WHITEPAPER

Prüfwerkzeuge in der Cyber- und Informationssicherheit

Risikobasierter und evidenzorientierter Einsatz von Selbstdeklaration, Nachweiskontrolle, Vor-Ort-Besuch und Audit unter Berücksichtigung knapper Ressourcen

Carsten Beck

Cybersecurity Auditor | ISO/IEC 27001 & ISO 22301 Lead Auditor

MAS Information Systems Management

Erstveröffentlichung April 2026 · Version 1.1 (Oktober 2026)

Executive Briefing

Wer Informationssicherheit prüfen will, steht vor einer doppelten Herausforderung: Die Bedrohungslage ist komplex und dynamisch, die verfügbaren Prüfressourcen sind begrenzt. Kein Prüfprogramm kann alle Risiken gleichzeitig abdecken. Entscheidend ist daher nicht, ob geprüft wird, sondern wie und mit welchen Mitteln: proportional zum Risiko und mit klarem Blick auf Aufwand und Wirkung.

Dieses Whitepaper beschreibt vier Prüfwerkzeuge, die in der Praxis der Cyber- und Informationssicherheit verbreitet sind: Selbstdeklaration, Dokumenten- und Nachweiskontrolle, Vor-Ort-Besuch und formales Audit. Sie unterscheiden sich im Aufwand und in den Nachweisen, die sie zugänglich machen. Wie belastbar ein Ergebnis ist, hängt aber nicht an der Bezeichnung des Werkzeugs, sondern an Prüfziel, Quelle, Erhebung, Zeitraum und Leistungsbezug der Nachweise. Der Ansatz orientiert sich an den Prüfgrundsätzen von ITAF und ISO 19011.

Die Grundsätze des Prüfprogramms und der Umgang mit wesentlichen Nachweislücken sind Governance-Entscheidungen: Sie bestimmen, wie belastbar die Entscheidungsgrundlagen des Managements sind. Die konkrete Werkzeugwahl erfolgt innerhalb dieses Rahmens nach fachlichem Ermessen.

Die Kernaussage lautet: Prüfwerkzeuge sind vom Risiko und vom erforderlichen Nachweis her zu wählen. Ihre Bezeichnung allein sagt noch nichts über die Belastbarkeit des Ergebnisses aus. Wo erforderliche Nachweise nicht erreichbar sind, wird die Lücke offengelegt und der Umgang damit entschieden. Sie darf nicht stillschweigend als Sicherheit gelten.

Dieses Papier richtet sich an Leitungs- und Aufsichtsgremien sowie an Verantwortliche in Informationssicherheit, Fachbereichen, Beschaffung, Risiko, Compliance und Audit. Kapitel 3 behandelt die Belastbarkeit von Nachweisen und den Umgang mit Nachweislücken, Kapitel 7 enthält Prüfnachweise, Kapitel 9 Leitfragen für Leitungs- und Aufsichtsgremien.

1 Ausgangslage: Prüfen unter Ressourcendruck

1.1 Das Grundproblem: Viele Risiken, begrenzte Mittel

Informationssicherheits-Audits und Kontrollen sind ressourcenintensiv. Allein die Planung und Vorbereitung eines formalen Audits bei einem kritischen Dienstleister kann mehrere Personentage (PT) binden, noch bevor die Prüfung selbst begonnen hat. Durchführung, Berichterstattung, Abstimmung und Follow-up kommen hinzu. Gleichzeitig wächst die Zahl zu prüfender Systeme und ausgelagerter Leistungen kontinuierlich.

Hinzu kommt: Nicht jedes Prüfwerkzeug eignet sich für jede Situation. Ein formales Audit bei einem externen Leistungserbringer mit geringem Risikopotenzial wäre unverhältnismässig und würde Ressourcen binden, die anderswo dringender gebraucht werden. Umgekehrt wäre eine blosse Selbstdeklaration bei einem Dienstleister, der hochkritische Systeme betreibt oder sensitive Daten verarbeitet, als alleiniges Prüfinstrument unzureichend. Sie liefert schlicht nicht die Nachweise, die eine belastbare Beurteilung erfordert.

«Dienstleister» und «Leistungserbringer» werden in diesem Papier gleichbedeutend verwendet. Gemeint sind externe Anbieter ebenso wie interne Leistungserbringer, etwa konzerninterne oder zentrale IT-Einheiten. Im Mittelpunkt steht die Prüfung bezogener Leistungen. Bei internen Leistungserbringern treten Leistungsvereinbarungen und interne Mandate an die Stelle des Vertrags; für eigene Systeme gelten die Prüfgrundsätze sinngemäss.

