

Implementing NIS-2 on the Basis of ISO 9001

Transitioning From Quality Management to Robust Information Security Governance—With a Worked Example, Roadmap and Evidence Model for Mid-Sized Companies

Derek Carson

AI Governance & Information Security
carson.de

As of October 2026

Key Points for Management

What must be clarified immediately: Is your registration data with the BSI (Germany's Federal Office for Information Security) up to date, and is someone responsible for it? Can your company report a significant security incident within 24 hours—including on the weekend? Has management attended training? These obligations already apply.

Existing assets: With ISO 9001, you already have document management, internal audits, corrective action and regular management review. These procedures can be used for information security—provided they are practiced day to day and extended to the whole company.

Where you will probably need to invest: first in information security expertise—internal or external. A formal risk assessment identifies mandatory controls while preventing over-engineering; without one, it is easy to invest in the wrong place. Technical hardening flows directly from that risk assessment—typically including offline backups, multi-factor authentication (MFA) for remote access, incident detection, and network segmentation between corporate IT and OT/production.

What you need to decide: who coordinates information security; which risks are treated first and which residual risks are accepted; what budget is available; and whether you will later seek certification under ISO/IEC 27001.

The next three steps:

1. Establish the ability to report incidents and train management—these obligations apply immediately.
2. Carry out an assessment across all ten areas of Section 30 BSIG, including all sites.
3. On this basis, adopt a prioritized action plan.

1. Target Readers and Core Promise

Germany's NIS-2 Implementation Act (NIS2UmsuCG), which amends the BSI Act (BSIG), has been in force since December 6, 2025, with no grace period. The number of companies affected is very large: by September 30, 2026, 20,141 entities had registered with the Federal Office for Information Security (BSI)—13,252 of them as "important entities" (*wichtige Einrichtungen*) (BSI, NIS-2 in Zahlen).

However, BSI registration fulfills only a single statutory obligation (Section 33 BSIG). The core legal mandate—implementing continuous, enforceable security controls and documenting compliance under Section 30 BSIG—remains fully in effect.

A survey of 51 affected companies from late summer 2026 shows how much catching up mid-sized companies have to do (*Kertos, NIS2 Readiness Study 2026*):

- **4 %** of the companies surveyed said they fully implement the requirements.
- **18 %** had not even started implementation.

(Note: Since this study comes from a software vendor and the sample is small, these figures serve as an indication, not as statistically representative values.)

Who This Guide Is For

This guide is written specifically for **management** and **those responsible for quality management** in companies that meet three criteria:

1. The company falls within the legal scope of NIS-2.
2. It already operates a quality management system certified under **ISO 9001**.
3. It does **not** yet have an established information security management system (ISMS under ISO/IEC 27001).

The Central Thesis

Organizations with an active ISO 9001 system don't need to build a NIS-2 compliance framework from scratch. They extend their existing system and put budget and expertise where NIS-2 genuinely requires something new: in the security measures.

Compared with a separate information security management system built alongside the quality management system, this approach has four advantages:

- **Your budget goes into security, not into organization.** Document management, internal audits, corrective action and regular management review already exist. A greenfield ISMS forces you to reinvent these workflows; building on ISO 9001 lets you focus immediately on technical hardening. (*Sections 4 and 7*)
- **Executive leadership oversees security through familiar governance workflows.** Under Section 38 BSIG, management must ensure that the security measures are implemented and must oversee their implementation. Your existing QMS management review cycle provides a built-in framework for this oversight. A separate system would need a new one. (*Section 8*)
- **One unified system, not two.** Employees, auditors and management work with one set of procedures and one audit program. Eliminates redundant documentation and audit overhead.

- **Keeps the path open for formal certification.** Because ISO 9001 and ISO/IEC 27001 share the same Harmonized Structure (HS, formerly High-Level Structure), you extend the system once more instead of rebuilding it if a customer later requires an ISO/IEC 27001 certificate. (*Section 9*)

Where QMS falls short: A quality management system does not replace technical or IT-specific security measures. Technical cybersecurity controls must still be engineered from the ground up. ISO 9001 does, however, provide a suitable organizational framework for them.

