIG; Art. 23(4) NIS2			
71	Reporting templates contain all mandatory content for each reporting stage § 32(1) BSIG			

No.	Requirement	What an audit wants to see	Status	Evidence / note
72	A procedure for progress reports on ongoing incidents is described Section 32(2) BSIG			
73	Operators of critical facilities: additional details on the critical facility are included in the template Section 32(3) BSIG			
74	Parallel reporting obligations (GDPR, insurance, customers) are linked in the plan Art. 33 GDPR; Section 35 BSIG			
75	Access to the BSI portal is possible even if your own IT has failed § 32(1) BSIG			

Informing service recipients and reporting exercises

No.	Requirement	What an audit wants to see	Status	Evidence / note
76	Communication templates and an approval process for service recipients are available Section 35 BSIG; Art. 23(1) NIS2			
77	Duties to inform under customer contracts are recorded § 30(2), no. 4 BSIG (German BSI Act)			
78	A reporting exercise has been carried out and the time to the early warning measured Section 32(1) BSIG; Section 30(2) no. 6 BSIG			
79	Findings from exercises and incidents are carried over into the action plan § 30(2), no. 6 BSIG (German BSI Act)			

About this template

Template version 1.0-1f588a0c
Content as of 12 November 2026
Published by Made with Complass, https://complass.eu

Legal basis (as of): BSIG 2025 (gesetze-im-internet.de, Stand: zuletzt geändert durch Art. 8 G v. 22.10.2026 I Nr. 318), KRITISDachG (BGBl. 2026 I Nr. 66, in Kraft seit 17.3.2026), BSI-KritisV (Stand: G v. 15.5.2026 I Nr. 148), DVO (EU) 2024/2690 (EUR-Lex), BSI-Infopaket NIS-2-Meldepflicht und BSI-FAQ zu NIS-2

This template is not legal advice. It does not replace checking which requirements apply to your company and does not guarantee any audit or certification result.

License: Creative Commons Attribution 4.0 International (CC BY 4.0). You may use, change and pass on the template, also commercially, as long as you name the source. Attribution: "Template: Complass (complass.eu), CC BY 4.0". https://creativecommons.org/licenses/by/4.0/deed.en