1.2 Risikobasierte Prüfplanung als Antwort

Die Antwort auf diesen Widerspruch ist ein risikobasiertes Vorgehen: Prüfintensität und Prüfmethodik richten sich nach dem tatsächlichen Risikoniveau der jeweiligen Situation, abhängig von der Kritikalität der bezogenen Leistung, dem Schutzbedarf der betroffenen Informationen, der Abhängigkeit vom Dienstleister und den möglichen Folgen eines Ausfalls oder einer Kompromittierung. Dieser Ansatz ist in internationalen Standards (z.B. ISO/IEC 27001, ISO 19011) ebenso verankert wie in etablierten Prüfframeworks. Die Verantwortung für bezogene Leistungen bleibt bei der beauftragenden Organisation (vgl. Whitepaper IT-Outsourcing & Governance dieser Reihe). Wo Personendaten im Auftrag bearbeitet werden, kommen ausdrückliche datenschutzrechtliche Pflichten hinzu: Nach Art. 9 Abs. 2 DSG muss sich der Verantwortliche vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Soweit die DSGVO anwendbar ist, verlangt Art. 28 Abs. 1 DSGVO hinreichende Garantien; Art. 28 Abs. 3 Bst. h DSGVO regelt die Bereitstellung von Nachweisen und die Ermöglichung von Überprüfungen. Welche Prüfungshandlungen angemessen sind, richtet sich nach Risiko und Kontext.

Die bisherigen Beiträge dieser Reihe haben gezeigt, dass Anforderungen erst dann tragen, wenn ihre Erfüllung nachgewiesen ist. Das Whitepaper Business Continuity Management beschreibt diesen Nachweis als Rückweg: Anforderungen werden bis zum Dienstleister weitergegeben, ihre Erfüllung muss in umgekehrter Richtung belegt werden. Die hier beschriebenen Prüfwerkzeuge sind die Instrumente dieses Rückwegs.

Methodischer Rahmen: ITAF und ISO 19011

Für das Modell dieses Whitepapers sind aus dem IT Audit Framework (ITAF), 5. Ausgabe, von ISACA drei Aspekte besonders relevant: risikobasierte Prüfplanung, hinreichende (sufficient) und geeignete (appropriate) Prüfungsnachweise sowie die Auswahl angemessener Prüfmethoden nach fachlichem Ermessen.

ISO 19011 («Leitfaden zur Auditierung von Managementsystemen») empfiehlt ausdrücklich, Umfang, Häufigkeit und Tiefe von Audits risikobasiert auszurichten und dabei einen nachweisbasierten Auditansatz zu verfolgen.

Dieses Whitepaper überträgt diese Ansätze auf ein eigenes Modell mit vier Prüfwerkzeugen. Prüfintensität und Aufwand werden risikogerecht bemessen; die Nachweise müssen eine belastbare Beurteilung der jeweiligen Prüffrage ermöglichen.

Wie Risikokategorien, Prüfschwerpunkte und Prüfrhythmus zusammenhängen, beschreibt Kapitel 2.

1.3 Vier Grundwerkzeuge im Überblick

Für die praktische Umsetzung stehen vier Grundwerkzeuge zur Verfügung, die sich in Tiefe, Aufwand und in den Nachweisen unterscheiden, die sie zugänglich machen. Sie lassen sich kombinieren und ergänzen sich gegenseitig:

- Selbstdeklaration: Schriftliche Bestätigung des Leistungserbringers anhand eines Fragebogens; kostengünstig und breit einsetzbar, aber ohne unabhängige Verifikation.
- Dokumenten- und Nachweiskontrolle (kurz: Nachweiskontrolle): Gezielte Prüfung eingeforderter Unterlagen (Vorgaben, Betriebsnachweise wie Logs oder Tickets, Auditberichte, Zertifikate); effizient und ortsunabhängig.
- Vor-Ort-Besuch: Direkte Inaugenscheinnahme beim Dienstleister; kooperativ, dialogorientiert, mit Einblick in ausgewählte Abläufe und die Sicherheitskultur.
- Formales Audit: Systematische Prüfung gegen festgelegte Kriterien, methodisch nach ISO 19011; tiefgehend und dokumentiert, aber ressourcenintensiv.

Die vier Werkzeuge sind praxisbezogene, teilweise überlappende Formen der Nachweisgewinnung, keine getrennten Methoden oder zwingenden Eskalationsstufen. Ein formales Audit kann Dokumentenprüfungen, Interviews, Beobachtungen und technische Tests verbinden und vor Ort, remote oder kombiniert erfolgen. Technische Prüfungen, etwa Konfigurationsprüfungen, Wiederherstellungstests oder Penetrationstests, können eigenständige Prüfaktivitäten sein oder Nachweise für die beschriebenen Werkzeuge liefern.

