

NIS-2 auf Basis von ISO 9001 umsetzen

Vom bestehenden QM-System zum wirksamen
Informationssicherheitsmanagement – mit Praxisbeispiel, Fahrplan und
Nachweismodell für den Mittelstand

Derek Carson

KI-Governance & Informationssicherheit
carson.de

Stand: Oktober 2026

Das Wichtigste in Kürze für die Geschäftsführung

Was sofort geklärt werden muss: Sind Ihre Registrierungsdaten beim BSI aktuell, und ist jemand dafür zuständig? Kann Ihr Unternehmen einen erheblichen Sicherheitsvorfall innerhalb von 24 Stunden melden – auch am Wochenende? Hat die Geschäftsführung an einer Schulung teilgenommen? Diese Pflichten gelten bereits.

Was Sie schon haben: Mit ISO 9001 bestehen Dokumentenverwaltung, interne Audits, Korrekturmaßnahmen und die regelmäßige Bewertung durch die Geschäftsführung. Diese Verfahren lassen sich für die Informationssicherheit nutzen – sofern sie im Alltag gelebt werden und auf das ganze Unternehmen ausgeweitet werden.

Wo Sie wahrscheinlich investieren müssen: zuerst in Fachwissen der Informationssicherheit – intern oder von außen. Denn erst eine fachkundige Risikobewertung zeigt, welche Maßnahmen Ihr Unternehmen wirklich braucht und welche nicht; ohne sie investieren Sie leicht an der falschen Stelle. Aus der Risikobewertung ergeben sich dann die technischen Investitionen, typischerweise eine vom Netz getrennte Datensicherung, Mehr-Faktor-Authentifizierung für Fernzugänge, die Erkennung von Vorfällen und gegebenenfalls die Trennung von Büro- und Produktionsnetz.

Was Sie entscheiden müssen: wer die Informationssicherheit koordiniert; welche Risiken zuerst behandelt und welche Restrisiken akzeptiert werden; welches Budget bereitsteht; und ob Sie später eine Zertifizierung nach ISO/IEC 27001 anstreben.

Die nächsten drei Schritte:

1. Meldefähigkeit herstellen und die Geschäftsführung schulen – diese Pflichten gelten sofort.
2. Eine Bestandsaufnahme über alle zehn Bereiche des § 30 BSIG durchführen, einschließlich aller Standorte.
3. Auf dieser Grundlage einen Maßnahmenplan mit Prioritäten beschließen.

1. Zielgruppe und Kernversprechen

Seit dem 6. Dezember 2025 ist das deutsche NIS-2-Umsetzungsgesetz (NIS2UmsuCG / BSIG) ohne Übergangsfrist in Kraft. Die schiere Zahl der Betroffenen ist gewaltig: Zum 30. September 2026 waren beim Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits 20.141 Einrichtungen registriert – darunter 13.252 als „wichtige Einrichtungen“ (BSI, NIS-2 in Zahlen).

Mit der reinen BSI-Registrierung haben Unternehmen jedoch erst eine einzige Anforderung erfüllt (§ 33 BSIG). Die eigentliche gesetzliche Pflicht – das dauerhafte Umsetzen und Belegen wirksamer Sicherheitsmaßnahmen nach § 30 BSIG – besteht unverändert fort.

Wie groß der Nachholbedarf im Mittelstand tatsächlich ist, zeigt eine Befragung von 51 betroffenen Unternehmen aus dem späten Sommer 2026 (Kertos, NIS2 Readiness Study 2026):

- **4 %** der befragten Unternehmen gaben an, die Anforderungen vollständig umzusetzen.
- **18 %** hatten noch nicht einmal mit der Umsetzung begonnen.

(Hinweis zur Einordnung: Da diese Studie von einem Softwareanbieter stammt und die Stichprobe klein ist, dienen diese Werte als Orientierung, nicht als statistischer Repräsentativwert.)

Für wen dieser Leitfaden geschrieben ist

Dieser Leitfaden richtet sich gezielt an die **Geschäftsführung** und **QM-Verantwortliche** in Unternehmen, auf die drei Kriterien zutreffen:

1. Das Unternehmen fällt rechtlich unter den Anwendungsbereich von NIS-2.
2. Es betreibt bereits ein zertifiziertes Qualitätsmanagementsystem nach **ISO 9001**.
3. Es verfügt bisher über **kein** verankertes Informationssicherheits-Managementsystem (ISMS nach ISO/IEC 27001).

Die zentrale These

Wer ein funktionierendes ISO-9001-System hat, muss den organisatorischen Rahmen für NIS-2 nicht neu aufbauen. Er erweitert das bestehende System und setzt Budget und Fachwissen dort ein, wo NIS-2 tatsächlich Neues verlangt: bei den Sicherheitsmaßnahmen.

Im Vergleich zu einem eigenständigen Informationssicherheits-Managementsystem, das neben dem QM-System aufgebaut wird, hat dieser Weg vier Vorteile:

- **Ihr Budget fließt in die Sicherheit, nicht in die Organisation.** Dokumentenverwaltung, interne Audits, Korrekturmaßnahmen und die regelmäßige Bewertung durch die Geschäftsführung bestehen bereits. Ein eigenständiges System müsste diese Verfahren ein zweites Mal aufbauen. Die Arbeit beginnt deshalb gleich bei den Sicherheitsmaßnahmen. (Abschnitte 4 und 7)
- **Die Geschäftsführung überwacht die Informationssicherheit in einem Ablauf, den sie schon kennt.** Nach § 38 BSIG muss die Geschäftsführung dafür sorgen, dass die Sicherheitsmaßnahmen umgesetzt werden, und die Umsetzung überwachen. Die regelmäßige Bewertung im QM-System bietet dafür einen festen, dokumentierten Termin. Ein eigenständiges System bräuchte einen neuen. (Abschnitt 8)
- **Ein System statt zwei.** Beschäftigte, Auditoren und Geschäftsführung arbeiten mit einem Satz von Abläufen und einem Auditprogramm. Doppelte Dokumente und doppelte Audits entfallen.
- **Der Weg zur Zertifizierung bleibt offen.** ISO 9001 und ISO/IEC 27001 haben dieselbe Grundstruktur. Verlangt ein Kunde später ein Zertifikat nach ISO/IEC 27001, erweitern Sie das System ein weiteres Mal, statt es neu aufzubauen. (Abschnitt 9)

Die klare Grenze dieses Ansatzes: Ein QM-System ersetzt keine technischen oder IT-spezifischen Sicherheitsmaßnahmen. Die fachlichen Schutzmechanismen der Informationssicherheit müssen Sie gezielt aufbauen. ISO 9001 liefert dafür jedoch einen geeigneten organisatorischen Rahmen.

