Leitfaden: IT-Risiken im Qualitätsmanagementsystem

Inhalt

Normverankerung (DIN EN ISO 9001:2025-Entwurf)

In der überarbeiteten Ausgabe der DIN EN ISO 9001 (DIN EN ISO 9001:2025-Entwurf) sind auch IT-bezogene Risiken normativ stärker verankert. Die Übersicht gibt einen ersten Überblick. *Die Inhalte entsprechen nicht der endgültigen Fassung.*

Abschnitt	Anforderung (Kurzfassung)	Relevanz für IT-Risiken
4.1, Anm. 2	Externe und interne Themen bestimmen und überwachen – inkl. technologischer Faktoren	IT-Abhängigkeiten als Teil des Organisationskontexts; Änderungen in der IT-Landschaft sind zu beobachten
4.2	Anforderungen relevanter interessierter Parteien bestimmen	Kunden, Behörden und Lieferanten stellen zunehmend Anforderungen an IT-Sicherheit (z. B. NIS-2-Umsetzungsgesetz)
6.1.1	Risiken UND Chancen bestimmen	Beide Dimensionen sind gleichwertig anzusprechen – nicht nur Risikominimierung
6.1.2 + Anm. 1	Risiken analysieren und bewerten; inkl. **Störungsszenarien** (Disruption)	IT-Ausfälle und Cyberangriffe sind bei allen IT-nutzenden Unternehmen relevante Szenarien
6.1.2 b) 1+2	Maßnahmen in QMS-Prozesse integrieren; Wirksamkeit bewerten	Maßnahmen zur Reduktion der IT-Risiken müssen nachweisbar umgesetzt und auf ihre Wirksamkeit hin überprüft sein
8.4	Extern erbrachte Prozesse, Produkte und Dienstl. steuern und bewerten	Betrifft u.a. IT-Dienstleister und Cloud-Dienste

Möglicher Einstieg im (internen) Audit

IT-Risiken fehlen in Risikoregistern häufig ganz, sind nur pauschal benannt oder inhaltlich nicht bewertet. Die folgenden, aufeinander aufbauenden Fragen können genutzt werden, um den Betrachtungsgrad besser zu erfassen.

Drei typische Ausgangslevel von Organisationen:

Situation	Einstiegsfragen	Weitere Indikatoren
IT-Risiken fehlen im Register vollständig	• Nach welchen Kriterien wurde entschieden, welche Risiken aufgenommen werden? • Wie sind dabei IT-bezogene Themen berücksichtigt worden?	• Gibt es ein nachvollziehbares Verfahren zur Risikoidentifikation – oder wurden Risiken einmalig gesammelt und seitdem nicht mehr hinterfragt?
IT taucht pauschal auf (z. B. 'IT-Ausfall') ohne Bewertung	• Sie haben IT-Ausfall als Risiko erfasst. Wie haben Sie Auswirkung und Wahrscheinlichkeit bewertet – und welche konkreten Szenarien stecken dahinter?	• Ist das Risiko wirklich bewertet oder nur benannt? • Gibt es Maßnahmen, die konkret auf dieses Risiko einzahlen?
Unternehmen nennt bereits vorhandene Maßnahmen	• Wie stellen Sie sicher, dass diese Maßnahmen auch wirksam sind? • Wann wurde das zuletzt überprüft?	• Wirksamkeitsprüfung ist explizite Anforderung (6.1.2 b) 2). • Wurden die Maßnahmen nur umgesetzt, oder auch deren Wirksamkeit überprüft?

Kernrisiken: Steckbriefe

Für manche Unternehmen ist die Vielfalt der IT-Risiken noch schwer greifbar. Die nachfolgenden typischen Szenarien sollen dabei helfen diese Risiken konkreter zu erfassen, auch in Bezug auf mögliche Maßnahmen und den Chancen eines gezielten Umgangs mit diesen.
Mögliche Fragestellungen für Auditsituationen sollen die Diskussion möglicher IT-Risiken anregen. Die Szenarien und Details erheben keinen Anspruch auf Vollständigkeit, sondern stellen einen Ausgangspunkt dar.