2 Risikokategorien und Werkzeugzuweisung

Die Risikokategorie wird aus der Kritikalität der bezogenen Leistung, dem Schutzbedarfsprofil der betroffenen Informationen und Systeme sowie den wesentlichen Risiken der Leistungsbeziehung abgeleitet. Berücksichtigt werden insbesondere die möglichen Folgen einer Offenlegung, Verfälschung, Nichtverfügbarkeit oder fehlenden Nachvollziehbarkeit sowie Exposition, Abhängigkeiten, Konzentrationsrisiken, Subdienstleister und Exit-Fähigkeit. Ein einzelnes kritisches Schutzziel wird dabei nicht durch eine Gesamtbetrachtung relativiert. Die Kategorie bestimmt die Prüfpriorität, das Profil der betroffenen Schutzziele die Prüfschwerpunkte: Bei hohen Verfügbarkeitsanforderungen stehen etwa Wiederherstellungs- und Kontinu-

itätstests im Vordergrund, bei hohen Anforderungen an die Nachvollziehbarkeit die Auswertung von Protokollen. Tabelle 1 zeigt das grundlegende Mapping; Kategorie 1 bezeichnet geringes, Kategorie 4 sehr hohes Risiko, und die Tabelle beginnt mit der kritischsten Kategorie.

Kategorie	Typische Merkmale (Beispiele)	Werkzeuge (Auswahl)	Typischer Prüfauftrag und Schwerpunkte	Aufwand je Prüfauftrag und Rhythmus
Kat. 4 Sehr hoch	• Mindestens ein Schutzziel sehr hoch • z.B. GEHEIM klassifizierte Informationen oder für zentrale Prozesse unverzichtbare Leistungen	• Selbstdeklaration • Nachweiskontrolle • Vor-Ort-Besuch • formales Audit (ISO 19011)	Umfangreiche leistungsbezogene Prüfung relevanter ISMS-Prozesse und Kontrollen: Prozessbegehung, Interviews, technische Stichproben, Prüfung von BCM-Testnachweisen	**Aufwand:** 9–17 PT, bei hoher Komplexität mehr **Rhythmus:** vertiefte Prüfung jährlich, ergänzend Selbstdeklaration und Nachweiskontrolle
Kat. 3 Hoch	• Mindestens ein Schutzziel hoch • z.B. vertrauliche Informationen, besonders schützenswerte oder umfangreiche Personendaten • kritische oder abhängigkeitssensitive Systeme und Dienste	• Selbstdeklaration • engmaschige Nachweiskontrolle • Vor-Ort-Besuch • formales Audit	Vertiefte Prüfung ausgewählter Schwerpunkte: ISMS-Review, Schlüsselkontrollen, Schwachstellen-Management, Incident-Prozesse, Interviews	**Aufwand:** 5–9 PT **Rhythmus:** vertiefte Prüfung alle 1–2 Jahre; in Jahren ohne vertiefte Prüfung Selbstdeklaration und gezielte Nachweiskontrolle
Kat. 2 Mittel	• Interne, nicht öffentliche Informationen • Personendaten ohne hohes Risiko; Standardsysteme	• Selbstdeklaration • stichprobenartige Nachweiskontrolle • Vor-Ort-Besuch bei Bedarf	Thematisch begrenzte Nachweiskontrolle: Compliance-Check ausgewählter Kontrollen, Stichproben	**Aufwand:** 1–3 PT **Rhythmus:** Nachweiskontrolle alle 2–3 Jahre, Selbstdeklaration regelmässig
Kat. 1 Gering	Kein Zugang zu nicht öffentlichen Informationen oder kritischen Systemen	• initiale Selbstdeklaration • anlassbezogene Kontrolle	Kurzes Screening oder begrenzte anlassbezogene Nachweiskontrolle; Fokus auf vertragliche Absicherung	**Aufwand:** 0.25–0.5 PT **Rhythmus:** nur anlassbezogen, keine planmässigen Audits

Tabelle 1: Risikokategorien und zugeordnete Prüfwerkzeuge (eigene Darstellung)

Die Zuordnung von Werkzeugen zu Risikokategorien ist kein mechanisches Schema. Zusätzliche Faktoren können dazu führen, dass trotz gleicher Grundkategorie eine höhere Prüftiefe erforderlich ist. Beispiele sind Konzentrationsrisiken bei wenigen Schlüsseldienstleistern, fehlende Exit-Fähigkeit, hohe Subdienstleisterdichte, eine belastete Incident-Historie oder bekannte regulatorische Schwächen. Die Werkzeugwahl bleibt eine risikoorientierte Ermessensentscheidung, die über die Kategorie hinaus den spezifischen Kontext berücksichtigt.

Die Personentage (PT) sind Orientierungswerte für die Planung je Prüfauftrag und geprüfter Leistung. Sie umfassen den Aufwand aller beteiligten Personen der prüfenden Organisation für Vorbereitung, Durchführung, Berichterstattung und erste Massnahmenabstimmung; zwei Prüfende mit je drei Tagen Einsatz ergeben sechs PT. Den Werten liegt ein Prüfteam von einer bis zwei Personen zugrunde, in Kategorie 4 von zwei

Personen mit zwei bis vier Durchführungstagen. Mehrere Standorte, technische Tests über die vorgesehenen Stichproben hinaus oder die Begleitung einer BCM-Übung erhöhen den Aufwand und werden gesondert geplant. Der Jahresaufwand ergibt sich aus der Zahl der geplanten Prüfaufträge. Ergänzende Selbstdeklarationen, Nachweiskontrollen, Nachtests und anlassbezogene Prüfungen werden im Jahresplan gesondert berücksichtigt, soweit sie nicht Bestandteil des Auftrags sind. Der konkrete Aufwand richtet sich nach Prüfziel, Scope, Komplexität, Kooperationsbereitschaft und verfügbaren Nachweisen. Der Aufwand des geprüften Leistungserbringers ist nicht enthalten und kann in ähnlicher Grössenordnung liegen. Aus der Kategorie allein lässt sich kein verbindlicher Mindestaufwand ableiten.

