

NIS2 & Hardware Maintenance

— *what auditors check.*

Maintenance contracts under the NIS2 Directive: which of the ten mandatory measures in Art. 21 reach into hardware operations, what evidence auditors ask for — and how to document SLAs, supply chain and accountability in the contract so they hold up in an audit.

10

mandatory measures in Art. 21
— four reach hardware directly

~30,000

German entities in scope of
NIS2 (BSIG, in force since Dec
2025)

24h / 72h

early warning / incident
notification — the partner must
feed in

Contents

01	Management Summary
02	NIS2 in ten minutes: who, what, from when
03	Why hardware maintenance is a NIS2 topic
04	The ten measures of Art. 21 — and their hardware relevance
05	What auditors check: the audit matrix
06	Supply chain security: the maintenance provider as supplier
07	SLA requirements under NIS2: availability is a security objective
08	Firmware, patches, vulnerabilities: OPS.1.1.3 and EOSL hardware
09	The 24h / 72h / 1-month reporting cascade: what the maintenance partner must deliver
10	Media, spare parts, access: the physical controls
11	Documented accountability: § 38 BSIG and management
12	The maintenance contract in the audit: 12-point clause checklist
13	Conclusion
14	About TechCare & sources

Highlighted chapters contain the working aids: the audit matrix (ch. 5), the SLA building blocks (ch. 7) and the 12-point clause checklist (ch. 12).

Management Summary

The central thesis of this whitepaper: **under NIS2, hardware maintenance is no longer a procurement topic — it is an audit item.** Anyone operating servers, storage and network equipment that falls within the directive's scope must be able to show an auditor that these systems are kept available, that their vulnerabilities are handled, that they are maintained through a secured supply chain — and that management approves and oversees exactly that.

The reason lies in the directive's structure. Art. 21 of Directive (EU) 2022/2555 requires in-scope entities to implement a minimum set of ten technical and organisational measures [1]. At least four of them reach directly into hardware operations: business continuity and backup (point c), supply chain security including relationships with service providers (point d), security in the acquisition, development *and maintenance* of systems including vulnerability handling (point e), and access control and asset management (point i). Germany transposed this catalogue into § 30 BSIG with the NIS2 Implementation Act in December 2025; roughly 30,000 companies across 18 sectors are affected [3][4].

For the maintenance contract, this shifts the yardstick. Until now, an SLA was judged on response time and price. Under NIS2 it must additionally answer three questions an auditor will ask:

- **Availability as a security objective:** Is the restoration time of critical systems contractually guaranteed, backed by spare-parts stocking and evidenced in reports (Art. 21(2)(c))?
- **The service provider as supply chain:** Has the maintenance partner been assessed as a supplier — certifications, subcontractors, origin of spare parts, personnel and access rules (points d, i)?
- **Vulnerabilities and end of support:** Is it documented how firmware is patched, which systems run beyond vendor support, and which compensating controls management has accepted for them (point e, § 38 BSIG)?

Add to this the reporting cascade: early warning within 24 hours, incident notification within 72 hours, final report within one month [1][3]. Those deadlines can only be met if inventory, patch status and the maintenance partner's contacts are documented *before* the incident. A maintenance contract that does not regulate participation in reporting becomes an open flank in the audit.

What this means for operators

This whitepaper translates the directive into checkable items. Chapter 4 maps the ten measures to hardware operations. Chapter 5 provides the audit matrix — ten audit fields with the evidence auditors typically request. Chapters 6 to 10 go deeper into supply chain, SLA, vulnerabilities, reporting and physical controls. Chapter 11 covers management's responsibility under § 38 BSIG; Chapter 12 condenses everything into a 12-point clause checklist for the maintenance contract.

KEY TAKEAWAY

NIS2 turns the maintenance contract into an evidence document. Whoever documents SLA, supply chain, patch process and accountability cleanly today has no hardware problem in the audit — but a file that speaks in their favour.

NIS2 in ten minutes: who, what, from when

Directive (EU) 2022/2555 — NIS2 for short — entered into force on 16 January 2023 and had to be transposed into national law by 17 October 2024 [1][2]. It replaces the first NIS Directive of 2016 and considerably widens its scope: from a handful of critical-infrastructure operators to a broad circle of medium and large enterprises across 18 sectors.

Who is affected

NIS2 distinguishes two categories of entities. **Essential entities** (in German law: "besonders wichtige Einrichtungen") are typically large enterprises from 250 employees or EUR 50 million turnover in the high-criticality sectors of Annex I — energy, transport, banking, financial markets, health, drinking water, waste water, digital infrastructure, ICT service management, public administration, space. **Important entities** are medium-sized companies from 50 employees or EUR 10 million turnover in these and in the seven further sectors of Annex II — including postal services, waste, chemicals, food, manufacturing (medical devices, electronics, machinery, vehicles), digital providers and research [1].

Decisive for the mid-market: the size threshold is an *either/or* rule. A machinery manufacturer with 60 employees is in scope just as a food producer with EUR 12 million turnover. Whether your own company is affected can be clarified in a few minutes with the BSI's scope check [4].