Welche Fragen dieser Leitfaden beantwortet

1. Was müssen Sie sofort tun, und welche Fristen gelten? *(Abschnitt 2)*
2. Woran erkennen Sie, ob eine Anforderung tatsächlich erfüllt ist – und nicht nur auf dem Papier? *(Abschnitt 2)*
3. Welche Ihrer QM-Prozesse können Sie weiterverwenden, und wo reicht das QM-System nicht aus? *(Abschnitt 4)*
4. Welche Sicherheitsmaßnahmen müssen Sie neu aufbauen? *(Abschnitt 5)*
5. In welcher Reihenfolge gehen Sie vor? *(Abschnitt 6)*
6. Mit welchem Aufwand müssen Sie rechnen, und wovon hängt er ab? *(Abschnitt 7)*
7. Wie belegen Sie die Umsetzung, und wie behält die Geschäftsführung den Überblick? *(Abschnitt 8)*

Durchgängiges Praxisbeispiel

Um die Theorie greifbar zu machen, begleitet ein durchgehendes Szenario alle Abschnitte:

Muster Maschinenbau GmbH

- **Struktur:** 180 Beschäftigte, seit Jahren nach ISO 9001 zertifiziert.
- **IT-Setup:** Ein interner IT-Leiter in Kombination mit einem externen IT-Systemhaus.
- **NIS-2-Status:** Beim BSI als „wichtige Einrichtung“ registriert.
- **Leitszenario:** Ein Ransomware-Angriff könnte das zentrale ERP-System verschlüsseln; die Angreifer würden Lösegeld fordern. Eingetreten ist ein solcher Angriff bisher nicht. Wir verfolgen durch alle Abschnitte, wie sich das Unternehmen gegen dieses Risiko absichert.

Kasten: Sind Sie wirklich betroffen? (Schnellcheck)

Für eine erste Orientierung genügen drei Kernfragen *(Hinweis: Dies ersetzt keine Rechtsberatung, da für Spezialsektoren wie KRITIS Sonderregeln gelten)*:

1. **Sektor:** Gehört Ihr Unternehmen zu einem Sektor gemäß Anlage 1 oder Anlage 2 des BSI (z. B. Maschinenbau, Chemie, Lebensmittel, Energie, Logistik)?
2. **Größe:** Beschäftigt Ihr Unternehmen **mindestens 50 Mitarbeiter** oder erwirtschaftet es **mehr als 10 Mio. € Jahresumsatz** bei gleichzeitig **über 10 Mio. € Bilanzsumme**?
(Wichtig: Wird dieser Schwellenwert überschritten, gilt die Einstufung für das gesamte Unternehmen – nicht nur für die betroffene Sparte.)
3. **Sonderkonstellation:** Greifen Ausnahmen für vernachlässigbare Nebentätigkeiten (§ 28 Abs. 3 BSI) oder Konzernverflechtungen (§ 28 Abs. 4 BSI)?

Praxistipp: Nutzen Sie für die Erstprüfung den Betroffenen-Check des BSI. Dokumentieren Sie das Ergebnis explizit in Ihren Akten – auch wenn es „nicht betroffen“ lautet. Nur so können Sie bei späteren Behördenanfragen belegen, dass Sie die Frage geprüft haben.

2. Die gesetzlichen Anforderungen im Detail

Das BSIG unterscheidet zwei Grundtypen von Pflichten: **Pflichten, die ab sofort gelten**, und **dauerhafte Risikomanagement-Pflichten**, die ein fortlaufendes Handeln erfordern.

2A. Pflichten, die ab sofort gelten

Diese Pflichten dulden keinen Aufschub und dürfen nicht in spätere Projektphasen verschoben werden. Die fünf wichtigsten:

1. Registrierung und Stammdaten-Aktualisierung (§ 33 BSIG):

Die Registrierung beim BSI war binnen drei Monaten fällig, nachdem Ihr Unternehmen unter NIS-2 fiel – für die meisten Unternehmen also bis zum 6. März 2026; dieser Leitfaden geht davon aus, dass sie erfolgt ist. Seitdem gilt: Änderungen bei Unternehmensdaten, Anschriften oder Sicherheitsansprechpartnern müssen Sie dem BSI **unverzüglich** melden – spätestens innerhalb von **zwei Wochen**. In Ihrem Unternehmen muss daher eine Rolle explizit für diese Datenpflege benannt sein.

2. Meldepflicht bei Sicherheitsvorfällen (§ 32 BSIG):

Sobald Sie Kenntnis von einem „erheblichen Sicherheitsvorfall“ erlangen, müssen Sie ihn in mehreren Stufen an die gemeinsame Meldestelle von BSI und BBK melden (über das BSI-Portal). Grundsätzlich gilt: so schnell wie möglich. Das Gesetz setzt dafür Höchstfristen:

- **Innerhalb von 24 Stunden nach Entdeckung des Vorfalls:** Abgabe einer *frühen Erstmeldung* (Verdacht auf rechtswidrige oder böswillige Handlung, mögliche grenzüberschreitende Auswirkung).
- **Innerhalb von 72 Stunden nach Entdeckung:** Formale *Meldung* mit Erstbewertung und technischen Indikatoren (IoCs).
- **Auf Ersuchen des BSI:** *Zwischenmeldung* zum aktuellen Stand.
- **Innerhalb eines Monats nach der Meldung:** Einreichen der *Abschlussmeldung* mit Ursachenanalyse und Behebung (dauert der Vorfall noch an, zunächst eine *Fortschrittmeldung*).

Wichtig: Die Uhr tickt ab dem Moment der ersten Kenntnisnahme – nicht erst, wenn Ihre IT die Ursache analysiert hat. Da die Fristen auch am Wochenende laufen, muss die Meldefähigkeit rund um die Uhr (24/7) sichergestellt sein.

Die Bewältigung des Vorfalls selbst – erkennen, eindämmen, wiederherstellen – gehört dagegen zu den Sicherheitsmaßnahmen nach § 30 BSIG (Abschnitt 2B).

3. Unterrichtung Ihrer Kunden auf Anordnung (§ 35 BSIG):

Ordnet das BSI es an, müssen Sie die Empfänger Ihrer Dienste unverzüglich über einen erheblichen Sicherheitsvorfall informieren, der Ihre Leistung beeinträchtigen kann.

4. Umsetzung und Überwachung durch die Geschäftsführung (§ 38 Abs. 1 und 2 BSIG):

Die Geschäftsführung muss die Risikomaßnahmen nicht nur absegnen, sondern deren Umsetzung **aktiv überwachen**. Bei schuldhaften Pflichtverletzungen haftet sie dem Unternehmen gegenüber für den entstandenen Schaden nach den Regeln des Gesellschaftsrechts.

5. Schulung der Geschäftsführung (§ 38 Abs. 3 BSIG):

Die Geschäftsführung muss regelmäßig an Schulungen teilnehmen, damit sie Risiken der Informationssicherheit erkennen und bewerten kann.

Darüber hinaus gibt es weitere Pflichten, etwa die Mitwirkung, wenn das BSI Aufsichtsmaßnahmen ergreift (§ 62 BSIG).

2B. Die Pflicht zu wirksamen Maßnahmen (§ 30 BSIG)

Paragraph 30 BSIG verpflichtet Sie zu „geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen“ zum Schutz von Verfügbarkeit, Integrität und Vertraulichkeit Ihrer IT-Systeme. Die fünf wichtigsten Anforderungen:

1. **Risikoanalyse als Grundlage:** Welche Maßnahmen geeignet und verhältnismäßig sind, ergibt sich aus den Risiken Ihres Unternehmens (§ 30 Abs. 2 Nr. 1).
2. **Zehn vorgegebene Bereiche:** Das Gesetz nennt zehn konkrete Bereiche, die Ihre Maßnahmen abdecken müssen – darunter die Bewältigung von Sicherheitsvorfällen, Datensicherung und Notfallmanagement sowie die Sicherheit der Lieferkette (§ 30 Abs. 2; alle zehn in Abschnitt 5).
3. **Alle Gefahren berücksichtigen:** Neben Cyberangriffen sind auch Ereignisse wie Stromausfälle, Hitzewellen, Brand, Wasser oder menschliches Versagen zu berücksichtigen (§ 30 Abs. 2).
4. **Wirksamkeit prüfen:** Sie brauchen Verfahren, mit denen Sie bewerten, ob Ihre Maßnahmen wirken (§ 30 Abs. 2 Nr. 6).
5. **Nachweis:** Sie müssen dokumentieren, wie Sie diese Anforderungen erfüllen (§ 30 Abs. 1).