Exemplarische behandelte Risiken:

- Datensicherung & Wiederherstellung
- Ransomware & Systemausfall
- Phishing & menschliches Versagen
- Datenleck & unbefugter Zugriff
- Ausfall externer IT-Dienstleister & Cloud-Dienste
- Operational Technology & Maschinensteuerung

Legende

Risikobeschreibung	Auswirkungen, insb. in Bezug auf ein Qualitätsmgmt-System	**e**xemplarische Fragestellungen

Risiko 1: Datensicherung & Wiederherstellung

	Datenverlust oder Systemausfall ohne gesicherte, geprüfte Wiederherstellungsmöglichkeiten.
	Die Fähigkeit, konforme Produkte und Dienstleistungen kontinuierlich zu erbringen (6.1.2 Note 1), ist direkt gefährdet, wenn im Störungsfall keine funktionsfähige Sicherung verfügbar ist. Betroffen sind Lieferfähigkeit, Qualitätsdokumentation, Kundenkommunikation und regulatorische Nachweispflichten.
	• Wie lange wäre das Unternehmen lieferfähig, wenn alle zentralen IT-Systeme heute ausfallen würden? • Wann wurde zuletzt geprüft, ob eine Wiederherstellung tatsächlich funktioniert?

Hintergrund & Erklärung:

Eine Festplatte gibt den Geist auf, ein Brand zerstört den Serverraum, es kommt zu einem Überspannungsschaden durch Blitzeinschlag. In allen drei Fällen stellt sich sofort dieselbe Frage: Gibt es eine aktuelle, funktionierende Sicherung? Liegt die Sicherung am gleichen Ort wie die Originaldaten, ist sie im Brandfall verloren. Liegt sie extern, aber enthält nur Dateien ohne Systemkonfigurationen, lässt sich der Server möglicherweise nicht wiederherstellen. Die weniger offensichtliche Gefahr: Ein Angreifer ist seit Wochen unentdeckt im System. In dieser Zeit wurden Backups erstellt. Wer dieses Backup wiederherstellt, stellt das Problem gleich mit zurück. Deshalb ist nicht nur die Existenz von Backups relevant, sondern auch ihre Integrität. Wer alle Bereiche in einem gemeinsamen System sichert, hat im Ernstfall die Wahl zwischen allem oder nichts. Wer Bereiche separat sichert, bleibt zumindest teilweise handlungsfähig.

Fragen zur Risikohandhabung:

Grundsätzlich	• Gibt es ein dokumentiertes Backup-Konzept? • Wer ist verantwortlich für Durchführung und Überwachung?
Umfang	• Werden nur Daten gesichert – oder auch Systemkonfigurationen? • Sind alle geschäftskritischen Systeme erfasst?
Speicherort	• Gibt es mindestens eine Sicherung extern oder offline – physisch getrennt vom Primärsystem? • Ist berücksichtigt, dass Speichermedien eine begrenzte Lebensdauer haben?
Wiederherstellung	• Wird die tatsächliche Wiederherstellbarkeit regelmäßig getestet – nicht nur die Erstellung der Sicherung? • Gibt es Zielwerte, wie schnell welche Systeme wiederhergestellt sein sollen?
Integrität	• Wird die Integrität von Backups sichergestellt? • Werden Backups vor Wiederherstellung auf Schadsoftware geprüft?
Bereichstrennung	• Werden unterschiedliche Unternehmensbereiche oder Standorte separat gesichert? • Wäre das Unternehmen teilweise arbeitsfähig, wenn nur ein Bereich betroffen ist?