Die Rhythmen in Tabelle 1 sind Orientierungswerte für die Prüfplanung: Intervalle und Schwerpunkte werden anhand des Risikoprofils, vorhandener Nachweise und wesentlicher Veränderungen festgelegt. Auch bei jährlicher vertiefter Prüfung können die Schwerpunkte wechseln, und geeignete Fremdprüfungen können nach Abschnitt 5.2 angerechnet werden.

Diese Kategorisierung ist nicht statisch: Verändert sich das Risikoprofil (z.B. durch neue Leistungen, Sicherheitsvorfälle oder eine veränderte Bedrohungslage), wird die Einstufung angepasst und das Prüfprogramm entsprechend aktualisiert. Anlassbezogene Prüfungen können jederzeit und unabhängig von der Kategorie ausgelöst werden.

> **Prinzip der Verhältnismässigkeit**
>
> Risikobasiertes Prüfen bedeutet nicht, bei niedrigen Kategorien die Augen zu schliessen.
>
> Auch bei geringem Risiko gelten vertragliche Mindestanforderungen; die Prüfintensität bleibt bewusst schlank.

3 Belastbarkeit von Prüfungsnachweisen

Prüfwerkzeuge unterscheiden sich nicht nur im Aufwand, sondern auch in den Prüfungsnachweisen (Evidenz), die sie zugänglich machen. Das IT Audit Framework (ITAF) von ISACA verlangt, Prüfziele, Prüfmethoden und erwartete Nachweise so aufeinander abzustimmen, dass auf Basis ausreichender (sufficient) und geeigneter (appropriate) Nachweise eine verlässliche Beurteilung möglich ist. Die Belastbarkeit von Prüfungsnachweisen ergibt sich aus ihrer Eignung für das Prüfziel, der Verlässlichkeit ihrer Quelle, der Art ihrer Erhebung sowie ihrem sachlichen und zeitlichen Bezug. Das gewählte Werkzeug schafft dafür unterschiedliche Möglichkeiten, legt die Nachweisqualität aber nicht allein fest. Eine systematische Auswertung von Betriebsnachweisen oder eines unabhängigen Typ-II-Berichts kann für eine bestimmte Prüffrage belastbarer sein als ein kurzer Vor-Ort-Besuch.

Entscheidend ist, ob die Nachweise die beabsichtigte Aussage ausreichend und nachvollziehbar tragen. Fehlt es am Umfang, kann eine grössere Stichprobe oder ein längerer Betrachtungszeitraum genügen. Fehlt es an der Eignung, helfen mehr gleichartige Nachweise nicht; dann sind andere oder ergänzende Nachweise und Prüfungshandlungen zu wählen.

Die Beurteilung unterscheidet zwischen der Angemessenheit einer Kontrolle (Design Effectiveness) und ihrer tatsächlichen Wirksamkeit im betrachteten Zeitraum (Operating Effectiveness). Design Effectiveness bedeutet mehr als das Vorhandensein einer Vorgabe: Gefragt ist, ob die Kontrolle bei sachgerechter Anwendung das Kontrollziel erreichen kann. Vorgabedokumente zeigen, wie eine Kontrolle ausgestaltet ist. Betriebsnachweise, etwa Tickets, Rezertifizierungen, Protokolle oder Wiederherstellungstests, können ihre Anwendung und Ergebnisse über einen Zeitraum belegen, sofern Inhalt, Abdeckung und Ergebnisse ausge-

wertet werden. Beobachtung und Nachvollzug vor Ort ergänzen diese Nachweise, zeigen aber zunächst einen Zeitpunkt. Welche Perspektive ein Werkzeug ermöglicht, hängt deshalb von den erhobenen Nachweisen und Prüfungshandlungen ab. Eine belastbare Beurteilung erfordert bei höheren Risikokategorien in der Regel beide Perspektiven.

Eng damit verbunden ist das Risiko einer falschen Sicherheit: Formale Nachweise wie ausgefüllte Fragebögen, aktuelle Zertifikate oder vorgelegte Richtlinien können Sicherheit suggerieren, ohne diese tatsächlich ausreichend zu belegen. Dieses Risiko ist besonders dann hoch, wenn Nachweise ohne kritische Einordnung ihrer Grenzen verwendet werden oder wenn das Ergebnis einer Prüfung mit dem Zustand der tatsächlichen Sicherheitslage gleichgesetzt wird. Tabelle 2 zeigt den typischen Beitrag und die Grenzen der vier Werkzeuge.