Darüber hinaus gibt es weitere Anforderungen, etwa die Orientierung am Stand der Technik und an einschlägigen Normen (§ 30 Abs. 2).

Das 3-Ebenen-Nachweismodell

Um die gesetzlichen Anforderungen auditfest zu dokumentieren, nutzen wir ein dreistufiges Nachweisraster:

DAS 3-EBENEN-NACHWEISMODELL	
1. DIE REGEL	Was ist verbindlich vorgegeben? (z. B. Backup- und Restore-Richtlinie)
2. DIE MAßNAHME	Was ist technisch/organisatorisch umgesetzt? (z. B. Tägliches, isoliertes Immutable Backup)
3. DER WIRKSAMKEITSNACHWEIS	Was beweist die tatsächliche Funktion? (z. B. Protokoll des letzten Wiederherstell-Tests)

Der Merksatz:

Eine Richtlinie ohne technische Umsetzung ist wirkungslos. Eine technische Umsetzung ohne Wirksamkeitsnachweis ist nicht belegt.

Warum NIS-2 kein „Einmal-Projekt“ ist

Risikomanagement nach § 30 BSIG lässt sich nicht einmalig abarbeiten und abheften. Vier gesetzliche Gründe erzwingen einen kontinuierlichen Kreislauf:

- **Ausrichtung am Risiko:** Schutzmaßnahmen müssen exakt zum identifizierten Risiko passen.
- **Dynamische Bedrohungslage:** Neue Angriffsvektoren und IT-Systeme verändern das Risikoprofil ständig.
- **Wirksamkeitsprüfung (§ 30 Abs. 2 Nr. 6 BSIG):** Ob ein Schutzmechanismus wirkt, zeigt erst die Prüfung.
- **Überwachungspflicht (§ 38 BSIG):** Die Geschäftsführung muss fortlaufend über den Sicherheitsstatus informiert werden.

Dieses Zusammenspiel ergibt einen klassischen Steuerungskreislauf (**Plan-Do-Check-Act**), wie ihn Ihre QM-Abteilung aus der ISO 9001 seit Jahren kennt.

3. Typische Lücken in der Praxis

Dass vielerorts Handlungsbedarf besteht, zeigen aktuelle Zahlen:

- **39 %** der deutschen Unternehmen besitzen kein Notfallmanagement für Spionage, Sabotage oder Datendiebstahl (*Bitkom, Wirtschaftsschutz 2025*).
- **20 %** verzichten völlig auf IT-Sicherheitsschulungen für ihre Mitarbeiter (*Bitkom 2025*).
- In **63 %** der NIS-2-relevanten Betriebe liegt die Sicherheitsthematik bei der IT-Leitung, aber nur in **22 %** direkt bei der Geschäftsleitung (*Kertos 2026*).
- **84 %** verfügen über keinen ausgewiesenen Informationssicherheitsbeauftragten (CISO) – weder intern noch extern (*Kertos 2026*).

Wo die Muster Maschinenbau GmbH heute steht

Unser Praxisunternehmen spiegelt diese Realität wider:

1. **Regel-Ebene:** Die IT-Sicherheitsrichtlinie stammt unverändert aus dem Jahr 2019.
2. **Maßnahmen-Ebene:** Es existieren zwar tägliche Datensicherungen, doch der externe IT-Dienstleister wurde rein nach Stundensatz und Reaktionszeit ausgewählt – ohne seine eigenen Sicherheitsvorkehrungen zu prüfen.
3. **Wirksamkeits-Ebene:** Eine vollständige System-Wiederherstellung (Restore-Test) des zentralen ERP-Systems aus dem Backup wurde **noch nie** praktisch durchgespielt.

Hinzu kommt eine vierte Lücke, die zu keiner der drei Ebenen gehört: Für alle Sicherheitsfragen ist allein der IT-Leiter zuständig. Wie sich das beheben lässt, zeigt Abschnitt 4.

Hinter solchen Lücken stehen meist mehrere Ursachen, die sich gegenseitig verstärken. Häufig wurden Sicherheitsmaßnahmen in der Vergangenheit als einmalige Projekte umgesetzt – ohne feste Verantwortliche, ohne festgelegte Prüfintervalle und ohne ordentliche Verwaltung der zugehörigen Dokumente. Hinzu kommt ein organisatorisches Risiko, das unser Beispielunternehmen zeigt: Liegt die Zuständigkeit allein bei der IT-Leitung, sind technischer Betrieb, Risikobewertung, unternehmensweite Priorisierung und der Bericht an die Geschäftsleitung womöglich nicht ausreichend miteinander verbunden. Ob diese Lücke tatsächlich besteht, muss die Bestandsaufnahme zeigen. Häufig kommen zudem knappe Budgets sowie fehlendes Fachwissen im Bereich der Informationssicherheit hinzu.

Daraus folgt, dass in solchen Unternehmen zwei Dinge fehlen: erstens ein wiederkehrender Ablauf, der die Maßnahmen dauerhaft aktuell und wirksam hält, und zweitens das Fachwissen, mit dem sich angemessene Maßnahmen gegen konkrete Risiken bestimmen lassen. Abschnitt 4 zeigt, dass ein bestehendes ISO-9001-System den ersten Punkt bereits in großen Teilen mitbringt. Abschnitt 5 zeigt, dass das Fachwissen gezielt aufgebaut werden muss.

4. Was das ISO-9001-System mitbringt – und was nicht

4.1 Der vorhandene Ablauf

Ein nach ISO 9001 zertifiziertes Unternehmen unterhält bereits eine Reihe verbindlicher Prozesse, die dem wiederkehrenden Ablauf aus Abschnitt 2 entsprechen – bislang allerdings mit dem Schwerpunkt Qualität statt Informationssicherheit. Dazu gehören festgelegte Rollen und Verantwortlichkeiten (Abschnitt 5.3 der Norm), der Umgang mit Risiken und Chancen (6.1), die Schulung und Sensibilisierung der Beschäftigten (7.2 und 7.3), die Verwaltung und Freigabe von Dokumenten (7.5), die Steuerung von Lieferanten und Dienstleistern (8.4), Überwachung und Messung (9.1), das interne Audit (9.2), die regelmäßige Bewertung durch die Geschäftsführung (9.3) sowie der Korrekturprozess (10.2).

ISO 9001 und ISO/IEC 27001 (die Norm für Informationssicherheits-Managementsysteme) folgen derselben Grundstruktur und gliedern ihre Anforderungen in die Kapitel 4 bis 10 mit identischen Überschriften. Das bedeutet: Ein Unternehmen mit einem funktionierenden ISO-9001-System kann seine bestehenden Prozesse auf die Informationssicherheit ausdehnen, anstatt parallel ein zweites System aufzubauen.