Germany: NIS2UmsuCG and BSIG

Germany missed the deadline and brought the NIS2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) into force in December 2025. Its core is the amended BSI Act (BSIG). According to the Federal Ministry of the Interior's estimate, roughly 30,000 entities are covered — about 8,250 essential and around 21,600 important [3][16]. The central sections:

§ BSIG	Subject	Relevance to hardware maintenance
§ 28	Scope	Clarifies whether the maintained infrastructure is in NIS2 scope at all
§ 30	Risk management measures	Counterpart to Art. 21 — supply chain, maintenance, vulnerabilities, BCM
§ 31	Special requirements for operators of critical facilities	Attack detection systems — also concerns network and management hardware
§ 32	Reporting obligations	24h/72h/1-month cascade — the maintenance partner must feed in
§ 33	Registration obligation	Registration with the BSI within three months of falling in scope
§ 38	Duties of management	Approval, oversight, training — personal responsibility
§ 65	Fines	Up to EUR 10 million / 2 % or EUR 7 million / 1.4 % of global turnover

When audits happen

Unlike a certification, NIS2 has no fixed audit date. Essential entities are subject to ongoing supervision by the BSI and must present evidence on request; operators of critical facilities demonstrate their measures at regular intervals. Important entities are audited on an event basis — typically after an incident or a tip-off [1][3]. In practice, however, the audit questions arrive sooner: through customers who must assess their own supply chain under Art. 21(2)(d), through insurers, and through statutory auditors who include management's duties under § 38 BSIG in their review.

KEY TAKEAWAY

The auditor rarely comes by appointment. Whoever starts collecting evidence only for the audit is too late — the first "auditor" is often your own key account with a supplier questionnaire.

Why hardware maintenance is a NIS2 topic

At first glance NIS2 is about cybersecurity — attacks, vulnerabilities, reporting channels. The pressure is real: in its Wirtschaftsschutz 2024 study, the German digital association Bitkom puts the annual damage to the German economy from cyberattacks, sabotage and espionage at around EUR 266.6 billion [15]. Next to that, hardware maintenance sounds like spare parts and response times. The connection becomes clear when three of the directive's protection goals are applied to physical operations.

1. Availability is a security objective

Art. 21(1) obliges entities to take measures "to manage the risks posed to the security of network and information systems ... and to prevent or minimise the impact of incidents" [1]. "Incident" is defined broadly in Art. 6: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered. A failed storage controller without an available spare is therefore not merely an operational problem — it can be a reportable incident, regardless of whether an attacker was involved.

2. The maintenance partner is part of the supply chain

Art. 21(2)(d) requires measures on "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers". Paragraph 3 specifies that the vulnerabilities specific to each supplier and the overall quality of its products and cybersecurity practices must be taken into account [1]. A maintenance provider whose engineers obtain physical and remote access to servers and bring spare parts into the environment is a direct service provider within the meaning of this provision. It must be assessed, contractually bound and monitored.

3. Maintenance is named explicitly

Point (e) requires "security in network and information systems acquisition, development and **maintenance**, including vulnerability handling and disclosure" [1]. The directive thus names the maintenance phase not in passing but as a regulatory subject in its own right — and couples it to vulnerability handling. For hardware this means: firmware levels, management controllers (BMC, iLO, iDRAC, CIMC), network operating systems and storage microcode are part of vulnerability management, not just the application stack.

What auditors derive from this

Auditors rarely work from the directive text; they use audit catalogues derived from it — in Germany primarily the BSI IT-Grundschutz Compendium [5] and ISO/IEC 27001:2022 [8]. Both have dedicated modules for exactly this interface: OPS.2.3 "Use of outsourcing", OPS.1.1.3 "Patch and change management", CON.6 "Deletion and destruction", DER.2.1 "Security incident handling" on the BSI side; controls 5.19 to 5.22 (supplier relationships), 7.13 (equipment maintenance), 7.14 (secure disposal or re-use) and 8.8 (management of technical vulnerabilities) in Annex A of ISO 27001. Whoever holds their maintenance contract against these modules knows what the auditor wants to see.

KEY TAKEAWAY

Availability, supply chain, maintenance: three terms from Art. 21 that together describe precisely the service a hardware maintenance contract delivers. That is why it is on the audit list.

The ten measures of Art. 21 — and their hardware relevance

Art. 21(2) lists ten areas of measures that every in-scope entity must implement "at least". § 30(2) BSIG adopts the catalogue almost verbatim [1][3]. The following overview maps each area to what it means for operating and maintaining physical infrastructure and which evidence an auditor typically wants to see.