Werkzeug	Typischer Beitrag zur Beurteilung	Wesentliche Begrenzung
Selbstdeklaration	Strukturierte Selbstauskunft und Screening; die Aussage bleibt indikativ	Angaben werden durch die Deklaration allein nicht unabhängig verifiziert
Dokumenten-/Nachweiskontrolle	Prüfung von Vorgabedokumenten, Betriebsnachweisen und Berichten Dritter	Aussage hängt von Herkunft, Verlässlichkeit, Vollständigkeit, Zeitraum und Leistungsbezug der Nachweise ab
Vor-Ort-Besuch	Beobachtung, Gespräche und gezielter Nachvollzug ausgewählter Abläufe	Punktuelle, bei angekündigten Besuchen möglicherweise vorbereitete Situation
Formales Audit (ISO 19011)	Systematische Bewertung gegen festgelegte Kriterien mit dokumentierter Schlussfolgerung	Aussage bleibt durch Scope, Methoden, Stichprobe und Nachweisqualität begrenzt

Tabelle 2: Typische Beiträge und Grenzen der Prüfwerkzeuge (eigene Darstellung)

Je höher das Risiko, desto belastbarere Nachweise sind erforderlich. Typische Prüfmethoden sind Befragung, Inspektion von Dokumenten und Aufzeichnungen, Beobachtung, Nachvollzug und technische Tests. In der Praxis werden sie kombiniert; ihre Gewichtung richtet sich nach Prüfziel und Risikokategorie.

3.1 Nachweislücken entscheiden

Die Werkzeugwahl erfolgt innerhalb des genehmigten Prüfprogramms nach fachlichem Ermessen. Ressourcen beeinflussen Priorität, Zeitpunkt, Scope und Stichprobenumfang. Sie ändern aber nicht, welche Nachweise eine bestimmte Schlussfolgerung tragen müssen. Wird weniger geprüft, wird die Reichweite der Aussage entsprechend enger.

Reichen die verfügbaren Nachweise für eine wesentliche Prüfaussage nicht aus, werden die Nachweislücke, ihre Ursachen und die daraus entstehende Unsicherheit dokumentiert. Ursachen können begrenzte Ressourcen, fehlende Prüfrechte oder die Marktmacht eines Anbieters sein. Die zuständige Entscheidinstanz legt fest, ob zusätzliche Mittel, andere Nachweisquellen, ergänzende Prüfungen oder ausgleichende Massnahmen erforderlich sind. Verbleibt eine wesentliche Unsicherheit, ist deren Akzeptanz ausdrücklich zu entscheiden und mit einer Frist zur erneuten Beurteilung zu versehen. Zwingende rechtliche Anforderungen bleiben dabei einzuhalten.

Eine Nachweislücke beweist noch keine unwirksame Kontrolle. Sie begrenzt zunächst die Sicherheit der Aussage. Wird sie aber nicht benannt, gilt sie stillschweigend als Sicherheit, und das verbleibende Risiko wird getragen, ohne dass jemand darüber entschieden hat.

> **Beispiel: Die offene Prüffrage bestimmt den nächsten Schritt**
>
> Für einen kritischen SaaS-Dienst liegt ein aktueller SOC-2-Typ-II-Bericht vor. Die Auswertung zeigt, dass die Rezertifizierung der Berechtigungen als kundenseitige Kontrolle der eigenen Organisation zugewiesen ist und dass für die Zeit seit Berichtsende keine Angaben vorliegen. Statt eines allgemeinen Vor-Ort-Besuchs werden deshalb gezielt die eigenen Rezertifizierungsnachweise geprüft und beim Anbieter eine Bestätigung zu wesentlichen Änderungen seit Berichtsende eingeholt. Nicht das nächsthöhere Werkzeug ist der nächste Schritt, sondern die Prüfhandlung, die die offene Frage beantwortet.

4 Die vier Prüfwerkzeuge im Detail

4.1 Selbstdeklaration

Die Selbstdeklaration ist das ressourcenschonendste Prüfinstrument. Der Leistungserbringer bestätigt schriftlich auf Basis eines standardisierten Fragebogens oder einer Checkliste, dass er definierte Sicherheitsanforderungen einhält. Typische Inhalte sind: Vorhandensein eines Informationssicherheits-Managementsystems (ISMS), Patch-Management, Zugangskontrollen, Incident-Response-Prozesse, Backup-Strategie und Schulungsmassnahmen.