Questions This Guide Answers

1. What must you do immediately, and which deadlines apply? (*Section 2*)
 2. How do you verify compliance in practice, beyond paper checklists? (*Section 2*)
 3. Which of your quality management processes can you reuse, and where is the quality management system not enough? (*Section 4*)
 4. Which security measures do you need to build from scratch? (*Section 5*)
 5. In what order should you proceed? (*Section 6*)
 6. What resource investment should you anticipate, and what drives costs? (*Section 7*)
 7. How do you provide evidence of implementation, and how does management keep track? (*Section 8*)
-

A Continuous Worked Example

To make the theory tangible, one scenario runs through all sections:

Muster Maschinenbau GmbH (a fictitious machine-building company)

- **Structure:** 180 employees, certified under ISO 9001 for years.
 - **IT set-up:** An internal head of IT working with an external IT service provider.
 - **NIS-2 status:** Registered with the BSI as an "important entity".
 - **Lead scenario:** A ransomware attack could encrypt the central ERP system, and the attackers would demand a ransom. No such attack has happened so far. Throughout the sections, we follow how the company protects itself against this risk.
-

Box: Are you really in scope? (Quick check)

Three core questions are enough for initial orientation (*Note: This does not replace legal advice, as special rules apply to particular sectors such as critical infrastructure*):

1. **Sector:** Does your company belong to a sector listed in Annex 1 or Annex 2 of the BSIG (e.g. machinery manufacturing, chemicals, food, energy, logistics)?
2. **Size:** Does your company employ **at least 50 people** or generate **annual turnover of more than €10 million** together with a **balance sheet total of more than €10 million**? (*Important: If this threshold is exceeded, the classification applies to the entire company—not only to the affected business unit.*)
3. **Special cases:** Do exceptions for negligible secondary activities (Section 28(3) BSIG) or group structures (Section 28(4) BSIG) apply?

Practical tip: Use the BSI's scope check (*Betroffenheitsprüfung*) for the initial assessment. Record the result explicitly in your files—even if it is "not in scope". Only then can you show, if the authorities ask later, that you examined the question.

2. The Legal Requirements in Detail

The BSIG distinguishes two basic types of obligation: **obligations that apply immediately** and **ongoing risk management obligations** that require continuous action.

2A. Obligations That Apply Immediately

These obligations cannot wait and must not be pushed into later project phases. The five most important:

1. **Registration and keeping data up to date (Section 33 BSIG):** Registration with the BSI was due within three months after your company came within the scope of NIS-2—for most companies, therefore, by March 6, 2026; this guide assumes it has been done. Since then, changes to company data, addresses or security contacts must be reported to the BSI **without delay**—at the latest within **two weeks**. Your company therefore needs a role explicitly assigned to keeping this data up to date.
2. **Reporting security incidents (Section 32 BSIG):** As soon as you become aware of a "significant security incident", you must report it in several stages to the joint reporting office of the BSI and the BBK (Germany's Federal Office of Civil Protection and Disaster Assistance), via the BSI portal. The basic rule is: as quickly as possible. The law sets maximum deadlines:
 - **Within 24 hours of detecting the incident:** submit an *early warning* (suspicion of unlawful or malicious action, possible cross-border impact).
 - **Within 72 hours of detection:** formal *incident notification* with an initial assessment and technical indicators (IoCs).
 - **At the BSI's request:** *intermediate report* on the current status.
 - **Within one month of the notification:** submit the *final report* with root-cause analysis and remediation (if the incident is still ongoing, a *progress report* first).

Important: The clock starts the moment you first become aware of the incident—not when your IT has analyzed the cause. Since the deadlines also run on weekends, the ability to report must be ensured around the clock (24/7).

Handling the incident itself—detecting, containing, recovering—is, by contrast, part of the security measures under Section 30 BSIG (Section 2B).

3. **Informing your customers when ordered (Section 35 BSIG):** If the BSI orders it, you must inform the recipients of your services without delay about a significant security incident that may affect your service.
4. **Implementation and oversight by management (Section 38(1) and (2) BSIG):** Management must not merely sign off the risk management measures but **actively oversee** their implementation. In the event of culpable breaches of duty, management is liable to the company for the resulting damage under the rules of company law.
5. **Training for management (Section 38(3) BSIG):** Management must attend training regularly so that it can recognize and assess information security risks.

There are further obligations, such as cooperating when the BSI takes supervisory measures (Section 62 BSIG).