4.2 Die entscheidende Unterscheidung: gleiche Methode, anderer Gegenstand

Auch das QM-System bewertet Risiken und trifft Maßnahmen. Methode und Ablauf sind dieselben wie in der Informationssicherheit. Der Unterschied liegt allein im Gegenstand: Das QM-System verringert Qualitätsrisiken, die Informationssicherheit dagegen Risiken für die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen. Deshalb lassen sich die vorhandenen Abläufe auch für die Informationssicherheit nutzen.

Für das Unternehmen ergeben sich daraus drei Vorteile. Erstens lassen sich bestehende Verfahren für die Dokumentenverwaltung, interne Audits, Korrekturmaßnahmen und die Bewertung durch die Geschäftsführung auch für die Informationssicherheit nutzen. Das QM-System muss dafür nicht neu aufgebaut, sondern gezielt erweitert werden, damit es auch informationssicherheitsbezogene Risiken und Anforderungen abdeckt.

Zweitens sind die dafür nötigen Rollen und Erfahrungen bereits vorhanden. Die QM-Leitung kann die Dokumentation, die Auditplanung, die Vorbereitung der Bewertung durch die Geschäftsführung und die Nachverfolgung von Korrekturmaßnahmen koordinieren. Die fachliche Verantwortung für die Informationssicherheit ersetzt sie damit jedoch nicht: Risikobewertungen, die Auswahl geeigneter Sicherheitsmaßnahmen und die Prüfung ihrer Wirksamkeit erfordern entsprechende Fachkenntnisse – intern oder durch externe Unterstützung.

Drittens – und das ist der größte Vorteil – gibt es den Kreislauf bereits: Maßnahmen werden geplant, im internen Audit geprüft, von der Geschäftsführung bewertet und bei Bedarf nachverfolgt. Informationssicherheit wird dadurch nicht zu einem einmaligen Projekt, sondern zu einer wiederkehrenden Führungsaufgabe. Genau diese kontinuierliche Steuerung fehlt häufig, wenn Informationssicherheit vor allem als technische Aufgabe der IT behandelt wird (siehe Abschnitt 3).

4.3 Welche Prozesse sich wie verwenden lassen

Für jeden QM-Prozess stellt sich die Frage, wie er für die Informationssicherheit genutzt werden kann. Es gibt vier Möglichkeiten:

- **wiederverwenden:** Der Prozess kann nach Prüfung seiner Eignung unverändert genutzt werden; es kommen lediglich die neuen Inhalte der Informationssicherheit hinzu.
- **erweitern:** Der Prozess muss gezielt um spezifische Anforderungen der Informationssicherheit ergänzt werden.
- **neu aufbauen:** Die erforderliche Fähigkeit fehlt ganz oder weitgehend und muss etabliert werden – meist, weil ISO 9001 sie schlicht nicht fordert.
- **prüfen:** Der Prozess ist zwar dokumentiert, vor der Weiternutzung ist jedoch kritisch zu hinterfragen, ob er im Betrieb tatsächlich gelebt wird.

QM-Prozess (ISO 9001)	Einstufung	Was sich ändert	Was der Prozess nicht leistet
Rollen und Verantwortlichkeiten (5.3)	erweitern	Zuständigkeit für Informationssicherheit, für Registrierungsdaten und für BSI-Meldungen festlegen	Fachwissen der Informationssicherheit

QM-Prozess (ISO 9001)	Einstufung	Was sich ändert	Was der Prozess nicht leistet
Risiken und Chancen (6.1)	erweitern	Risikoquellen der Informationssicherheit aufnehmen; Bewertungsmethode und Fortschreibung definieren	Bewertung technischer Bedrohungen ohne Expertenwissen
Schulung und Sensibilisierung (7.2, 7.3)	erweitern	Sicherheitsschulungen für die Belegschaft; Schulung der Geschäftsleitung nach § 38 BSIg; Teilnahmenachweise	Die fachlichen Schulungsinhalte
Dokumentenverwaltung (7.5)	wiederverwenden	Sicherheitsrichtlinien, Konzepte und Nachweise aufnehmen; Zugriff auf vertrauliche Dokumente regeln	Schutz der Informationen direkt in den IT-Systemen
Lieferanten und Dienstleister (8.4)	erweitern	Sicherheitskriterien und Einstufung nach Bedeutung für den Betrieb für IT-Dienstleister und Zulieferer; Sicherheitsklauseln in Verträgen	Technische Prüfung der Dienstleister
Überwachung und Messung (9.1)	erweitern	Wirksamkeitsprüfungen wie Wiederherstellungstests und Auswertungen von Vorfällen integrieren	Die technischen Prüfmethode selbst
Internes Audit (9.2)	erweitern	Prüfpunkte für Informationssicherheit ergänzen; Auditoren mit Sicherheitskompetenz einsetzen	Technische Sicherheits-Penetrationstests
Bewertung durch die Geschäftsführung (9.3)	erweitern	Feste Tagesordnungspunkte zur Informationssicherheit etablieren	Die inhaltliche Bewertung – sie bleibt Aufgabe der Geschäftsführung
Korrekturmaßnahmen (10.2)	wiederverwenden	Befunde aus Sicherheitsprüfungen und Vorfällen aufnehmen	Erkennung und Meldung von Vorfällen
– (Neu aufzubauen)	neu	Erkennung und Bewertung von Sicherheitsvorfällen; Meldeprozess an das BSI nach § 32 BSIg	–
– (Neu aufzubauen)	neu	Notfall- und Krisenmanagement für den Ausfall kritischer IT-Infrastruktur	–

Ob ein Prozess die Einstufung *prüfen* bekommt, hängt vom einzelnen Unternehmen ab. Dass das QM-System zertifiziert ist, heißt nicht, dass jeder Prozess im Alltag gelebt wird – das Zertifizierungsaudit prüft nur Stichproben. Drei Fragen helfen bei der Einschätzung: Finden die internen Audits planmäßig statt? Werden Korrekturmaßnahmen termingerecht abgeschlossen? Trifft die Geschäftsführung bei ihrer regelmäßigen Bewertung Entscheidungen, oder nimmt sie Berichte nur zur Kenntnis?

4.4 Der Geltungsbereich (Scope)

Ein ISO-9001-Zertifikat gilt nicht unbedingt für das ganze Unternehmen; es kann auf einzelne Standorte, Produktlinien oder Teilbereiche begrenzt sein. NIS-2 erfasst dagegen das gesamte Unternehmen mit allen IT-Systemen, die es für seine Dienste nutzt. Sie können für die Informationssicherheit deshalb nicht einfach vom Geltungsbereich Ihres QM-Systems ausgehen, sondern müssen von Anfang an das ganze Unternehmen einbeziehen.

4.5 Das Praxisbeispiel

Bei der Muster Maschinenbau GmbH ergibt die Bestandsaufnahme zunächst zwei Befunde. Erstens gilt das ISO-9001-Zertifikat nur für das Hauptwerk, nicht für das Vertriebsbüro in der Nachbarstadt, das mit demselben ERP-System arbeitet. Zweitens sind die Fertigungsmaschinen direkt mit dem Büronetz verbunden. Ein Angriff auf das ERP-System kann deshalb auch die Produktion stilllegen – die Risikoanalyse muss das berücksichtigen.