Chancen:

Nachweisbare Wiederherstellungsfähigkeit als Kriterium in Kundenanfragen und Ausschreibungen
Grundlage für Cyber-Versicherungskonditionen
Reduzierte Ausfallzeit bei technischen Störungen jeder Art – nicht nur Cyberangriffe

Risiko 2: Ransomware & Systemausfall

	Verschlüsselung oder Zerstörung von IT-Systemen durch Schadsoftware oder technisches Versagen mit weitreichender Betriebsunterbrechung.
	Unmittelbarer Ausfall der Fähigkeit, konforme Produkte und Dienstleistungen zu erbringen. Betroffen sind typischerweise ERP-Systeme, Produktionssteuerung, Qualitätsdokumentation, Kundenkommunikation und Rechnungswesen – je nach Digitalisierungsgrad gleichzeitig.
	• Welche Kernprozesse wären innerhalb von 24 Stunden nicht mehr funktionsfähig, wenn alle Server ausfallen? • Gibt es einen definierten Prozess für den Fall, dass Schadsoftware entdeckt wird?

Hintergrund & Erklärung:

Ransomware-Angriffe folgen meist demselben Muster: Ein Mitarbeiter wird Opfer eines Phishing-Angriffs und öffnet einen infizierten Anhang. Die Schadsoftware verbreitet sich still im Netzwerk – oft tagelang – bevor sie aktiv wird. Dann werden alle erreichbaren Dateien verschlüsselt, häufig innerhalb von Minuten. Der entscheidende Faktor ist die Ausbreitung: Sind alle Systeme im selben Netzwerksegment, trifft es alles gleichzeitig. Sind Bereiche sicher getrennt, kann die Ausbreitung begrenzt werden. Dasselbe gilt für Benutzerrechte: Wer mit Administratorrechten arbeitet, gibt der Schadsoftware denselben Zugriff. Wer im Ernstfall nicht weiß, wen er zuerst anruft, verliert wertvolle Zeit. Wer keinen Kommunikationsplan hat, informiert Kunden und Behörden zu spät – mit eigenen rechtlichen Konsequenzen.

- **Fragen zur Risikohandhabung:**

Prävention	• Gibt es aktuelle Virenschutz-Lösungen auf allen Systemen (Endgeräte+Server)? • Werden Sicherheitsupdates zeitnah eingespielt – nach welchem Prozess? • Sind Benutzerrechte nach dem Prinzip der minimalen Berechtigung vergeben? • Werden regelmäßig Schulungen zum Umgang mit Phishing vorgenommen?
Netzwerk	• Sind unterschiedliche Bereiche oder Systeme netztechnisch voneinander getrennt? • Haben externe Dienstleister Fernzugriff – und ist dieser auf das Notwendige beschränkt und protokolliert?
Erkennung	• Gibt es Mechanismen, die ungewöhnliche Aktivitäten im Netzwerk erkennen und melden? • Wer wird wie informiert, wenn ein Verdacht besteht?
Reaktion	• Gibt es einen dokumentierten Reaktionsplan („Incident Response Plan“) für den Ernstfall? • Gibt es klare Rollen- und Aufgabenverteilung für den Ernstfall. z.B in Form eines Notfallstabs • Sind externe Ansprechpartner für den Ernstfall bekannt und erreichbar?
Kommu-nikation	• Gibt es einen Kommunikationsplan für Kunden, Lieferanten und ggf. Behörden? • Wie wird intern kommuniziert, wenn die üblichen Kanäle (E-Mail, Telefon) betroffen sind?

Chancen:

- Strukturierte Notfallplanung reduziert Ausfallzeit bei jeder Art von Betriebsunterbrechung
- Klare Verantwortlichkeiten im Ernstfall stärken das Vertrauen von Kunden und Partnern
- Nachweisbare Schutzmaßnahmen als Differenzierungsmerkmal in sensiblen Branchen

Risiko 3: Phishing & menschliches Versagen

	Unbeabsichtigte Preisgabe von Zugangsdaten oder Auslösung von Schadprozessen durch Mitarbeitende infolge gezielter Täuschung.
	Phishing ist in den meisten Fällen der Ausgangspunkt für weitergehende Angriffe. Die Kompetenzanforderungen der ISO 9001 (Kap. 7.2 / 7.3) schließen das Bewusstsein für Risiken ein, die aus dem eigenen Handeln entstehen.
	• Wie wird sichergestellt, dass Mitarbeiter gefälschte E-Mails erkennen können? • Was passiert konkret, wenn ein Mitarbeiter auf einen verdächtigen Link geklickt hat – wohin wendet er sich?