2B. The Obligation to Take Effective Measures (Section 30 BSIG)

Section 30 BSIG requires you to take "appropriate, proportionate and effective technical and organizational measures" to protect the availability, integrity and confidentiality of your IT systems. The five most important requirements:

1. **Risk analysis as the basis:** Which measures are appropriate and proportionate follows from your company's risks (Section 30(2) No. 1).
2. **Ten specified areas:** The law names ten specific areas that your measures must cover—including incident handling, backup and business continuity management, and supply chain security (Section 30(2); all ten in Section 5).
3. **Consider all hazards:** Besides cyberattacks, events such as power cuts, heatwaves, fire, water or human error must also be considered (Section 30(2)).
4. **Check effectiveness:** You need procedures to assess whether your measures are working (Section 30(2) No. 6).
5. **Evidence:** You must document how you meet these requirements (Section 30(1)).

There are further requirements, such as taking account of the state of the art and relevant standards (Section 30(2)).

The Three-Level Evidence Model

To document the legal requirements in a way that stands up to audit, we use a three-level evidence grid:

THE THREE-LEVEL EVIDENCE MODEL	
1. THE RULE	What is formally required? (e.g. backup and restore policy)
2. THE MEASURE	What has been implemented technically or organizationally? (e.g. daily isolated immutable backup)
3. THE PROOF OF EFFECTIVENESS	What proves that it actually works? (e.g. record of the last restore test)

The rule of thumb: *A policy without technical implementation has no effect. A technical implementation without proof of effectiveness is not evidenced.*

Why NIS-2 Is an Ongoing Operational Mandate

Risk management under Section 30 BSIG cannot be completed once and filed away. Four legal reasons require a continuous cycle:

- **Alignment with risk:** Protective measures must match the identified risk precisely.
- **Changing threat landscape:** New attack vectors and IT systems constantly change the risk profile.
- **Effectiveness review (Section 30(2) No. 6 BSIG):** Only testing shows whether a protective mechanism works.
- **Duty of oversight (Section 38 BSIG):** Management must be kept informed of the security status on an ongoing basis.

Together, this results in a classic management cycle (**Plan-Do-Check-Act**), which your quality management department has known from ISO 9001 for years.

3. Typical Gaps in Practice

Current figures show that action is needed in many places:

- **39 %** of German companies have no emergency management for espionage, sabotage or data theft (*Bitkom, Wirtschaftsschutz 2025*).
- **20 %** provide no IT security training at all for their employees (*Bitkom 2025*).
- In **63 %** of companies relevant to NIS-2, security is the responsibility of the head of IT, but in only **22 %** does it lie directly with management (*Kertos 2026*).
- **84 %** have no designated information security officer (CISO)—neither internal nor external (*Kertos 2026*).

Where Muster Maschinenbau GmbH Stands Today

Our example company reflects this reality:

1. **Rule level:** The IT security policy dates unchanged from 2019.
2. **Measure level:** Daily backups exist, but the external IT service provider was selected purely on hourly rate and response time—without checking its own security precautions.
3. **Effectiveness level:** A full system restore (restore test) of the central ERP system from backup has **never** been carried out in practice.

There is also a fourth gap that does not belong to any of the three levels: the head of IT alone is responsible for all security matters. Section 4 shows how this can be remedied.

Such gaps usually have several causes that reinforce each other. Security measures were often implemented in the past as one-off projects—without fixed owners, without set review intervals and without proper management of the related documents. In addition, there is an organizational risk that our example company illustrates: if responsibility lies solely with the head of IT, technical operations, risk assessment, company-wide prioritization and reporting to management may not be sufficiently connected. Whether this gap actually exists must be shown by the assessment. Tight budgets and a lack of information security expertise are often added to this.

It follows that two things are missing in such companies: first, a recurring process that keeps the measures up to date and effective over time, and second, the expertise to determine appropriate measures against specific risks. Section 4 shows that an existing ISO 9001 system already provides much of the first. Section 5 shows that the expertise must be built in a targeted way.

4. What the ISO 9001 System Provides—and What It Does Not

4.1 The Existing Process

A company certified under ISO 9001 already maintains a number of binding processes that correspond to the recurring process described in Section 2—so far, however, with a focus on quality rather than information security. These include defined roles and responsibilities (clause 5.3 of the standard), actions to address risks and opportunities (6.1), competence and awareness of employees (7.2 and 7.3), the management and approval of documents (7.5), the control of suppliers and service providers (8.4), monitoring and measurement (9.1), internal audit (9.2), management review (9.3) and corrective action (10.2).

ISO 9001 and ISO/IEC 27001 (the standard for information security management systems) follow the same Harmonized Structure and organize their requirements in clauses 4 to 10 with identical headings. This means that a company with a working ISO 9001 system can extend its existing processes to information security instead of building a second system in parallel.