Wie die vorhandenen QM-Prozesse und die neuen Sicherheitsmaßnahmen zusammenwirken, zeigt das Ransomware-Risiko. Die Schritte folgen dem Aufbau von ISO/IEC 27001; die letzte Spalte zeigt, welcher QM-Prozess dafür genutzt wird.

Schritt (ISO/IEC 27001)	Muster Maschinenbau GmbH	Genutzter QM-Prozess
1. Risiken einschätzen (6.1.2, 8.2)	Der IT-Leiter bewertet mit externer fachlicher Unterstützung, was ein Ausfall des ERP-Systems bedeuten würde – durch Ransomware, aber auch durch Hardwaredefekt oder Brand im Serverraum. Als Ausgangspunkt dient die Liste der 47 „elementaren Gefährdungen“, die das BSI kostenlos veröffentlicht. Ergebnis: Das Risiko ist hoch. Es wird im Risikoregister erfasst – der laufend gepflegten Liste aller bekannten Risiken des Unternehmens mit Bewertung, Verantwortlichen und Maßnahmen.	Risiken und Chancen (6.1), <i>erweitern</i>

Schritt (ISO/IEC 27001)	Muster Maschinenbau GmbH	Genutzter QM-Prozess
2. Risikobehandlung festlegen (6.1.3)	Als Maßnahme wird eine vom Netz getrennte, nicht veränderbare Sicherung mit regelmäßigen Wiederherstellungstests gewählt. Ein Behandlungsplan legt Verantwortliche und Termine fest. Die Geschäftsführung genehmigt Plan und Budget und akzeptiert das verbleibende Restrisiko.	Bewertung durch die Geschäftsführung (9.3), <i>erweitern</i>
3. Maßnahmen umsetzen (8.1, 8.3)	Der IT-Dienstleister richtet die Sicherung ein. Eine Verfahrensanweisung beschreibt, was wie oft gesichert und wie die Wiederherstellung getestet wird. Die Pflichten des Dienstleisters stehen im Vertrag.	Lieferanten und Dienstleister (8.4), <i>erweitern</i> ; Sicherung selbst <i>neu aufbauen</i>
4. Dokumentieren (7.5)	Risikoregister, Behandlungsplan, Verfahrensanweisung, Vertrag und Testprotokolle werden wie andere QM-Dokumente verwaltet.	Dokumentenverwaltung (7.5), <i>wiederverwenden</i>
5. Wirksamkeit überwachen (9.1)	Einmal im Quartal wird das ERP-System testweise aus der Sicherung wiederhergestellt.	Überwachung und Messung (9.1), <i>erweitern</i>
6. Internes Audit (9.2)	Der Auditplan enthält die Datensicherung als festen Prüfpunkt.	Internes Audit (9.2), <i>erweitern</i>
7. Bewerten und korrigieren (9.3, 10.2)	Die Testergebnisse gehen in den Bericht an die Geschäftsführung; ein fehlgeschlagener Test wird als Korrekturmaßnahme verfolgt (Abschnitt 8.4).	Bewertung durch die Geschäftsführung (9.3), <i>erweitern</i> ; Korrekturmaßnahmen (10.2), <i>wiederverwenden</i>

Die Informationssicherheitsleitlinie bleibt dabei übergeordnet: Sie legt Ziele und Verantwortlichkeiten fest, enthält aber keine einzelnen Maßnahmen. Die Unterlagen aus den Schritten 1 bis 7 sind zugleich der Nachweis, den § 30 BSIG verlangt. Außerdem wird die alleinige Zuständigkeit des IT-Leiters aufgelöst: Die Geschäftsführung benennt eine Person, die die Informationssicherheit koordiniert, und legt fest, wer Vorfälle an das BSI meldet.

5. Was neu aufgebaut werden muss

5.1 Die zehn Bereiche nach § 30 Abs. 2 BSIG

Während das QM-System den übergeordneten Steuerungsrahmen liefert, müssen die fachlichen Schutzmaßnahmen über die zehn gesetzlichen Bereiche des § 30 Abs. 2 BSIG konkretisiert werden. Die Beispiele sind kein Pflichtkatalog: Welche Maßnahmen angemessen sind, ergibt sich aus Ihrer Risikoanalyse und dem Grundsatz der Verhältnismäßigkeit. Alle zehn Bereiche müssen abgedeckt werden – anders als bei den Maßnahmen in Anhang A von ISO/IEC 27001 lässt sich keiner davon ausschließen. Offen ist nur, wie tief und mit welchen Maßnahmen.

Nr.	Gesetzlicher Anforderungsbereich (§ 30 Abs. 2)	Wovon die Umsetzungstiefe abhängt	Organisatorische Beispiele	Technische Beispiele
1	Risikoanalyse & Sicherheitskonzepte	Zahl und Kritikalität der Systeme; Produktionsabhängigkeit von der IT	Risikobewertungsmethode; Sicherheitsrichtlinie; lückenloses Asset-Inventar	Automatisierte Inventarisierungs- und Discovery-Tools
2	Bewältigung von Sicherheitsvorfällen	Schadenspotenzial; Erreichbarkeit außerhalb der Kernarbeitszeiten	Incident-Response-Plan mit klaren Eskalationen und BSI-Meldewegen	Zentrales Logging (SIEM) und Anomalie-Alarmierung
3	Betriebskontinuität & Notfallmanagement	Tolerierbare Ausfallzeit (RTO) der Kernprozesse	Notfallhandbuch, Krisenstab, definierte Wiederanlauf-Reihenfolge	Netzisierte, unveränderbare Backups (Immutable Storage); regelmäßige Restore-Tests
4	Lieferkettensicherheit	Abhängigkeit von externen Dienstleistern und deren Systemzugriffen	Strukturiertes Dienstleister-Verzeichnis; vertragliche Sicherheitsstandards	Verschlüsselte, protokollierte und restriktiv begrenzte Remote-Zugänge
5	Beschaffung, Entwicklung & Wartung (inkl. Schwachstellenmanagement)	Anteil veralteter Software; OT-Vernetzung; eigene Software-Entwicklung	Verbindliche Beschaffungsrichtlinie; Patch-Management-Prozess	Zentral gesteuerte Software-Updates; regelmäßige Vulnerability Scans
6	Wirksamkeitsbewertung des Risikomanagements	Komplexität der implementierten Schutzmaßnahmen	Strukturierter Prüfplan; Audit-Prüfpunkte; aussagekräftige KPIs	Technische Verifikationen, Konfigurations-Audits, Wiederherstellungstests
7	Schulung & Sensibilisierung	Gesamtbelegschaft und spezifische Rollen mit erweiterten Rechten	Zielgruppenspezifischer Schulungsplan; Pflichtschulung der Geschäftsleitung	E-Learning-Plattformen; regelmäßige, simulierte Phishing-Kampagnen
8	Kryptografische Verfahren	Schutzbedarf der Daten; Grad der mobilen und dezentralen Arbeit	Richtlinie für schutzbedürftige Daten; geregelte Schlüsselverwaltung	Vollverschlüsselung von Notebooks; TLS-Absicherung aller Kanäle
9	Personal- und Zugriffssicherheit	Anzahl privilegierter Konten; Mitarbeiterfluktuation	Rollenbasiertes Berechtigungsmodell (RBAC); strukturierter Offboarding-Prozess	IAM-Systeme (Identity & Access Management); getrennte Admin-Konten
10	Multi-Faktor-Authentifizierung (MFA) & sichere Kommunikation	Umfang externer Zugriffe; Cloud-Nutzung; E-Mail-abhängige Notfälle	Richtlinie für verbindliche MFA; krisenfester Out-of-Band-Kommunikationskanal	MFA für alle Fern- und Administratorzugänge; verschlüsselte Kollaborationstools

5.2 Pflichten gegenüber dem BSI

Die laufende Aktualisierung der Stammdaten (§ 33 BSIG) und die fristgerechte Meldung von Sicherheitsvorfällen (§ 32 BSIG) besitzen kein Äquivalent in ISO 9001. Sie erfordern eine neue organisatorische Verankerung – inklusive dedizierter Vertretungsregelungen und eines funktionierenden BSI-Portalzugangs.