Stärken

- Geringe Kosten für beide Seiten, skalierbar über viele Leistungserbringer
- Breitenwirkung: Erzeugt Bewusstsein und verpflichtet zur Selbstreflexion
- Eignet sich als Einstiegsinstrument (Onboarding) und für regelmässige Statusabfragen
- Kann anlassbezogen oder periodisch eingesetzt werden, ohne grossen Planungsaufwand

Grenzen

- Indikative Aussage: Angaben werden durch die Deklaration allein nicht unabhängig verifiziert
- Anfällig für «Check-the-Box»-Verhalten, insbesondere ohne klare Konsequenzen
- Deckt nur deklarierte, nicht tatsächlich gelebte Sicherheitspraktiken ab
- Fehlende Tiefe bei komplexen, vernetzten Systemen oder Subdienstleistern

> **Praktische Empfehlung**
>
> Selbstdeklarationen sind als alleiniges Instrument nur bei geringem Risikopotenzial angemessen (Kategorie 1). Bei höheren Kategorien dienen sie als Einstiegs- und Screening-Instrument, dessen Unstimmigkeiten oder Lücken eine Beurteilung nach Abschnitt 6.2 auslösen. Empfehlenswert ist eine regelmässige Selbstdeklaration, deren Rhythmus sich nach Risiko und Veränderungen richtet (in der Praxis meist jährlich), mit gezielten Nachfragen zu sicherheitsrelevanten Ereignissen (Vorfälle, Systemänderungen, Zertifizierungsstatus).

4.2 Dokumenten- und Nachweiskontrolle

Die Nachweiskontrolle geht einen Schritt weiter: Der Prüfer fordert konkrete Unterlagen und Nachweise ein und prüft diese systematisch. Dies kann remote erfolgen (Desk Audit) oder als punktuelle Prüfung vor Ort. Typische Nachweise sind: Penetrationstest-Reports, Berechtigungskonzepte, Sicherheitsrichtlinien, Audit-Logs, Tickets, Berechtigungsrezertifizierungen, Wiederherstellungsprotokolle, Zertifikate (z.B. ISO/IEC 27001), Schulungsnachweise und Vorfallmeldungen. Zu unterscheiden sind Vorgabedokumente, die das Design einer Kontrolle zeigen, und Betriebsnachweise, die ihre Anwendung über einen Zeitraum belegen können.

Stärken

- Prüft konkrete, nachvollziehbare Artefakte, einschliesslich Betriebsnachweisen über einen Zeitraum
- Effizient und ortsunabhängig, keine Reisekosten, zeitlich flexibel
- Geeignet für spezifische, thematisch begrenzte Prüfungen und Follow-up
- Kann kurzfristig und anlassbezogen eingesetzt werden

Grenzen

- Aussage ist auf die vorgelegten und verifizierten Nachweise begrenzt; Vorgabedokumente allein belegen keine tatsächliche Wirksamkeit
- Dokumente können veraltet, unvollständig oder selektiv aufbereitet sein
- Direkte Beobachtung und informelle Gesprächseindrücke fehlen; Sicherheitskultur bleibt schwer erkennbar
- Erfordert klare Vorab-Definition, welche Nachweise einzufordern sind

> **Typische Anwendungsfälle**
>
> Die Nachweiskontrolle ist besonders wertvoll für die Nachverfolgung von Massnahmenplänen (Follow-up nach Audits), für die Überprüfung von Zertifizierungen und deren Gültigkeit sowie für stichprobenartige Prüfungen bei Dienstleistern der Kategorie 2.

4.3 Vor-Ort-Besuch

Als Vor-Ort-Besuch wird in diesem Papier eine thematisch begrenzte, dialogorientierte Prüfmassnahme ausserhalb eines formalen Audits bezeichnet. Er erfolgt in der Regel angemeldet und umfasst Gespräche mit Verantwortlichen, Begehungen relevanter Bereiche (z.B. Rechenzentrum, Büroumgebung) sowie Stichproben ausgewählter Kontrollen. Gerade weil er keinen formalen Prüfcharakter hat, ist die Atmosphäre oft offen: Gesprächspartner sprechen direkter über Herausforderungen und offene Punkte als in einem formalen Auditkontext. Vor-Ort-Aktivitäten können ebenso Bestandteil eines formalen Audits sein.

Eine strukturelle Einschränkung verdient dabei besondere Beachtung: Ein angekündigter Besuch kann einen gezielt vorbereiteten Zustand zeigen; seine Aussage über den Regelbetrieb ist daher kritisch einzuordnen. Das ist kein Argument gegen das Instrument, aber ein blinder Fleck, den man kennen muss, um die Ergebnisse richtig zu gewichten. Abfedern lässt er sich durch vor Ort spontan gewählte Stichproben, Gespräche mit operativ tätigen Mitarbeitenden statt ausschliesslich mit Führungsverantwortlichen sowie den Abgleich der Beobachtungen mit vorab eingeforderten Dokumenten.