Art. 21(2)	Measure	Hardware / maintenance relevance	Typical evidence
a	Risk analysis and security policies	Hardware assets are part of the risk analysis — incl. age, support status, redundancy	Risk register with asset reference
b	Incident handling	Hardware failure and firmware compromise as incident types; role of the maintenance partner	Incident process, escalation matrix
c	Business continuity, backup, crisis management	Restoration times, spare-parts stocking, redundancy — the SLA core	BCM plan, SLA reports, test records
d	Supply chain security	Maintenance provider, origin of spare parts, subcontractors	Supplier assessment, contract, certificates
e	Security in acquisition, development, maintenance; vulnerabilities	Firmware patching, EOSL handling, vendor advisories	Patch log, vulnerability tracking
f	Assessing effectiveness	Regular check whether SLA and patch process are working	KPI review, internal audits
g	Cyber hygiene and training	On-site engineer conduct, handling of removable media and diagnostic tools	Training records, code of conduct
h	Cryptography and encryption	Encrypted drives; key handling when replacing disks	Crypto concept, erase certificates
i	HR security, access control, asset management	Asset inventory, third-party site access, remote access	Inventory, access logs, entry records
j	MFA, secure communications, emergency communication	MFA for remote maintenance access; emergency reachability of the service desk	MFA evidence, reachability matrix

Four areas with direct reach

Areas c, d, e and i act directly on the maintenance contract. Together they answer the question the auditor asks: *Is this hardware kept available, by an assessed partner, with current firmware, under controlled access?* The remaining six act indirectly — they set the organisational frame in which the contract lives.

State of the art and proportionality

Art. 21(1) requires measures to reflect the "state of the art" and to be proportionate — measured against risk exposure, size of the entity, likelihood and severity of incidents [1]. For the mid-market this is both relief and obligation: nobody expects an 80-person supplier to run a network operator's processes. But appropriateness must be reasoned and documented. A maintenance contract with 4-hour on-site response for the ERP cluster and next-business-day for the test environment is exactly such a reasoned gradation — provided it follows from the risk analysis (point a) and not from the budget.

KEY TAKEAWAY

Ten measures, four with direct hardware reach: BCM (c), supply chain (d), maintenance and vulnerabilities (e), access and assets (i). They form the grid along which Chapter 5 builds the audit matrix.

What auditors check: the audit matrix

Auditors do not check whether an entity is "NIS2-compliant" — no such certificate exists. They check whether the required measures are *implemented, documented and effective*. For hardware operations, a pattern of ten audit fields has emerged that can be derived from Art. 21, the BSI modules and ISO 27001. The following matrix is a TechCare working aid: for each field it names the audit question, the evidence auditors typically request, and the reference they rely on [1][5][8].

#	Audit field	Audit question	Expected evidence	Reference
1	Asset inventory	Is every hardware system recorded with model, location, owner, support status and criticality?	Current inventory, CMDB reconciliation, last update	Art. 21(2)(i) · ISO 5.9 · IR 2024/2690 sect. 12
2	Criticality & risk	Is the failure impact assessed per system and the protection measure derived from it?	Risk register, protection needs assessment, SLA mapping	Art. 21(2)(a) · BSI Standard 200-3
3	Availability & SLA	Are response and restoration times contractually fixed and backed by spare-parts stocking? Are they met?	Maintenance contract, SLA performance reports, ticket analysis	Art. 21(2)(c) · ISO 5.30 · BSI OPS.2.3
4	Supplier assessment	Is the maintenance partner assessed as a supplier — certificates, subcontractors, locations, security practice?	Supplier assessment, ISO 27001 certificate, sub-outsourcing list	Art. 21(2)(d), (3) · ISO 5.19–5.22
5	Contract & clauses	Does the contract contain security requirements, reporting participation, audit rights, exit rules?	Contract text with security annex	Art. 21(2)(d) · ISO 5.20 · DORA Art. 30 (blueprint)
6	Firmware & patches	Are vendor advisories tracked and firmware updates applied with documentation?	Patch log per system, advisory reconciliation, reasoned exceptions	Art. 21(2)(e) · BSI OPS.1.1.3 · ISO 8.8
7	End of support (EOSL)	Which systems run beyond vendor support — and with what documented risk acceptance?	EOSL list, management risk acceptance, compensating controls	BSI OPS.1.1.3 (MUST) · § 38 BSIG
8	Incidents & reporting	Is it defined how hardware incidents are detected, escalated and fed into the 24h/72h cascade?	Incident process, escalation matrix incl. partner, exercise record	Art. 23 · § 32 BSIG · BSI DER.2.1
9	Media & spare parts	Are replaced drives verifiably erased or destroyed? Is the origin of spare parts evidenced?	Erase/destruction certificates, chain of custody, serial-number log	BSI CON.6 · ISO 7.10, 7.14 · NIST SP 800-88
10	Third-party access	Are engineers' physical and remote access controlled, logged and secured with MFA?	Entry records, access logs, MFA evidence, escort rule	Art. 21(2)(i), (j) · BSI ORP.4, INF.2

How auditors proceed

The order of the matrix follows the typical audit flow: the auditor starts with the inventory (without a complete asset list every further statement is unsupported), moves via criticality to SLA and supplier, and ends with the physical controls. Sampling is standard: "Show me, for this storage system, the support status, the last firmware update, the responsible contact at the maintenance partner and the last spare-parts replacement with media evidence." Whoever can produce these four items for any system within minutes has passed the field.