5.3 Wo die Kompetenz des QM-Systems endet

Das QM-System steuert Prozesse und verwaltet Dokumente und Nachweise. Zwei Kernaufgaben erfordern zwingend echtes Informationssicherheits-Fachwissen:

1. Die fundierte Identifikation und Bewertung von Cyber-Risiken.
2. Die Auswahl, technische Konfiguration und Überprüfung von Schutzmaßnahmen.

Eine klassische QM-Abteilung kann nicht aus eigener Kraft beurteilen, ob eine Backup-Architektur vor Ransomware schützt oder ob ein VPN-Zugang dem aktuellen Stand der Technik entspricht. Dieses Fachwissen muss intern aufgebaut oder extern (z. B. durch spezialisierte Beratung) eingebunden werden.

6. Fahrplan: Drei Spuren zur Umsetzung

6.1 Drei Spuren statt starrer Linearität

Da die gesetzlichen Fristen für Vorfälle und Geschäftsführungspflichten (Spur A) sofort greifen, während technische Schutzmaßnahmen (Spur B) und die Verankerung im Managementsystem (Spur C) Monate beanspruchen, arbeiten wir in drei parallelen Spuren:

DER 3-SPUREN-UMSETZUNGSFAHRPLAN
SPUR A: Gesetzliche Sofortpflichten (Woche 1 ff. / Dauerhaft aktiv)
SPUR B: Risikobasierte Schutzmaßnahmen (ab Monat 1 / Dringendes zuerst)
SPUR C: Systemreife & Integration (ab Monat 1 / Audit & Review)

- **Spur A (Sofortpflichten):** BSI-Meldeprozess, Schulung der Geschäftsleitung, Stammdaten-Verantwortung und vorläufige Sicherheitsleitlinie.
- **Spur B (Schutzmaßnahmen):** Asset-Inventar, Risikoanalyse, priorisierter Maßnahmenplan, Umsetzung technischer Härtungen und Notfallpläne. Die Maßnahmen gegen die höchsten Risiken kommen zuerst – im Beispielunternehmen stehen sie nach etwa drei Monaten; weniger dringende Maßnahmen folgen nach und nach.
- **Spur C (Systemreife):** Interne Audits, Wirksamkeitsprüfungen und die erweiterte Bewertung durch die Geschäftsführung zur Schließung des PDCA-Zyklus.

7. Aufwand, Kosten und interne Kapazitäten

7.1 Ein realistisches Aufwandsmodell

Pauschale Preisschilder für NIS-2 greifen zu kurz, da die Ausgangslage der Unternehmen stark variiert. Der Aufwand teilt sich in drei Säulen:

1. **Externe Begleitung:** Beratung für Bestandsaufnahme, Risikoanalyse und die Erweiterung des QM-Systems um die Informationssicherheit.
2. **Technische Nachrüstung:** Investitionen in Hardware/Software (MFA, Backup-Isolation, SIEM) sowie Integrationsleistungen des IT-Dienstleisters.
3. **Laufender Betrieb:** Interner Personalaufwand für Audits, Schulungen und die kontinuierliche Dokumentenpflege.

7.2 Wesentliche Kostentreiber

- **Technischer Reifegrad:** Existieren bereits moderne Sicherheitsstrukturen oder herrscht großer Nachholbedarf?
- **Infrastruktur-Komplexität:** Anzahl der Standorte, vernetzte OT-Anlagen in der Produktion und Anteil ausgelagerter IT (*Managed Services*).
- **Verfügbares Fachwissen:** Muss Security-Know-how komplett neu eingekauft werden?

7.3 Wo ISO 9001 spürbar Budget spart

Weil Kernprozesse wie Dokumentenverwaltung, interne Audits und die Bewertung durch die Geschäftsführung bereits existieren, entfällt der organisatorische Grundaufbau weitgehend – sofern diese Prozesse im Betrieb tatsächlich gelebt werden. Sie können sich deshalb gleich auf die technischen und fachlichen Inhalte der Informationssicherheit konzentrieren.

7.4 Beispiel: interner Aufwand der Muster Maschinenbau GmbH

Szenarioannahmen für das erste Jahr

Die Spannen sind Annahmen für das fiktive Beispielunternehmen – keine Erfahrungswerte und keine Vorgabe.

Rolle	Hauptaufgaben	Interner Aufwand im ersten Jahr	Was die Spanne bestimmt
Geschäftsführung	Schulung, Freigaben, Entscheidungen, regelmäßige Bewertung	einige Tage	Zahl der Entscheidungen über Investitionen und Prioritäten
QM-Leitung	Dokumentenverwaltung, Auditplanung, Vorbereitung der Bewertung durch die Geschäftsführung	mehrere Wochen	Reife des QM-Systems; Umfang externer Unterstützung
IT-Leitung	Inventar, Risikobewertung, Steuerung der Maßnahmen, Abstimmung mit dem Dienstleister	mehrere Wochen bis wenige Monate	technischer Nachrüstbedarf; Anteil ausgelagerter IT
Prozessverantwortliche	Mitwirkung an Risikoanalyse und Notfallplänen	je ein bis wenige Tage	Zahl der kritischen Geschäftsprozesse

Nicht enthalten: Lizenz- und Anschaffungskosten für Technik; Honorare des IT-Dienstleisters für die Umsetzung; externe Beratung; Kosten einer Zertifizierung; die Ablösung veralteter Systeme, etwa nicht mehr unterstützter Betriebssysteme.

8. Nachweise, Wirksamkeit und Geschäftsführung

8.1 Das Nachweisregister

Das Nachweisregister führt für jeden der zehn Bereiche die drei Ebenen zusammen. Es dokumentiert Regel, umgesetzte Maßnahme, Wirksamkeitsnachweis, verantwortliche Person und das nächste Prüfintervall in einer kompakten Übersicht.