Stärken

- Beobachtung und Nachvollzug ausgewählter Abläufe im Betrieb
- Deckt «weiche» Faktoren auf: Sicherheitskultur, Awareness, Priorisierung im Alltag
- Fördert Vertrauen und Zusammenarbeit, vermittelt Erwartungen klar
- Geringerer formaler Aufwand als ein vollständiges Audit

Grenzen

- Keine formale Auditfeststellung; Befunde sind informeller Natur
- Begrenzte Prüftiefe: Keine umfassende, kriterienbasierte Prüfung aller vereinbarten Themen
- Ergebnis abhängig von Vorbereitung und ausgewählten Schwerpunktthemen
- Reise und Koordination: höherer Logistikaufwand als Remote-Kontrolle

> **Vorbereitung als Erfolgsfaktor**
>
> Ein Vor-Ort-Besuch ist nur so gut wie seine Vorbereitung. Ohne klare Schwerpunkte (z.B. Zugangskontrollen, Backup-Prozesse, Incident-Management) und strukturierte Leitfäden entstehen unproduktive Rundgänge ohne verwertbare Erkenntnisse. Empfehlenswert: Kurzbericht mit Protokoll der wesentlichen Beobachtungen und offenen Punkten, auch wenn kein formaler Auditbericht erstellt wird.

4.4 Formales Audit (geplante, vertiefte Prüfung)

Ein formales Audit ist eine systematische, unabhängige, dokumentierte Prüfung gegen festgelegte Kriterien. Es folgt einem definierten Auditprogramm, orientiert sich methodisch an den Leitlinien von ISO 19011 und an ITAF und kombiniert geeignete Prüfmethoden entsprechend Auftrag, Prüfziel und Risiko, vor Ort, remote oder kombiniert. Seine Aussagekraft hängt von Scope, Methoden, Stichprobe und Qualität der erhobenen Nachweise ab.

Kernelemente eines formalen Audits umfassen: Auditplanung mit Definition von Scope, Kriterien und Prüfteam; Auditvorbereitung mit Dokumentenstudium und Prüfprogrammentwicklung; Auditdurchführung mit Eröffnungsgespräch, Interviews, Begehungen, Stichproben und Nachweisprüfungen; Auditberichterstattung mit Feststellungen (Nichtkonformitäten, Beobachtungen, Verbesserungspotenziale); sowie Nachverfolgung mit verbindlichem Massnahmenplan und Follow-up-Kontrolle.

Stärken

- Systematische Prüfung aller Kontrollbereiche im vereinbarten Scope
- Formale, kriterienbasierte Feststellungen als Grundlage verbindlicher Massnahmen
- Belastbare Grundlage für vertragliche Folgemassnahmen
- Vergleichbarkeit über Zeit und Prüfobjekte hinweg (festgelegte Kriterien)

Grenzen

- Sehr hoher Ressourcenaufwand, auch auf Seiten des geprüften Dienstleisters: Koordination, Dokumentenbereitstellung, Ansprechpartner-Verfügbarkeit
- Nicht für alle Risikosituationen und Kategorien verhältnismässig
- Zeitverzug: Zwischen Planung, Durchführung und finalem Bericht vergehen oft mehrere Wochen
- Erfordert fachlich qualifiziertes, unabhängiges Prüfteam

Auditgrundsätze nach ISO 19011

ISO 19011 beschreibt sieben Grundsätze für die Auditierung von Managementsystemen: Integrität, objektive Darstellung, professionelle Sorgfalt, Vertraulichkeit, Unabhängigkeit sowie einen nachweisbasierten und einen risikobasierten Ansatz. Die Auditziele ergeben sich aus Zweck und Auftrag der Prüfung; vertragliche Vorgaben, Normen (z.B. Kontrollen nach ISO/IEC 27002) und regulatorische Anforderungen dienen als Auditkriterien. Die Befunde werden zur sachlichen Klärung besprochen, nicht aufgelöste Meinungsunterschiede dokumentiert. Prüfung und Freigabe des Auditberichts erfolgen nach den im Auditprogramm festgelegten Zuständigkeiten. Der Bericht wird unter Wahrung der Vertraulichkeit an die vorgesehenen Empfänger verteilt. Für erforderliche Massnahmen werden Verantwortliche, Termine und die Überprüfung der Wirksamkeit festgelegt.

5 Kombination und Anrechnung von Nachweisen

5.1 Kombination und Sequenzierung

In der Praxis werden die Werkzeuge selten isoliert eingesetzt. Eine durchdachte Kombination und Sequenzierung erhöht die Aussagekraft der Nachweise bei gezieltem Ressourceneinsatz. Bewährte Muster:

- Screening → Vertiefung: Selbstdeklaration als Basis-Screening; bei Auffälligkeiten oder höherer Risikokategorie Eskalation zur Nachweiskontrolle oder zum Audit.
- Nachweiskontrolle + Vor-Ort-Besuch: Unterlagenprüfung im Vorfeld schärft die Schwerpunkte des Besuchs. Das ist effizienter, als beide Instrumente unabhängig voneinander einzusetzen.
- Audit + Follow-up: Nach einem formalen Audit werden Umsetzung und, soweit risikorelevant, Wirksamkeit der vereinbarten Massnahmen anhand geeigneter Nachweise und bei Bedarf durch Nachtests überprüft, ohne erneuten vollen Auditaufwand.