The most common gaps

From audit practice against BSI Grundschutz and ISO 27001, three gaps are typical and recur under NIS2: first, an inventory that does not flag hardware beyond vendor support; second, maintenance contracts without a security annex — response time yes, reporting participation, subcontractors and media rules no; third, missing evidence for replaced media. All three are organisationally solvable; none requires new hardware.

KEY TAKEAWAY

Ten audit fields, four items per sample: support status, patch level, contact, media evidence. Whoever can deliver these for every system leads the audit — not the auditor.

Supply chain security: the maintenance provider as supplier

According to ENISA, supply chain attacks have for years been among the defining threats to the European cybersecurity landscape; the agency dedicates separate chapters to them in its Threat Landscape series [14]. NIS2 responds with Art. 21(2)(d) and (3) and with coordinated risk assessments of critical supply chains under Art. 22 [1]. For operators this means every direct service provider with access to network and information systems must be assessed — and the hardware maintenance partner is among the providers with the deepest access of all.

What "assess" means

Art. 21(3) names three dimensions: the provider's specific vulnerabilities, the overall quality of its products and cybersecurity practices, and its secure development procedures [1]. Applied to maintenance providers, this yields an assessment grid that ISO/IEC 27001:2022 makes concrete in controls 5.19 to 5.22 [8]:

- **5.19 Information security in supplier relationships** — Is there a policy on which requirements apply to providers with system access?
- **5.20 Addressing security within supplier agreements** — Are these requirements in the contract (Chapter 12)?
- **5.21 Managing security in the ICT supply chain** — Is it known where spare parts come from and which subcontractors the provider uses?
- **5.22 Monitoring, review and change management** — Are SLA reports reviewed, certificates tracked, changes (new subcontractors, new locations) reported?

The BSI view: OPS.2.3

Module OPS.2.3 "Use of outsourcing" of the IT-Grundschutz Compendium (2023 edition) is the German concretisation [5]. Among other things it requires an outsourcing strategy, a security requirements specification for the provider, contractual rules on security and control, an orderly termination and ongoing monitoring. Applied to hardware maintenance, four points are audit-relevant: Who may access which system when, with which authorisation? Which subcontractors are involved with which access? Where are spare parts stored and how is their origin evidenced? How does the relationship end — return of access, documentation, handover?

DORA as a blueprint

For financial entities, the DORA Regulation (EU) 2022/2554 has since January 2025 specified in Arts. 28 to 30 very concretely what contracts with ICT third-party providers must contain: service description, locations of service provision, availability and integrity commitments, incident assistance, cooperation with authorities, termination rights, exit strategies [9]. NIS2 is less detailed, but auditors increasingly use DORA as the yardstick for what an "appropriate" provider contract contains. Whoever structures their maintenance contract along DORA lines today is over-documented for NIS2 — the more comfortable position in an audit.

Sub-outsourcing: the invisible second tier

The most frequent finding in supplier audits concerns the second tier: the contracting party is known and assessed, its subcontractors — spare-parts logistics, regional engineer partners, remote support centres — are not. Art. 21(2)(d) speaks of "direct" suppliers, yet ISO 5.21 and OPS.2.3 require transparency across the chain. In practice: the maintenance contract should contain a list of subcontractors with role and location and provide for a notification duty on changes.

KEY TAKEAWAY

The maintenance partner has physical access, remote access and brings parts into the environment — no other supplier gets closer to the infrastructure. The assessment must reach correspondingly deep: to subcontractors, spare-parts origin and exit arrangements.

SLA requirements under NIS2: availability is a security objective

A service level agreement was long a commercial instrument: response time against price. Under NIS2 it becomes security evidence for Art. 21(2)(c) — business continuity, backup management, disaster recovery [1]. The auditor therefore reads the SLA section with a different question: not "Is this cheap?" but "Is the restoration time of critical systems guaranteed, evidenced and tested?"

Why outages are security incidents

The Uptime Institute reports in its Annual Outage Analysis 2024 that a good half of surveyed operators had at least one significant outage in the preceding three years; more than half of serious outages cost over USD 100,000 and around one in six over one million [13]. For NIS2, what counts is less the financial loss than the service disruption: as soon as an essential service is significantly disrupted, the reporting obligation under Art. 23 applies — even for a purely technical cause.