Hintergrund & Erklärung:
Phishing-Angriffe sind heute, oft mithilfe von KI-Tools, professionell gestaltet. Sie imitieren E-Mails von Kollegen, Vorgesetzten oder Lieferanten – mit korrektem Logo, passendem Kontext, manchmal mit dem Namen des tatsächlichen Ansprechpartners. Der Mitarbeiter, der auf einen Link oder Anhang klickt, macht keinen Fehler aus Nachlässigkeit – er reagiert auf etwas, das sorgfältig auf ihn zugeschnitten wurde. Technisch kann ein gestohlenes Passwort allein wenig ausrichten, wenn eine zweite Bestätigung notwendig ist. Wer das nicht hat, öffnet mit einem Passwort die Tür zu allem. Menschlich entscheidet die Frage: Traut sich der Mitarbeiter, den Vorfall zu melden? Unternehmen, in denen Fehler gemeldet werden dürfen, erkennen Angriffe früher. Unternehmen, in denen Mitarbeitende Konsequenzen fürchten, erfahren vom Angriff oft erst dann, wenn es zu spät ist.

Fragen zur Risikohandhabung:

Bewusstsein	• Werden Mitarbeitende regelmäßig zu IT-Sicherheitsthemen sensibilisiert – in welcher Form und in welchem Rhythmus?
Zugangssicherheit	• Ist für externe Zugänge und kritische Systeme eine Zwei-Faktor-Authentifizierung aktiv? • Werden Passwörter nach definierten Regeln vergeben und regelmäßig erneuert?
Meldeprozess	• Gibt es einen niedrigschwelligen, bekannten Meldeprozess für Sicherheitsvorfälle? • Werden gemeldete Vorfälle ausgewertet und als Lerngrundlage genutzt?
Zugriffsrechte	• Haben Mitarbeitende nur Zugriff auf Systeme und Daten, die sie für ihre Aufgaben benötigen? • Werden Zugriffsrechte bei Rollenwechsel oder Austritt zeitnah angepasst?
Überprüfung	• Wird das Bewusstsein der Mitarbeitenden gelegentlich praktisch überprüft? • Wie wird die Wirksamkeit von Schulungsmaßnahmen bewertet?

Chancen:
- Sensibilisierte Mitarbeitende erkennen nicht nur IT-Angriffe früher, sondern auch andere Unregelmäßigkeiten
- Gelebte Meldekultur stärkt die interne Kommunikation insgesamt
- Nachweisbare Schulungsmaßnahmen erfüllen gleichzeitig Anforderungen aus Kap. 7.2 / 7.3

Risiko 4: Datenleck & unbefugter Zugriff

	Unbefugte Weitergabe, Einsichtnahme oder Entwendung von Unternehmens-, Kunden- oder Mitarbeiterdaten – durch externe Angreifer, interne Fehler oder ausscheidende Mitarbeitende.
	Verlust von Kundenvertrauen, vertragliche Konsequenzen und regulatorische Meldepflichten (DSGVO: 72-Stunden-Frist). Qualitätsdaten, Konstruktionszeichnungen oder Prüfprotokolle können in falsche Hände geraten.
	• Wissen Sie, wo alle kunden- und mitarbeiterbezogenen Daten in Ihrem Unternehmen gespeichert sind? • Was würde passieren, wenn ein Mitarbeiter das Unternehmen heute verlässt – welche Zugänge bleiben wie lange aktiv?