4.2 The Key Distinction: Same Method, Different Subject

The quality management system also assesses risks and takes measures. Method and process are the same as in information security. The difference lies solely in the subject: the quality management system reduces quality risks, whereas information security reduces risks to the availability, integrity and confidentiality of information. That is why the existing processes can also be used for information security.

This gives the company three advantages. First, existing procedures for document management, internal audits, corrective action and management review can also be used for information security. The quality management system does not need to be rebuilt for this, but extended in a targeted way so that it also covers information security risks and requirements.

Second, the necessary roles and experience already exist. The quality manager can coordinate documentation, audit planning, the preparation of management review and the follow-up of corrective action. This does not, however, replace specialist responsibility for information security: risk assessments, the selection of suitable security measures and the testing of their effectiveness require the relevant expertise—internal or through external support.

Third—and this is the greatest advantage—the cycle already exists: measures are planned, checked in the internal audit, assessed by management and followed up where necessary. Information security thus becomes not a one-off project but a recurring management task. It is precisely this continuous management that is often missing when information security is treated primarily as a technical task for IT (see Section 3).

4.3 Which Processes Can Be Used, and How

For every quality management process, the question is how it can be used for information security. There are four options:

- **reuse:** After checking its suitability, the process can be used unchanged; only the new information security content is added.
- **extend:** The process must be supplemented in a targeted way with specific information security requirements.
- **build new:** The required capability is missing entirely or largely and must be established—usually because ISO 9001 simply does not require it.
- **verify:** The process is documented, but before reusing it you must critically question whether it is actually practiced in day-to-day operations.

Quality management process (ISO 9001)	Rating	What changes	What the process does not provide
Roles and responsibilities (5.3)	extend	Assign responsibility for information security, for registration data and for reports to the BSI	Information security expertise
Risks and opportunities (6.1)	extend	Add information security risk sources; define the assessment method and how it is updated	Assessment of technical threats without expert knowledge
Competence and awareness (7.2, 7.3)	extend	Security training for staff; management training under Section 38 BSIG; attendance records	The specialist training content
Document management (7.5)	reuse	Include security policies, concepts and evidence; control access to confidential documents	Protection of information directly in the IT systems
Suppliers and service providers (8.4)	extend	Security criteria and classification by importance to operations for IT service providers and suppliers; security clauses in contracts	Technical review of service providers
Monitoring and measurement (9.1)	extend	Integrate effectiveness checks such as restore tests and incident analyses	The technical testing methods themselves
Internal audit (9.2)	extend	Add information security audit points; use auditors with security competence	Technical penetration tests
Management review (9.3)	extend	Establish fixed agenda items on information security	The assessment itself—this remains management's task
Corrective action (10.2)	reuse	Include findings from security reviews and incidents	Detection and reporting of incidents
– (to be built new)	new	Detection and assessment of security incidents; reporting process to the BSI under Section 32 BSIG	–
– (to be built new)	new	Emergency and crisis management for the failure of critical IT infrastructure	–

Whether a process is rated *verify* depends on the individual company. The fact that the quality management system is certified does not mean that every process is practiced day to day—the certification audit only checks samples. Three questions help with the assessment: Do internal audits take place as planned? Are corrective actions completed on time? Does management make decisions during its regular review, or does it merely take note of reports?

4.4 The Scope

An ISO 9001 certificate does not necessarily cover the whole company; it can be limited to individual sites, product lines or parts of the business. NIS-2, on the other hand, covers the entire company with all the IT systems it uses for its services. For information security, you therefore cannot simply start from the scope of your quality management system, but must include the whole company from the outset.

4.5 The Worked Example

At Muster Maschinenbau GmbH, the assessment initially produces two findings. First, the ISO 9001 certificate covers only the main plant, not the sales office in the neighboring town, which works with the same ERP system. Second, the production machines are connected directly to the office network. An attack on the ERP system can therefore also bring production to a standstill—the risk analysis must take this into account.

The ransomware risk shows how the existing quality management processes and the new security measures work together. The steps follow the structure of ISO/IEC 27001; the last column shows which quality management process is used.