The four SLA building blocks auditors expect

Building block	What should be agreed	Evidence in the audit
Response and restoration time	Tiered by criticality (e.g. 4h on-site for tier 1, NBD for tier 3), mapped per system; restoration time as a target, not just response	SLA matrix with asset reference, monthly performance report
Spare-parts stocking	Regional depots, critical components pre-stocked, delivery time committed, origin documented	Depot list, parts reservation, chain of custody
Escalation and reachability	24/7 service desk, named escalation levels, emergency contact outside the ticket chain (Art. 21(2)(j))	Escalation matrix, reachability test
Reporting and review	Regular SLA reports, ticket analysis, annual service review with actions	Reports, review minutes (Art. 21(2)(f))

Response is not restoration

Many SLAs commit to a response time — the point at which an engineer accepts the case. For Art. 21(2)(c) what counts is restoration of the service. The difference is decisive in an audit: an SLA promising "response within 4 hours" says nothing about availability if the spare part is three days away. Auditors therefore expect either a committed restoration time or — more realistic for hardware — a response time *plus* verifiable spare-parts stocking from which the actual restoration time can be derived.

Test, don't trust

ISO 27001:2022 control 5.30 "ICT readiness for business continuity" requires recovery capabilities to be planned, implemented and *tested* [8]. For hardware maintenance this means at minimum: once a year, rehearse the failure of a critical system — including the call to the service desk, the spare-parts request and a record of the actual times.

KEY TAKEAWAY

Under NIS2 the SLA answers the question of restoration time, not response time. Committed times, stocked spares, measured reports and an annual test — that is the evidence for Art. 21(2)(c).

Firmware, patches, vulnerabilities: OPS.1.1.3 and EOSL hardware

In the reporting period of its 2024 situation report, the BSI registered an average of 78 new vulnerabilities in software products per day — an increase over the previous year [6]. A growing share concerns not applications but the layer beneath: firmware of servers, management controllers, storage systems and network devices. This is exactly the layer Art. 21(2)(e) addresses with the wording "security in ... maintenance, including vulnerability handling and disclosure" [1].

Why firmware stands out in audits

Management controllers (iLO, iDRAC, CIMC, BMC) run beneath the operating system, are often permanently networked and in many environments are updated less frequently than the application stack. Cisco PSIRT, HPE Security Bulletins and Dell Security Advisories regularly publish notices on these components [17]; the CISA Known Exploited Vulnerabilities (KEV) catalogue repeatedly lists entries on network and edge devices [11]. For the auditor the question is simple: "When was this system's firmware last updated, and who reconciled the vendor advisories?" If there is no answer, point (e) is not met.

The BSI module OPS.1.1.3

OPS.1.1.3 "Patch and change management" (2023 edition) requires a documented process for patches and changes — responsibilities, testing, approval, deployment, evidence [5]. Two requirements are central for hardware maintenance. First: patches must be assessed and applied promptly, including firmware. Second, phrased as a MUST requirement: where products no longer supported by the vendor are in use, it MUST be checked whether they can still be operated securely; if not, they MUST NOT continue to be used.

EOSL hardware under NIS2

This requirement makes end-of-service-life hardware an audit field in its own right (Chapter 5, field 7). It does not prohibit continued operation — it requires a documented assessment of secure operability. Continued operation holds up in an audit when four conditions are met:

- **Flagged in the inventory:** The system is marked EOSL, with the date of the vendor's end of support.
- **Vulnerability status:** It has been checked whether open, exploited vulnerabilities (KEV) are known for model and firmware level.
- **Compensating controls:** Network segmentation, hardened management access, increased monitoring, shutdown of unneeded services where applicable — documented and implemented.
- **Management risk acceptance:** Continued operation is documented as a deliberate decision with a review date and approved by management (§ 38 BSIG).

Vendor-independent maintenance delivers the operational part — spare parts, response time, operational reliability — but does not replace the security assessment. This separation should be clear in the contract: the maintenance partner guarantees availability and supplies firmware levels and advisories; the decision on continued operation rests with the operator. Whitepaper No. 02 "EOSL Strategy" covers the assessment process in depth with a six-dimension risk score.

The Cyber Resilience Act as outlook

Regulation (EU) 2024/2847 (Cyber Resilience Act) will oblige manufacturers of connected products to provide security updates over a support period of at least five years and to report actively exploited vulnerabilities; the reporting obligations apply from September 2026, full application from December 2027 [10]. Nothing changes for installed hardware — for new purchases, the support period becomes a contractually tangible criterion that belongs in lifecycle planning.

KEY TAKEAWAY

Firmware is part of vulnerability management, and end of support is an audit field: continued operation is permissible when inventory, vulnerability status, compensating controls and management risk acceptance are documented — not because the device still runs.

The 24h / 72h / 1-month reporting cascade: what the maintenance partner must deliver

Art. 23 NIS2 and § 32 BSIG oblige in-scope entities to report significant incidents in three stages: an **early warning within 24 hours** of becoming aware, an **incident notification within 72 hours** with an initial assessment of severity, impact and indicators of compromise, and a **final report within one month** covering root cause, measures and cross-border impact [1][3]. An incident is "significant" if it has caused or is capable of causing severe operational disruption or financial loss, or has affected other persons considerably.

Where hardware enters the cascade

Three scenarios make hardware maintenance part of the reporting process. First, the *outage with service impact*: a storage cluster loses redundancy and an essential service is down — technical cause, but severe operational disruption. Second, the *firmware compromise*: a management controller shows signs of unauthorised access. Third, the *incident at the provider*: the maintenance partner itself is compromised and its remote access or spare-parts logistics are affected. In all three cases the operator needs, within 24 hours, information that only the maintenance partner holds.