Hintergrund & Erklärung:

Datenlecks entstehen seltener durch spektakuläre Einbrüche als durch unspektakuläre Alltagssituationen: ein falsch adressiertes E-Mail, ein freigegebener Cloud-Ordner ohne Zugangsbeschränkung, ein ehemaliger Mitarbeiter, dessen Zugangsdaten nie gesperrt wurden. Das Besondere an Datenlecks ist ihre Zeitverzögerung: Oft vergehen Wochen, bis ein unbefugter Zugriff bemerkt wird. In dieser Zeit können Daten kopiert, weitergegeben oder für weitere Angriffe genutzt worden sein. Wer keine Protokollierung hat, weiß im Ernstfall nicht, was betroffen war – und kann die gesetzlich geforderte Meldung nicht sauber abgeben. Nicht jeder Mitarbeiter benötigt Zugriff auf alle Daten. Wer Zugriffsrechte nicht nach Aufgaben vergibt und regelmäßig überprüft, hat im Zweifelsfall keinen Überblick darüber, wer was gesehen oder verändert hat.

Fragen zur Risikohandhabung:

Überblick	• Gibt es eine Übersicht, welche Daten wo gespeichert sind – lokal, auf Servern, in Cloud-Diensten? • Ist bekannt, welche Daten als besonders schutzbedürftig eingestuft sind?
Zugriffs-steuerung	• Werden Zugriffsrechte nach dem Zero-Trust-Prinzip vergeben? • Gibt es einen definierten Prozess, wenn Mitarbeitende das Unternehmen verlassen oder die Rolle wechseln?
Externe Übertragung	• Gibt es Regelungen, wie Daten nach außen übermittelt werden dürfen – per E-Mail, Cloud, USB? • Werden Übertragungen protokolliert oder zumindest nachvollziehbar gestaltet?
Erkennung und Meldung	• Gibt es eine Protokollierung von Zugriffen auf sensible Daten? • Ist der interne Meldeprozess bei einer Datenpanne bekannt – und ist die 72-Stunden-Frist nach DSGVO bekannt?
Mobile Geräte	• Sind Notebooks und Mobiltelefone mit Unternehmensdaten verschlüsselt? • Können verloren gegangene Geräte aus der Ferne gesperrt oder gelöscht werden?

Chancen:

- Strukturiertes Datenzugriffsmanagement schafft Transparenz über Prozesse und Verantwortlichkeiten
- Nachweisbare Datenschutzmaßnahmen als Voraussetzung in Lieferketten und öffentlichen Ausschreibungen
- Vermeidung von Reputationsschäden durch proaktiver statt reaktiver Herangehensweise

Risiko 5: Ausfall externer IT-Dienstleister & Cloud-Dienste

	Betriebsunterbrechung durch Ausfall, Insolvenz oder Sicherheitsvorfall bei einem externen IT-Dienstleister oder Cloud-Anbieter, von dem kritische Geschäftsprozesse abhängen.
	Extern erbrachte Prozesse bleiben im Verantwortungsbereich der Organisation (8.4). Ein Ausfall des bereitgestellten ERP-Systems, der E-Mail-Infrastruktur des Dienstleisters oder eines cloudbasierten QMS trifft die Lieferfähigkeit unmittelbar – unabhängig davon, dass ein externer Anbieter betroffen ist.
	• Welche Ihrer IT-Systeme werden von externen Anbietern betrieben oder befinden sich in der Cloud? • Was würde passieren, wenn Ihr ERP-System oder Ihre E-Mail-Infrastruktur für eine Woche nicht verfügbar wäre?