Bereich	Regel (Ebene 1)	Maßnahme (Ebene 2)	Wirksamkeitsnachweis (Ebene 3)	Lenkender Prozess	Verantwortlich	Prüfintervall
Nr. 3: Datensicherung	Datensicherungsrichtlinie v2	Tägliche, netzgetrennte und unveränderbare Backups	Protokoll des erfolgreichen ERP-Wiederherstellungstests	7.5, 9.1, 9.2	IT-Leiter	Quartalsweise
Nr. 2: Sicherheitsvorfälle	Incident-Plan mit Meldeweg	Rufbereitschaft; vorbereiteter BSI-Portalzugang	Protokoll der halbjährlichen Krisen- und Meldeübung	7.5, 9.1	Sicherheitsverantwortlicher	Halbjährlich
Nr. 10: Authentifizierung	Richtlinie zur MFA-Pflicht	MFA für alle Fern- und Admin-Zugänge erzwungen	Audit-Report der Kontenkonfiguration ohne Ausnahmen	7.5, 9.2	IT-Leiter	Jährlich
Nr. 4: Lieferkette	Lieferantenrichtlinie mit Mindeststandards	Sicherheitsprüfung des IT-Dienstleisters & Vertragsergänzung	Jährliche Verifikation anhand aktueller Prüfberichte / ISO-Zertifikate	8.4, 7.5	QM-Leitung	Jährlich

8.2 Der Bericht an die Geschäftsleitung

Um die Überwachungspflicht nach § 38 BSIG nachweisbar wahrzunehmen, erhält die Geschäftsführung einen kompakten Quartalsbericht mit sechs Kernpunkten:

1. Wesentliche Veränderungen der Bedrohungslage.
2. Umsetzungsstand des Maßnahmenplans nach Spuren A, B und C.
3. Ergebnisse technischer Wirksamkeitsprüfungen und Notfalltests.
4. Aufgetretene Sicherheitsvorfälle und eventuelle BSI-Meldungen.
5. Offene, kritische oder überfällige Maßnahmen.
6. Konkrete Beschlussvorlagen (z. B. Budgetfreigaben oder Restrisiko-Akzeptanzen).

Der Bericht wird direkt in die regelmäßige Bewertung durch die Geschäftsführung integriert.

8.3 Was die Überwachungspflicht verlangt

Regelmäßige Berichte und dokumentierte Beschlüsse der Geschäftsführung bilden das Rückgrat des Nachweises ihrer gesetzlichen Überwachungspflicht nach § 38 Abs. 1 BSIG. Es genügt nicht, Sicherheitsberichte zur Kenntnis zu nehmen. Die Geschäftsleitung muss den Reifegrad der Maßnahmen aktiv bewerten, notwendige Investitionen oder Richtlinien beschließen und die Behebung bekannter Mängel konsequent einfordern.

Für Ihre Audit-Dokumentation bedeutet das:

Das Protokoll der Bewertung durch die Geschäftsführung muss neben der Berichtsübergabe explizit die inhaltliche Bewertung der Geschäftsleitung, ihre konkreten Beschlüsse, die zugewiesenen Budgets sowie die Nachverfolgung bis zum erfolgreichen Abschluss festhalten.

8.4 Das Praxisbeispiel

Bei der Muster Maschinenbau GmbH verläuft der erste praktische Wiederherstellungstest für das ERP-System nicht wie geplant: Die Daten sind zwar vollständig vorhanden, doch das Rückspielen dauert drei Tage statt der im Notfallhandbuch geforderten acht Stunden. Dieser Befund wird als Abweichung über den bestehenden Korrekturprozess der ISO 9001 (Kapitel 10.2) erfasst.

Der darauf folgende Sicherheitsbericht an die Geschäftsleitung stellt die Lücke transparent dar und stellt zwei technische Lösungswege inklusive Kostenfolgen gegenüber. Die Geschäftsführung wählt eine Lösung, gibt das erforderliche Budget frei und setzt eine Frist für den Wiederholungstest. Der darauffolgende Quartalsbericht dokumentiert den erfolgreichen Zweittest, woraufhin die Korrekturmaßnahme geschlossen wird. Jeder dieser Schritte ist lückenlos im Protokoll der Bewertung durch die Geschäftsführung und im Nachweisregister belegt.

9. ISO/IEC 27001: Wann lohnt sich eine formelle Zertifizierung?

9.1 Die drei Ebenen der Compliance

Im Umfeld von NIS-2 gilt es, drei Ebenen strikt voneinander zu unterscheiden:

DREI EBENEN DER COMPLIANCE-REIFE
1. GESETZLICHE PFLICHTERFÜLLUNG (§ 30 BSIG) • Zwingend vorgeschrieben für alle betroffenen Einrichtungen
2. BETRIEB EINES ISMS (z. B. nach ISO 27001) • Bewährter Rahmen, um Pflichten dauerhaft & strukturiert zu erfüllen
3. AKKREDITIERTE ZERTIFIZIERUNG (Durch TÜV, DEKRA, DQS etc.) • Freiwilliger externer Nachweis für Markt und Kunden

Das Gesetz verlangt die **nachweisbare Erfüllung** der Sicherheitsanforderungen. Es schreibt weder ein Managementsystem nach einer bestimmten Norm noch ein ISO-Zertifikat verbindlich vor. Die Erweiterung Ihres bestehenden ISO-9001-Systems ist rechtlich ein vollkommen ausreichender Rahmen – vorausgesetzt, die Sicherheitsmaßnahmen selbst sind umgesetzt und wirksam.

9.2 Wann sich eine Zertifizierung kommerziell auszahlt

Die Entscheidung für ein Audit nach ISO/IEC 27001 ist keine rechtliche, sondern eine strategische Geschäftsentscheidung. Drei Fragen weisen den Weg:

1. Fordern Kunden oder Ausschreibungen ein Zertifikat?

In B2B-Ausschreibungen und Lieferantenverträgen kann das ISO-27001-Zertifikat ein kaufmännisches K.-o.-Kriterium sein. *(Automobilzulieferer beachten bitte: Die Branche fordert in der Regel ein TISAX-Label statt eines reinen ISO-27001-Zertifikats.)*

2. Wie hoch ist der Aufwand für B2B-Sicherheitsfragebögen?

Ein akkreditiertes Zertifikat kürzt aufwendige Due-Diligence-Fragebögen (DDQs) deutlich ab, ersetzt sie aber nicht. Es dient als anerkannter Vertrauensbeweis und entlastet Ihre IT- und Vertriebsteams im Alltag.

3. Benötigt die Organisation einen externen Taktgeber?

Jährliche Überwachungsaudits und die dreijährliche Rezertifizierung zwingen das Unternehmen dazu, Sicherheitsanalysen, Tests und Dokumente kontinuierlich aktuell zu halten. Dies schützt effektiv vor dem "Einschlafen" umgesetzter Maßnahmen.

9.3 Welche Zusatzanforderungen entstehen

Eine formelle Zertifizierung erzeugt zusätzlichen Aufwand: Auditgebühren der Zertifizierungsstelle, Aufwände für Vor-Audits sowie spezifische Normfokussierungen der ISO/IEC 27001, die über die reine NIS-2-Compliance hinausgehen:

- **Statement of Applicability (SoA):** Eine detaillierte Begründung für den Einschluss oder Ausschluss jeder einzelnen Maßnahme aus Anhang A der Norm.
- **Formaler Risikobehandlungsplan (Risk Treatment Plan).**
- **Kennzahlenbasierte Informationssicherheitsziele (Clause 6.2).**

9.4 Die Entscheidung kann reifen

Das Erfreuliche an einer ISO-9001-Erweiterung: Da beide Normen derselben Grundstruktur folgen, geht kaum ein Arbeitsschritt verloren. Wenn Sie Ihre Sicherheitsstrukturen in das QM-System integrieren, bauen Sie die ISO-27001-Anforderungen organisch mit auf. Die Entscheidung für ein externes Zertifizierungsaudit können Sie beruhigt auf einen späteren Zeitpunkt verschieben – etwa wenn wichtige Schlüsselkunden dies explizit einfordern.