What the contract must regulate

Stage	Deadline	Input from the maintenance partner
Early warning	24 h	Immediate notification of hardware incidents with service impact; initial indication whether a security dimension is suspected; named 24/7 contact
Incident notification	72 h	Technical classification (affected components, firmware levels, access logs of the maintenance account), support in assessing severity, preservation of evidence
Final report	1 month	Root-cause analysis from the hardware perspective, spare-parts and replacement log, measures implemented, lessons learned

The incident at the provider

The third constellation is particularly audit-relevant. If the maintenance partner itself becomes the target of an attack, the operator must learn of it — quickly enough to meet its own 24-hour deadline. A contractual duty of the provider to report its own security incidents with possible customer impact is therefore, under NIS2, not a nice-to-have but the precondition for the operator's own reporting chain to work at all. ISO 27001 control 5.20 and DORA Art. 30(2) name exactly this clause [8][9].

The BSI module DER.2.1

DER.2.1 "Security incident handling" requires defined reporting channels, responsibilities, an escalation strategy and the involvement of external parties [5]. Applied to maintenance: the partner's service desk must appear in the operator's escalation matrix — with name, number and deputy rule. An auditor who looks at the matrix and finds no hardware partner will ask how a storage failure at three in the morning fits into the 24-hour deadline.

KEY TAKEAWAY

The reporting deadlines are the operator's, but the facts often sit with the maintenance partner. Without a contractual duty of the provider to participate and report, the 24-hour deadline cannot be met in a hardware case.

Media, spare parts, access: the physical controls

NIS2 is read as a cyber directive, yet a substantial share of the audit items in hardware operations is physical: What happens to a replaced disk? Where does the replacement controller come from? Who was in the server room, and when? Three control areas are in focus.

1. Storage media: erasure and destruction

Every disk or SSD replacement moves a medium with potentially confidential data out of the controlled environment. BSI module CON.6 "Deletion and destruction" requires an erasure concept with procedures per media type and protection level, plus evidence of execution [5]. ISO 27001 control 7.14 requires that equipment containing storage media be verified and data securely removed before disposal or re-use; control 7.10 governs the handling of storage media across their lifecycle [8]. NIST SP 800-88 "Guidelines for Media Sanitization", which defines the levels Clear, Purge and Destroy, has become the established technical yardstick [12].

Three rules for the maintenance contract follow: defective media remain with the customer or are destroyed on site; every replacement is logged with serial number; for every medium leaving the environment there is an erasure or destruction certificate. Auditors specifically ask for the last replacement and its certificate — field 9 of the matrix.

2. Spare parts: origin and chain of custody

Art. 21(2)(d) and ISO 5.21 require transparency over the ICT supply chain — including the origin of spare parts [1][8]. Counterfeit or manipulated components are a known risk in secondary markets; vendors regularly warn against unauthorised parts [17]. The evidence auditors expect is an unbroken chain of custody: source, incoming inspection, storage location, serial number, installation date, engineer. A maintenance partner with its own depots and documented incoming inspection can provide this; a contract should require it.

3. Third-party access: on-site and remote

Point (i) requires access control and asset management, point (j) multi-factor authentication [1]. For maintenance engineers this means two things. **Physical:** server-room entry only pre-announced, escorted or with a personal badge, and logged (BSI INF.2 "Data centre and server room") [5]. **Remote:** maintenance access only via MFA-secured, personal accounts, time-limited, logged, with no permanent standing-access connections; remote-support software and diagnostic laptops are subject to the rules for third-party devices (point g, cyber hygiene). Auditors sample entry records and access logs and compare them with maintenance tickets: every access needs a ticket, every ticket an access.

Personnel security

Point (i) explicitly names the security of personnel. For third-party engineers this means: confidentiality undertaking, documented qualification (vendor certifications), background check where required — and a named list of persons authorised to obtain access. The maintenance contract should oblige the partner to keep this list current and to report personnel changes.

KEY TAKEAWAY

Three physical questions decide audit fields 9 and 10: Where is the replaced disk and who erased it? Where does the spare part come from? Who was at the system, when, under which ticket? Each needs evidence — not an assurance.

Documented accountability: § 38 BSIg and management

The biggest change NIS2 brings to everyday corporate life is not technical. Art. 20 of the directive and § 38 BSIg personally oblige **management bodies** to approve the risk management measures, oversee their implementation and undergo regular training [1][3]. Whoever breaches these duties is liable to the entity under the rules of company law. Cybersecurity — and with it the secure operation of hardware — thus becomes a management duty, no longer a delegable IT task.

What "approve and oversee" means for hardware maintenance

Management need not read every maintenance contract. But it must be able to show that it knows and has backed the fundamental decisions: which systems are critical, which availability is committed for them, which partner maintains them, which systems run beyond vendor support and on what reasoning. In an audit this is typically checked through minutes: is there a resolution or acknowledgement by management on the risk analysis, the supplier strategy, the EOSL list?