Hintergrund & Erklärung:

Viele Unternehmen haben ihre IT-Infrastruktur ausgelagert – E-Mail, ERP, Dokumentenmanagement, manchmal das QMS selbst. Wenn der Anbieter ein Problem hat, hat das Unternehmen ein Problem – ohne selbst etwas falsch gemacht zu haben. Diese Abhängigkeit hat mehrere Dimensionen: Verfügbarkeit (fällt der Dienst aus, fällt der Prozess aus), Sicherheit (ein Angriff auf den Dienstleister kann Kundendaten betreffen – Supply-Chain-Angriff) und Kontinuität (was passiert, wenn der Anbieter insolvent wird?). Hinzu kommt die vertragliche Dimension: wenn Dienstleister oder Cloud-Dienste genutzt werden, sind Verträge möglicherweise unzureichend formuliert – ohne definierte Verfügbarkeitsgarantien, ohne Regelungen zur Datenherausgabe, ohne Auftragsverarbeitungsvertrag nach DSGVO.

Fragen zur Risikohandhabung:

Überblick	• Gibt es eine vollständige Liste aller extern bezogenen IT-Dienste und Dienstleister? • Sind diese in der Lieferantenbewertung des QMS erfasst und bewertet?
Vertragliche Absicherung	• Sind Verfügbarkeits- und Reaktionszeiten vertraglich definiert? • Gibt es für alle Anbieter, die personenbezogene Daten verarbeiten, einen Auftragsverarbeitungsvertrag? • Sind Regelungen zur Datenherausgabe und -löschung bei Vertragsende vereinbart?
Abhängigkeiten	• Welche Prozesse wären bei Ausfall welches Dienstleisters sofort betroffen? • Gibt es für kritische Dienste Alternativen oder Notfallprozeduren?
Sicherheit des Anbieters	• Ist bekannt, welche Sicherheitsmaßnahmen der Anbieter selbst umsetzt? • Sind Mindestanforderungen an die Sicherheit von Dienstleister definiert? • Gibt es Nachweise – z. B. Zertifizierungen oder Auditberichte des Anbieters?
Fernzugriff	• Haben externe Dienstleister Fernzugriff auf interne Systeme – und ist dieser dokumentiert, begrenzt und protokolliert?

Chancen:

- Strukturierte Lieferantenbewertung für IT-Dienste schafft Klarheit über tatsächliche Abhängigkeiten
- Verhandlungsstärke gegenüber Anbietern durch definierte Anforderungen
- Grundlage für informierte Entscheidungen bei IT-Diensten (Eigenbetrieb vs. Auslagerung)

Risiko 6: Operational Technology & Maschinensteuerung

	Ausfall oder Manipulation von IT-Systemen, die direkt mit Maschinen, Anlagen oder Steuerungssystemen verbunden sind – mit Auswirkungen auf Produktionsfähigkeit, Produktqualität und Arbeitssicherheit.
	Ausfall oder Manipulation von Steuerungssystemen kann die Konformität von Produkten unmittelbar gefährden – fehlerhafte Steuerparameter, veränderte Prüfprogramme, unterbrochene Prozessüberwachung. Schnittstellen bestehen zu ISO 45001 (Arbeitssicherheit) und ISO 50001 (Energiemanagementsysteme mit digitalisierten Zählern).
	• Welche Ihrer Maschinen oder Anlagen sind mit dem Firmennetzwerk oder dem Internet verbunden? • Was würde passieren, wenn die Steuerungsparameter einer Anlage unbemerkt verändert würden?

Hintergrund & Erklärung:
In produzierenden Unternehmen wächst die Vernetzung von IT und Produktionstechnik – Maschinen melden Produktionsdaten, Anlagen werden ferngewartet, Steuerungssysteme sind ins Firmennetzwerk eingebunden. Ein Angreifer, der ins Firmennetzwerk gelangt, kann unter Umständen auch auf Steuerungssysteme zugreifen. Im harmloseren Fall bedeutet das Produktionsausfall. Im schwereren Fall können Steuerparameter verändert werden – mit Auswirkungen auf Produktqualität, die erst am Endprodukt oder beim Kunden bemerkt werden. Ein besonderes Problem: Steuerungsrechner laufen oft mit veralteten Betriebssystemen, die keine Sicherheitsupdates mehr erhalten. Diese Systeme sind technisch besonders verwundbar. Hinzu kommt der Fernzugriff durch Wartungsdienstleister: Viele Maschinenhersteller haben permanenten oder anlassbezogenen Fernzugriff. Ist dieser nicht kontrolliert und protokolliert, entsteht ein unkontrollierter Zugangspunkt ins Produktionsnetz.