Step (ISO/IEC 27001)	Muster Maschinenbau GmbH	Quality management process used
1. Assess risks (6.1.2, 8.2)	With external specialist support, the head of IT assesses what a failure of the ERP system would mean—through ransomware, but also through hardware failure or a fire in the server room. The starting point is the list of 47 "elementary threats" (<i>elementare Gefährdungen</i>) that the BSI publishes free of charge. Result: the risk is high. It is recorded in the risk register—the continuously maintained list of all known risks to the company, with assessment, owners and measures.	Risks and opportunities (6.1), <i>extend</i>
2. Decide on risk treatment (6.1.3)	The chosen measure is an offline, immutable backup with regular restore tests. A treatment plan sets owners and deadlines. Management approves the plan and budget and accepts the remaining residual risk.	Management review (9.3), <i>extend</i>
3. Implement measures (8.1, 8.3)	The IT service provider sets up the backup. A work instruction describes what is backed up, how often, and how restoring is tested. The service provider's obligations are set out in the contract.	Suppliers and service providers (8.4), <i>extend</i> ; the backup itself <i>build new</i>
4. Document (7.5)	Risk register, treatment plan, work instruction, contract and test records are managed like other quality management documents.	Document management (7.5), <i>reuse</i>
5. Monitor effectiveness (9.1)	Once a quarter, the ERP system is restored from backup as a test.	Monitoring and measurement (9.1), <i>extend</i>
6. Internal audit (9.2)	The audit plan includes backup as a fixed audit point.	Internal audit (9.2), <i>extend</i>
7. Review and correct (9.3, 10.2)	The test results go into the report to management; a failed test is followed up as a corrective action (Section 8.4).	Management review (9.3), <i>extend</i> ; corrective action (10.2), <i>reuse</i>

The information security policy remains at the top level: it sets objectives and responsibilities but contains no individual measures. The documents from steps 1 to 7 are at the same time the evidence that Section 30 BSIg requires. In addition, the head of IT's sole responsibility is ended: management appoints a person to coordinate information security and decides who reports incidents to the BSI.

5. What Needs to Be Built From Scratch

5.1 The Ten Areas Under Section 30(2) BSIG

While the quality management system provides the overarching management framework, the specialist protective measures must be defined across the ten legal areas of Section 30(2) BSIG. The examples are not a mandatory catalog; which measures are appropriate follows from your risk analysis and the principle of proportionality. All ten areas must be covered—unlike the controls in Annex A of ISO/IEC 27001, none of them can be excluded. The only open questions are how far to go and with which measures.

No.	Legal requirement area (Section 30(2))	What the depth of implementation depends on	Organizational examples	Technical examples
1	Risk analysis & security concepts	Number and criticality of systems; dependence of production on IT	Risk assessment method; security policy; complete asset inventory	Automated inventory and discovery tools
2	Incident handling	Damage potential; availability outside core working hours	Incident response plan with clear escalation and BSI reporting channels	Central logging (SIEM) and anomaly alerting
3	Business continuity & crisis management	Tolerable downtime (RTO) of core processes	Emergency manual, crisis team, defined restart sequence	Network-isolated, immutable backups; regular restore tests
4	Supply chain security	Dependence on external service providers and their system access	Structured register of service providers; contractual security standards	Encrypted, logged and tightly restricted remote access
5	Acquisition, development & maintenance (incl. vulnerability management)	Share of outdated software; OT networking; in-house software development	Binding procurement policy; patch management process	Centrally managed software updates; regular vulnerability scans
6	Assessing the effectiveness of risk management	Complexity of the protective measures implemented	Structured test plan; audit points; meaningful KPIs	Technical verification, configuration audits, restore tests
7	Training & awareness	Entire workforce and specific roles with extended privileges	Target-group-specific training plan; mandatory training for management	E-learning platforms; regular simulated phishing campaigns
8	Cryptography	Protection requirements of the data; extent of mobile and remote work	Policy for sensitive data; controlled key management	Full-disk encryption of laptops; TLS protection of all channels
9	Personnel and access security	Number of privileged accounts; staff turnover	Role-based access model (RBAC); structured offboarding process	IAM systems (identity & access management); separate admin accounts
10	Multi-factor authentication (MFA) & secure communication	Extent of external access; cloud use; emergencies that depend on email	Policy on mandatory MFA; crisis-proof out-of-band communication channel	MFA for all remote and administrator access; encrypted collaboration tools

5.2 Obligations Toward the BSI

Keeping registration data up to date (Section 33 BSIg) and reporting security incidents on time (Section 32 BSIg) have no equivalent in ISO 9001. They require a new organizational anchor—including dedicated deputy arrangements and working access to the BSI portal.