The responsibility matrix

Auditors expect responsibilities to be unambiguous not only internally but also towards the maintenance partner. A simple allocation along the RACI pattern — who decides, who executes, who is consulted, who is informed — creates the clarity Art. 21(2)(a) and (i) require:

Task	Operator (management)	Operator (IT / CISO)	Maintenance partner
Define criticality and protection needs	Approves	Prepares	Is informed
Map SLA tiers per system	Approves	Decides	Implements, reports
Assess firmware advisories	—	Decides	Supplies, applies
Continued operation of EOSL systems	Approves risk acceptance	Assesses, proposes	Secures operation, supplies facts
Report hardware security incident (24h/72h)	Accountable for report	Reports to BSI	Reports to operator, supplies analysis
Erase / destroy media	—	Checks evidence	Executes, certifies
Annual supplier assessment	Acknowledges	Performs	Supplies evidence (certificates, sub list)

Documentation as relief

§ 38 BSIg is, at first, a liability risk for management. Read correctly, the provision is also a relief: whoever has demonstrably approved and overseen risk analysis, supplier selection and EOSL decisions has fulfilled their duty — even if an incident occurs. The file protects. Conversely, an incident on a system that was not inventoried, not assessed and had no documented decision is precisely the constellation in which personal responsibility bites.

Training duty

Management must attend training sufficient to assess risks and management practices [1][3]. For hardware operations, an annual briefing summarising the EOSL list, SLA performance and the status of supplier assessments is a natural fit — short, documented, signed. It fulfils the training duty and at the same time creates the evidence of acknowledgement.

KEY TAKEAWAY

§ 38 BSIg lifts the maintenance contract to management level: criticality, supplier and EOSL continuation need a documented decision. The file is the evidence — for the auditor and for management itself.

The maintenance contract in the audit: 12-point clause checklist

This checklist condenses the requirements of Chapters 4 to 11 into twelve checkable contract points. It is intended as a working template: for reviewing an existing maintenance contract as much as for tendering a new one. Each point names the reference an auditor would rely on [1][3][5][8][9].

- ☐ **1 • Scope with asset reference.** The contract lists the maintained systems (model, serial number, location) and maps an SLA tier to each.
Art. 21(2)(i) · ISO 5.9

- ☐ **2 • Response and restoration times.** Times fixed per tier; restoration named as the target; spare-parts stocking and depot locations described.
Art. 21(2)(c) · ISO 5.30

- ☐ **3 • SLA reporting and review.** Monthly performance reports, annual service review with action minutes.
Art. 21(2)(f) · ISO 5.22

- ☐ **4 • Security annex.** Binding security requirements for the provider (certification, personnel, access, media) as part of the contract.
Art. 21(2)(d) · ISO 5.20 · BSI OPS.2.3

- ☐ **5 • Subcontractor transparency.** List of subcontractors with role and location; notification duty on changes; approval reservation for security-relevant sub-awards.
ISO 5.21 · DORA Art. 30(2)

- ☐ **6 • Firmware and advisories.** Supply of vendor advisories and firmware levels; deployment after operator approval; documentation per system.
Art. 21(2)(e) · BSI OPS.1.1.3 · ISO 8.8

- ☐ **7 • Handling end of support.** Flagging of EOSL systems; supply of facts for risk acceptance; clear separation: operational assurance by the partner, continuation decision by the operator.
BSI OPS.1.1.3 · § 38 BSI G

- ☐ **8 • Reporting participation.** Immediate notification of hardware incidents with service impact; reporting of the provider's own security incidents; input for the 24h/72h/1-month cascade; 24/7 escalation contact.
Art. 23 · § 32 BSI G · BSI DER.2.1

- ☐ **9 • Storage media.** Defective media remain with the customer or are destroyed on site; serial-number log; erasure/destruction certificate per medium.
BSI CON.6 · ISO 7.10, 7.14 · NIST SP 800-88

- ☐ **10 • Spare-parts origin.** Sources, incoming inspection and chain of custody documented; no unauthorised parts.
Art. 21(2)(d) · ISO 5.21

- ☐ **11 • Access and personnel.** Named engineer list, confidentiality, qualification evidence; escorted and logged site entry; remote only with MFA, personal, time-limited, logged.
Art. 21(2)(i), (j) · BSI ORP.4, INF.2

- ☐ **12 • Audit rights and exit.** Audit right of the operator and its supervisory authority; cooperation in audits; orderly termination with return of access, documentation and handover.
ISO 5.22 · BSI OPS.2.3 · DORA Art. 30(2)

Application

For an existing contract, a security annex as an addendum covering points 4 to 12 is often sufficient — the commercial points 1 to 3 are usually in place. For a new award, the checklist should be part of the requirements specification; providers unable to meet individual points drop out of the supplier assessment before prices are compared.