Fragen zur Risikohandhabung:

Überblick	• Gibt es eine Übersicht aller Maschinen und Anlagen, die mit dem Netzwerk oder Internet verbunden sind? • Ist bekannt, welche Steuerungssysteme mit welchen IT-Systemen kommunizieren?
Netztrennung	• Sind Produktionsnetz und Büronetz voneinander getrennt? • Gibt es kontrollierte Übergabepunkte zwischen beiden Netzbereichen?
Fernzugriff Wartung	• Welche Maschinenhersteller oder Wartungsdienstleister haben Fernzugriff? • Ist dieser Zugriff zeitlich begrenzt, dokumentiert und nachvollziehbar?
Systemaktualität	• Auf welchen Betriebssystemen laufen die Steuerungsrechner? • Gibt es ein Konzept für den Umgang mit Systemen, die keine Sicherheitsupdates mehr erhalten?
Arbeitssicherheit	• Sind sicherheitsrelevante Steuerungssysteme (Not-Aus, Schutzeinrichtungen) von der allgemeinen IT-Infrastruktur getrennt?

Chancen:
- Strukturierte OT-Sicherheit als Grundlage für Digitalisierungs- und Industrie-4.0-Projekte
- Nachweisbare Integrität von Steuerungsparametern stärkt die Produktqualitätssicherung
- Fernwartungskonzepte schaffen Transparenz über Servicezugriffe und Wartungshistorie

Chancen Überblick

Gemäß der DIN EN ISO 9001:2025-Entwurf sind Chancen gleichwertig mit Risiken zu betrachten.

Chance	Kontext
Ausschreibungen & Lieferkette	IT-Sicherheitsnachweise werden zunehmend in Lieferantenbeurteilungen und Ausschreibungen gefordert – insbesondere im Kontext der EU-NIS2-Richtlinie, die Anforderungen in Lieferketten weiterdelegiert.
Versicherungskonditionen	Nachweisbare Schutzmaßnahmen sind Grundlage für Cyber-Versicherungen und können Konditionen direkt beeinflussen.
Effizienz & Prozessstabilität	Strukturiertes IT-Management reduziert ungeplante Ausfälle nicht nur durch Angriffe, sondern auch durch technisches Versagen – mit direktem Effekt auf Prozessstabilität und Qualität.
Vertrauen & Reputation	Kunden und Partner fragen zunehmend aktiv nach IT-Sicherheitsmaßnahmen – insbesondere in sensiblen Branchen und bei Verarbeitung personenbezogener Daten.
Integriertes Managementsystem	Unternehmen mit bestehendem QMS können IT-Risiken direkt in bestehende Strukturen integrieren – ohne neue Systeme aufzubauen (CAPA-Prozess, Management-Review, Lieferantenbewertung).

Mögliche nächste Schritte

Situation	Mögliche Schritte
IT-Risiken sind bisher kaum behandelt	• Verantwortlichkeiten zum IT-Risikomanagement festlegen • Beauftragung eines externen Cyber-Sicherheit-Checks (umfängliche Betrachtung der typischen Risikoquellen nach offiziellem Schema des BSI)
Risiken erkannt, keine Überprüfung	• Phishing-Assessment • Unabhängigen Schnelltest durchführen lassen
Risiken erkannt, erste Überprüfung stattgefunden	• Gezielte Validierung durch simulierte Angriffe in Form eines Penetrationstests • Einführung eines Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001

Weiterführende Ressourcen

1. **Das Bundesamt für Sicherheit in der Informationstechnik (BSI)**
2. **The Open Worldwide Application Security Project (OWASP)**
3. Die Seite der **Berlin Cert GmbH**
4. Schulungen & Seminare der **GUTcert Akademie**