5.3 Where the Competence of the Quality Management System Ends

The quality management system manages processes and administers documents and evidence. Two core tasks absolutely require genuine information security expertise:

1. Sound identification and assessment of cyber risks.
2. The selection, technical configuration and testing of protective measures.

A conventional quality management department cannot judge on its own whether a backup architecture protects against ransomware or whether a VPN connection reflects the current state of the art. This expertise must be built internally or brought in externally (e.g. through specialist consultancy).

6. Roadmap: Three Tracks to Implementation

6.1 Three Tracks Instead of a Rigid Sequence

Because the legal deadlines for incidents and management obligations (Track A) apply immediately, while technical protective measures (Track B) and embedding in the management system (Track C) take months, we work in three parallel tracks:

THE THREE-TRACK IMPLEMENTATION ROADMAP
TRACK A: Immediate legal obligations (week 1 onwards / permanently)
TRACK B: Risk-based protective measures (from month 1 / urgent first)
TRACK C: System maturity & integration (from month 1 / audit & review)

- **Track A (immediate obligations):** BSI reporting process, management training, responsibility for registration data and a provisional security policy.
- **Track B (protective measures):** Asset inventory, risk analysis, prioritized action plan, implementation of technical hardening and emergency plans. Measures against the highest risks come first—in the example company they are in place after about three months; less urgent measures follow step by step.
- **Track C (system maturity):** Internal audits, effectiveness checks and the extended management review to close the PDCA cycle.

7. Effort, Costs and Internal Capacity

7.1 A Realistic Effort Model

Flat price tags for NIS-2 fall short, as companies' starting points vary widely. The effort falls into three pillars:

1. **External support:** Consultancy for the assessment, the risk analysis and extending the quality management system to cover information security.
2. **Technical upgrades:** Investment in hardware and software (MFA, backup isolation, SIEM) and integration work by the IT service provider.
3. **Ongoing operation:** Internal staff time for audits, training and continuous document maintenance.

7.2 Main Cost Drivers

- **Technical maturity:** Are modern security structures already in place, or is there a large backlog?
- **Infrastructure complexity:** Number of sites, networked OT systems in production and the share of outsourced IT (*managed services*).
- **Available expertise:** Does security know-how have to be bought in entirely?

7.3 Where ISO 9001 Noticeably Saves Budget

Because core processes such as document management, internal audits and management review already exist, most of the basic organizational set-up is not needed—provided these processes are actually practiced in day-to-day operations. You can therefore concentrate straight away on the technical and specialist content of information security.

7.4 Example: Internal Effort at Muster Maschinenbau GmbH

Scenario assumptions for the first year

The ranges are assumptions for the fictitious example company—not empirical values and not a target.

Role	Main tasks	Internal effort in the first year	What determines the range
Management	Training, approvals, decisions, regular review	a few days	Number of decisions on investments and priorities
Quality manager	Document management, audit planning, preparing management review	several weeks	Maturity of the quality management system; extent of external support
Head of IT	Inventory, risk assessment, managing measures, coordination with the service provider	several weeks to a few months	Need for technical upgrades; share of outsourced IT
Process owners	Contributing to risk analysis and emergency plans	one to a few days each	Number of critical business processes

Not included: license and purchase costs for technology; fees of the IT service provider for implementation; external consultancy; the cost of certification; replacing outdated systems, such as operating systems that are no longer supported.

8. Evidence, Effectiveness and Management

8.1 The Evidence Register

The evidence register brings the three levels together for each of the ten areas. It documents the rule, the measure implemented, the proof of effectiveness, the person responsible and the next review interval in a compact overview.

Area	Rule (level 1)	Measure (level 2)	Proof of effectiveness (level 3)	Governing process	Responsible	Review interval
No. 3: Backup	Backup policy v2	Daily, network-isolated and immutable backups	Record of the successful ERP restore test	7.5, 9.1, 9.2	Head of IT	Quarterly
No. 2: Security incidents	Incident plan with reporting channel	On-call service; prepared BSI portal access	Record of the half-yearly crisis and reporting exercise	7.5, 9.1	Security coordinator	Half-yearly
No. 10: Authentication	Policy on mandatory MFA	MFA enforced for all remote and admin access	Audit report of the account configuration without exceptions	7.5, 9.2	Head of IT	Annually
No. 4: Supply chain	Supplier policy with minimum standards	Security review of the IT service provider & contract amendment	Annual verification against current audit reports / ISO certificates	8.4, 7.5	Quality manager	Annually

8.2 The Report to Management

To fulfill the duty of oversight under Section 38 BSIG in a verifiable way, management receives a compact quarterly report covering six core points:

1. Significant changes in the threat landscape.
2. Implementation status of the action plan by Tracks A, B and C.
3. Results of technical effectiveness checks and emergency tests.
4. Security incidents that have occurred and any reports to the BSI.
5. Open, critical or overdue measures.
6. Specific proposals for decision (e.g. budget approvals or acceptance of residual risks).