KEY TAKEAWAY

Twelve clauses, three commercial, nine security-related. A maintenance contract covering all twelve is not a risk in a NIS2 audit but evidence — for Art. 21, § 32 and § 38 at once.

Conclusion

NIS2 changes what a maintenance contract is. A commercial document about response times becomes an evidence document for four of the ten mandatory measures in Art. 21: business continuity, supply chain, maintenance and vulnerabilities, access and assets. The auditor reads it accordingly — and asks questions a classic SLA does not answer.

The good news: none of these questions requires new hardware or fundamentally different processes. They require documentation. A complete inventory with support status, a supplier assessment reaching to subcontractors and spare-parts origin, a firmware process with evidence, reporting participation by the partner, certificates for every replaced medium and a management decision on the critical calls — that is the scope. The audit matrix in Chapter 5 and the clause checklist in Chapter 12 make it workable.

The less comfortable news: the auditor rarely comes by appointment. They come as a key account with a supplier questionnaire, as an insurer, as a statutory auditor including § 38 BSIG in their review — or after an incident, when the 24-hour clock is already running. Whoever starts collecting evidence then loses not only time but the burden of proof.

Vendor-independent maintenance is not a risk in this situation but a lever: it makes the continued operation of proven systems possible, supplies the operational and spare-parts facts the operator needs for its risk acceptance — and a partner who contractually carries the twelve clauses of Chapter 12 turns, in the audit, from audit item into evidence.

IN ONE SENTENCE

NIS2 does not ask whether your hardware is maintained — it asks whether you can prove it.

About TechCare & sources

About TechCare Solutions

TechCare Solutions GmbH, headquartered in Hahnstätten, Germany, maintains server, storage and network hardware from all major enterprise vendors independently of the manufacturer — including beyond End of Service Life. Our maintenance contracts are designed for the requirements of NIS2, DORA, KRITIS, BAIT, TISAX and ISO 27001: SLA performance reports, documented incident response within 24 hours, sub-outsourcing transparency, chain of custody for spare parts and erase certificates for every replaced medium. A compliance officer accompanies audits as escalation instance.

Contact: techcaresolutions.de · 24/7 service desk (DE/EN) · Hahnstätten

Methodology & transparency

All specific figures in this whitepaper come from the publicly accessible sources listed below (EU legal acts, German legislation, BSI publications, ISO standard, agency and industry studies). Where sources contain ranges or estimates, this is marked in the wording ("around", "about", "estimated"). The audit matrix (Chapter 5), the responsibility matrix (Chapter 11) and the clause checklist (Chapter 12) are TechCare Research working aids derived from the cited frameworks; they do not constitute legal advice. In individual cases the legal text and the assessment of the competent supervisory authority prevail.

Sources

- [1] Directive (EU) 2022/2555 (NIS2), esp. Arts. 6, 20, 21, 22, 23. eur-lex.europa.eu/eli/dir/2022/2555
- [2] European Commission — NIS2 Directive (policy overview). digital-strategy.ec.europa.eu/en/policies/nis2-directive
- [3] German NIS2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) / BSI Act (BSIG), esp. §§ 28, 30–33, 38, 65. gesetze-im-internet.de/bsig
- [4] BSI — NIS-2: information for companies, scope check. bsi.bund.de/nis-2
- [5] BSI — IT-Grundschutz Compendium, 2023 edition: OPS.1.1.3, OPS.2.3, CON.6, DER.2.1, ORP.4, INF.2. bsi.bund.de/grundschutz
- [6] BSI — The State of IT Security in Germany 2024. bsi.bund.de/lagebericht
- [7] Commission Implementing Regulation (EU) 2024/2690 (technical requirements, Annex). eur-lex.europa.eu
- [8] ISO/IEC 27001:2022, Annex A — controls 5.9, 5.19–5.22, 5.30, 7.10, 7.13, 7.14, 8.8. iso.org
- [9] Regulation (EU) 2022/2554 (DORA), Arts. 28–30 ICT third-party risk. eur-lex.europa.eu/eli/reg/2022/2554
- [10] Regulation (EU) 2024/2847 (Cyber Resilience Act). eur-lex.europa.eu/eli/reg/2024/2847
- [11] CISA — Known Exploited Vulnerabilities (KEV) Catalog. cisa.gov/known-exploited-vulnerabilities-catalog
- [12] NIST SP 800-88 Rev. 1 — Guidelines for Media Sanitization. csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
- [13] Uptime Institute — Annual Outage Analysis 2024. uptimeinstitute.com
- [14] ENISA — Threat Landscape 2024. enisa.europa.eu/publications/enisa-threat-landscape-2024
- [15] Bitkom — Wirtschaftsschutz 2024 (damage from cyberattacks). bitkom.org
- [16] OpenKRITIS — NIS2 implementation in Germany, scope estimates. openkritis.de
- [17] Vendor security advisories: Cisco PSIRT, HPE Security Bulletins, Dell Security Advisories. cisco.com · support.hpe.com · dell.com/support