10. Der nächste Schritt: erste Einschätzung und Bestandsaufnahme

10.1 Orientierungs-Checklist

Nutzen Sie diese Schnellbewertung für eine erste Einschätzung im Führungskreis. Bewerten Sie jedes Thema auf allen drei Ebenen unseres Nachweismodells:

Thema / Anforderung	1. Regel vorhanden?	2. Maßnahme umgesetzt?	3. Wirksamkeit belegt?
BSI-Stammdaten (§ 33 BSIG): Aktuell, verantwortliche Person und Vertretung benannt	☐	☐	☐
Incident-Reporting (§ 32 BSIG): 24/7-Meldeweg und BSI-Portalzugang etabliert	☐	☐	☐
Geschäftsführung (§ 38 BSIG): Nachweisbare Schulung zur Risiko-Governance erfolgt	☐	☐	☐
Risikoanalyse: Gefahrenübergreifend erstellt und mit festem Überprüfungsintervall	☐	☐	☐
Datensicherung & BCM: Netzisoliertes Backup mit nachgewiesenem Wiederherstellungstest	☐	☐	☐
Lieferketten-Governance: Sicherheitsbewertung und Vertragsklauseln für IT-Provider	☐	☐	☐
Zugriffsschutz: Mehr-Faktor-Authentifizierung (MFA) für alle Fern- und Admin-Zugänge	☐	☐	☐
Berichterstattung an die Geschäftsleitung: Informationssicherheit als fixer Punkt in der Bewertung durch die Geschäftsführung	☐	☐	☐

(Hinweis: Zeitangaben wie „halbjährlich“ oder „quartalsweise“ sind interne Planungsintervalle. Das Gesetz schreibt für die Prüfungen nach § 30 BSIG keine starren Kalenderabstände vor.)

10.2 Bewertung des Checks

Ein positives Bild in dieser Schnellbewertung liefert erste Ansatzpunkte, ersetzt jedoch noch keine vollständige Nachweisführung. Zwei Gründe sind hierfür entscheidend:

1. Die Orientierungsfragen decken die zehn gesetzlichen Kriterien aus § 30 Abs. 2 BSIG nicht vollständig ab.
2. Ein Haken bei "Umgesetzt" belegt noch nicht, ob die Schutzmaßnahme dem spezifischen Risikoprofil und dem Stand der Technik entspricht.

10.3 Die strukturierte Bestandsaufnahme

Der nächste pragmatische Schritt ist eine **vollständige Bestandsaufnahme**, die alle zehn Bereiche des § 30 Abs. 2 BSIG abdeckt.

Diese Bestandsaufnahme:

- Steckt den erforderlichen Geltungsbereich ab,
- Klassifiziert die vorhandenen ISO-9001-Prozesse (*wiederverwenden, erweitern, neu aufbauen, prüfen*),
- Deckt konkrete Lücken auf allen drei Nachweisebenen auf,
- Mündet direkt in einen priorisierten Maßnahmenplan für die drei Umsetzungsspuren.

Beispiel: Ergebnis der Bestandsaufnahme bei der Muster Maschinenbau GmbH

So kann das Ergebnis einer Bestandsaufnahme aussehen (fiktives Beispiel, Auszug):

Thema	Was wir vorfinden	Was fehlt	Erforderlicher Nachweis	Wer entscheidet	Stand nach sechs Monaten
Datensicherung	Tägliche Sicherung, Wiederherstellung nie getestet	Vom Netz getrennte, nicht veränderbare Sicherung; regelmäßige Tests	Testprotokoll	Geschäftsführung (Budget)	Neue Sicherung in Betrieb; zweiter Test nach Korrektur erfolgreich
Vorfallobermittlung	Kein festgelegter Meldeweg	Zuständige, Vertretung, Erreichbarkeit, Vorlagen	Vorfallplan; Protokoll einer Meldeübung	Geschäftsführung (Zuständigkeit)	Meldeweg festgelegt; erste Übung durchgeführt
Fernzugänge	IT-Dienstleister greift per Passwort zu	Mehr-Faktor-Authentifizierung	Auswertung der Konten ohne zweiten Faktor	IT-Leiter mit Dienstleister	Mehr-Faktor-Authentifizierung für alle Fern- und Administratorzugänge
IT-Dienstleister	Ausgewählt nach Preis und Reaktionszeit	Sicherheitsbewertung; Pflichten im Vertrag	Bewertungsbericht; Vertragsanhang	Geschäftsführung (Vertrag), QM-Leitung (Bewertung)	Bewertung durchgeführt; Vertrag ergänzt
Standorte	QM-Zertifikat nur für das Hauptwerk; Produktion mit dem Büronetz verbunden	Vertriebsbüro und Produktionsnetz in der Risikoanalyse	Risikoregister für alle Standorte	Geschäftsführung	Risikoanalyse für alle Standorte; Trennung von Büro- und Produktionsnetz beauftragt

Gerade für Unternehmen mit einem etablierten Qualitätsmanagementsystem zeigt sich in dieser Phase, wie viel organisatorisches Fundament bereits vorhanden ist – und wie schlank sich NIS-2 verankern lässt.

Ihr nächster Schritt: NIS-2-Bestandsaufnahme für Unternehmen mit ISO 9001

- **Umfang:** Bestandsaufnahme über alle zehn Bereiche des § 30 BSIG und alle Standorte; Einstufung Ihrer QM-Prozesse (wiederverwenden, erweitern, neu aufbauen, prüfen).
- **Ergebnis:** eine Lückenübersicht wie im Beispiel oben, ein Maßnahmenplan mit Prioritäten für die drei Spuren und eine Entscheidungsvorlage für Ihre Geschäftsführung.
- **Dauer:** in der Regel wenige Wochen, abhängig von Größe und Zahl der Standorte.

Kontakt & Ansprechpartner

Derek Carson

KI-Governance & Informationssicherheit

Lead Implementer ISO/IEC 27001 & ISO/IEC 42001

Liedeweg 66 · 36093 Künzell (bei Fulda)

E-Mail: derek@carson.de

Telefon: +49 (0)661 9452622

Web: carson.de

Quellenverzeichnis (Stand 19.10.2026)

- **BSI:** *NIS-2 in Zahlen* (Stand 30.09.2026); BSI-Betroffenheitsprüfung.
- **BSIG (BSI-Gesetz):** §§ 28, 30, 32, 33, 35, 38, 62 (*gesetze-im-internet.de*, abgerufen 19.10.2026).
- **Deutscher Bundestag:** Gesetzentwurf der Bundesregierung, BT-Drs. 21/1501 (08.09.2025); Beschlussempfehlung, BT-Drs. 21/2782 (12.11.2025).
- **Kertos:** *NIS2 Readiness Study 2026* (n = 51, Befragungszeitraum 03.08.–04.09.2026).
- **Bitkom:** Studienbericht *Wirtschaftsschutz 2025* (n = 1.002, CATI-Befragung).
- **ENISA:** *NIS Investments 2024* (n = 1.350 Organisationen in der EU-27).
- **DIN EN ISO 9001:2015-11 & ISO/IEC 27001:2022.**