The report is integrated directly into the regular management review.

8.3 What the Duty of Oversight Requires

Regular reports and documented management decisions form the backbone of the evidence that management fulfills its legal duty of oversight under Section 38(1) BSIG. It is not enough to take note of security reports. Management must actively assess the maturity of the measures, decide on necessary investments or policies and consistently insist that known deficiencies are remedied.

For your audit documentation, this means: In addition to the handover of the report, the minutes of the management review must explicitly record management's assessment, its specific decisions, the budgets allocated and the follow-up through to successful completion.

8.4 The Worked Example

At Muster Maschinenbau GmbH, the first practical restore test of the ERP system does not go as planned: the data is complete, but restoring it takes three days instead of the eight hours required by the emergency manual. This finding is recorded as a nonconformity through the existing ISO 9001 corrective action process (clause 10.2).

The next security report to management sets out the gap transparently and compares two technical solutions, including their cost implications. Management chooses a solution, releases the necessary budget and sets a deadline for the repeat test. The following quarterly report documents the successful second test, after which the corrective action is closed. Each of these steps is fully recorded in the minutes of the management review and in the evidence register.

9. ISO/IEC 27001: When Is Formal Certification Worthwhile?

9.1 The Three Levels of Compliance

In the context of NIS-2, three levels must be clearly distinguished:

THREE LEVELS OF COMPLIANCE MATURITY
1. MEETING THE LEGAL OBLIGATIONS (SECTION 30 BSIG) • Mandatory for all entities in scope
2. OPERATING AN ISMS (E.G. UNDER ISO 27001) • Proven framework for meeting obligations in a lasting, structured way
3. ACCREDITED CERTIFICATION (BY TÜV, DEKRA, DQS ETC.) • Voluntary external proof for the market and customers

The law requires **demonstrable fulfilment** of the security requirements. It does not prescribe a management system under a particular standard or an ISO certificate. Extending your existing ISO 9001 system is a fully adequate framework in legal terms—provided the security measures themselves are implemented and effective.

9.2 When Certification Pays Off Commercially

The decision to undergo an ISO/IEC 27001 audit is not a legal decision but a strategic business decision. Three questions point the way:

1. **Do customers or tenders require a certificate?** In B2B tenders and supplier contracts, an ISO 27001 certificate can be a commercial knock-out criterion. *(Automotive suppliers please note: the industry usually requires a TISAX label rather than an ISO 27001 certificate alone.)*
 2. **How much effort goes into B2B security questionnaires?** An accredited certificate significantly shortens extensive due diligence questionnaires (DDQs), but does not replace them. It serves as recognized proof of trust and relieves your IT and sales teams in day-to-day work.
 3. **Does the organization need an external pacemaker?** Annual surveillance audits and recertification every three years force the company to keep security analyses, tests and documents continuously up to date. This effectively prevents implemented measures from "falling asleep".
-

9.3 What Additional Requirements Arise

Formal certification creates additional effort: audit fees of the certification body, effort for pre-audits and specific requirements of ISO/IEC 27001 that go beyond pure NIS-2 compliance:

- **Statement of Applicability (SoA):** A detailed justification for including or excluding each individual control from Annex A of the standard.
 - **Formal risk treatment plan.**
 - **Measurable information security objectives (clause 6.2).**
-

9.4 The Decision Can Mature

The good thing about extending ISO 9001: since both standards share the same Harmonized Structure, hardly any work is lost. When you integrate your security structures into the quality management system, you build up the ISO 27001 requirements along the way. You can safely postpone the decision on an external certification audit—for example until important key customers explicitly ask for it.

10. The Next Step: Initial Evaluation and Assessment

10.1 Orientation Checklist

Use this quick evaluation for an initial assessment within the management team. Rate each topic on all three levels of our evidence model:

Topic / requirement	1. Rule in place?	2. Measure implemented?	3. Effectiveness proven?
BSI registration data (Section 33 BSIG): up to date, responsible person and deputy appointed	☐	☐	☐
Incident reporting (Section 32 BSIG): 24/7 reporting channel and BSI portal access established	☐	☐	☐
Management (Section 38 BSIG): demonstrable training in risk governance completed	☐	☐	☐
Risk analysis: covers all hazards and has a fixed review interval	☐	☐	☐
Backup & business continuity: network-isolated backup with proven restore test	☐	☐	☐
Supply chain governance: security assessment and contract clauses for IT providers	☐	☐	☐
Access protection: multi-factor authentication (MFA) for all remote and admin access	☐	☐	☐
Reporting to management: information security as a fixed item in the management review	☐	☐	☐

(Note: Intervals such as "half-yearly" or "quarterly" are internal planning intervals. The law does not prescribe fixed calendar intervals for the reviews under Section 30 BSIG.)

10.2 Evaluating the Check

A positive picture in this quick evaluation provides initial starting points, but does not yet replace complete evidence. Two reasons are decisive:

1. The orientation questions do not fully cover the ten legal criteria of Section 30(2) BSIG.
 2. A check mark under "implemented" does not yet show whether the protective measure matches the specific risk profile and the state of the art.
-

10.3 The Structured Assessment

The next pragmatic step is a **complete assessment** covering all ten areas of Section 30(2) BSIG.

This assessment:

- Defines the required scope,
- Classifies the existing ISO 9001 processes (*reuse, extend, build new, verify*),
- Uncovers specific gaps at all three evidence levels,
- Leads directly to a prioritized action plan for the three implementation tracks.

Example: Assessment Result at Muster Maschinenbau GmbH

This is what the result of an assessment can look like (fictitious example, extract):

Topic	What we find	What is missing	Evidence required	Who decides	Status after six months
Backup	Daily backup, restore never tested	Offline, immutable backup; regular tests	Test record	Management (budget)	New backup in operation; second test successful after correction
Incident reporting	No defined reporting channel	Responsible person, deputy, availability, templates	Incident plan; record of a reporting exercise	Management (responsibility)	Reporting channel defined; first exercise carried out
Remote access	IT service provider logs in with a password	Multi-factor authentication	Review of accounts without a second factor	Head of IT with service provider	Multi-factor authentication for all remote and administrator access
IT service provider	Selected on price and response time	Security assessment; obligations in the contract	Assessment report; contract annex	Management (contract), quality manager (assessment)	Assessment carried out; contract amended
Sites	Quality certificate only for the main plant; production connected to the office network	Sales office and production network in the risk analysis	Risk register for all sites	Management	Risk analysis for all sites; separation of office and production networks commissioned

Especially for companies with an established quality management system, this phase shows how much of the organizational foundation is already in place—and how leanly NIS-2 can be embedded.

Your next step: NIS-2 Assessment for companies with ISO 9001

- **Scope:** Assessment across all ten areas of Section 30 BSIG and all sites; rating of your quality management processes (*reuse, extend, build new, verify*).
- **Result:** a gap overview as in the example above, a prioritized action plan for the three tracks and a decision paper for your management.
- **Duration:** usually a few weeks, depending on size and number of sites.

Contact

Derek Carson

AI Governance & Information Security

Lead Implementer exams passed for ISO/IEC 27001 & ISO/IEC 42001

Liedeweg 66 · 36093 Künzell (near Fulda), Germany

Email: derek@carson.de

Phone: +49 (0)661 9452622

Web: carson.de/EN

Sources (as of October 19, 2026)

- **BSI:** *NIS-2 in Zahlen* (as of September 30, 2026); BSI scope check (*Betroffenheitsprüfung*).
- **BSIG (BSI Act):** Sections 28, 30, 32, 33, 35, 38, 62 (*gesetze-im-internet.de*, accessed October 19, 2026).
- **German Bundestag:** Government bill, BT-Drs. 21/1501 (September 8, 2025); recommendation for a decision, BT-Drs. 21/2782 (November 12, 2025).
- **Kertos:** *NIS2 Readiness Study 2026* (n = 51, survey period August 3–September 4, 2026).
- **Bitkom:** Study report *Wirtschaftsschutz 2025* (n = 1,002, CATI survey).
- **ENISA:** *NIS Investments 2024* (n = 1,350 organizations in the EU-27).
- **DIN EN ISO 9001:2015-11 & ISO/IEC 27001:2022.**