5.2 Anrechnung fremder Prüfungen

Ein gültiges ISO/IEC-27001-Zertifikat enthält eine unabhängige Konformitätsaussage zum Informationssicherheits-Managementsystem im angegebenen Geltungsbereich. Es ist ein relevanter Nachweis, aber keine Garantie für die Sicherheit jeder bezogenen Leistung oder die Wirksamkeit jeder einzelnen Kontrolle, und es belegt nicht, dass die Verhältnisse seit dem letzten Audit unverändert geblieben sind. Für die eigene Beurteilung sind Geltungsbereich, Gültigkeit, zugrunde liegende Prüfungen und die Relevanz für die bezogene Leistung zu berücksichtigen. Geeignete Prüfungen Dritter, etwa Zertifizierungsaudits akkreditierter Stellen nach ISO/IEC 27006-1 oder unabhängige Assuranceberichte, können eigene Prüfungshandlungen reduzieren oder teilweise ersetzen, wenn Scope, Kriterien, Zeitraum, Kompetenz, Unabhängigkeit und Ergebnisse zur eigenen Prüffrage passen. Das eigene Prüfrecht ersetzen sie nicht. Die Verantwortung für ihre Auswertung und den Umgang mit verbleibenden Nachweislücken bleibt bei der beauftragenden Organisation. Stützt sich die Beurteilung ausschliesslich auf Zertifikate, bleibt zu entscheiden und zu dokumentieren, welche Nachweislücken damit verbleiben (Abschnitt 3.1).

Grenzfall Cloud und Grossanbieter

Bei Hyperscalern und grossen SaaS-Anbietern sind eigene Prüfungen häufig nur eingeschränkt und in standardisierten Formen möglich. Ein Rechenzentrumsbesuch allein genügt nicht zur Beurteilung der bezogenen Cloud-Leistung. Im Vordergrund stehen Assuranceberichte, ergänzende Nachweise zu Cloud-Kontrollen (ISO/IEC 27017) und zum Schutz von Personendaten (ISO/IEC 27018), gemeinsame Kundenprüfungen (Pooled Audits) sowie Remote-Prüfaktivitäten unter Berücksichtigung von ISO 19011:2026. Geeignet sind SOC-2-Typ-II-Berichte oder passend abgegrenzte Berichte nach ISAE 3000 (Revised). ISAE-3402-Berichte kommen nur infrage, soweit ihre auf die Finanzberichterstattung bezogenen Kontrollziele die eigene Prüffrage abdecken. Vorhandene Prüfrechte und ihre praktische Nutzung sind zu klären.

Entscheidend ist die Auswertung: Ein Typ-II-Bericht deckt nur den geprüften Zeitraum, die einbezogenen Services und Kontrollziele ab. Zu beurteilen sind Scope, Ausnahmen, Feststellungen, Prüfungssicherheit und die Behandlung wesentlicher Subdienstleister. Die Complementary User Entity Controls bezeichnen die der eigenen Organisation zugewiesenen Kontrollen; deren Umsetzung ist sicherzustellen. Bei ausgeschlossenen Subdienstleistern (Carve-out) sind verbleibende Abhängigkeiten und ergänzende Nachweise zu klären. Für die Zeit seit Berichtsende sind relevante Änderungen, Vorfälle und zusätzliche Nachweise zu berücksichtigen.

Verbleibende Nachweislücken werden nach Abschnitt 3.1 entschieden. Weitere Auswertungskriterien enthält das Whitepaper IT-Outsourcing & Governance dieser Reihe.

6 Anlassbezogene Prüfungen

Anlassbezogene Prüfungen ergänzen den geplanten Prüfzyklus bei neuen Risikosignalen, unabhängig von der Risikokategorie des Leistungserbringers.

6.1 Typische Auslöser

- Sicherheitsvorfälle: Cyberangriff auf den Leistungserbringer, Datenleck, Ransomware-Befall, ungeplante Systemausfälle
- Wesentliche Änderungen: Architekturwechsel, Major Release, Wechsel kritischer Subdienstleister, Fusion oder Übernahme
- Vertragskontext: Vertragsverletzungen, nicht fristgerecht umgesetzte Massnahmen, Verzug bei der Behebung von Mängeln
- Externe Signale: Medienberichte über Sicherheitsprobleme, regulatorische Massnahmen gegen den Leistungserbringer
- Befunde und Warnungen: Kritische Feststellungen bei Zertifizierungsaudits, öffentlich bekannte Schwachstellen (CVEs), Warnungen nationaler und internationaler Cybersicherheitsbehörden[1]

[1] z.B. BACS (Bundesamt für Cybersicherheit, CH), BSI (Bundesamt für Sicherheit in der Informationstechnik, DE), ENISA (European Union Agency for Cybersecurity) sowie CISA (Cybersecurity and Infrastructure Security Agency, US). Diese Behörden veröffentlichen regelmässig Warnungen, Advisories und Threat Alerts zu bekannten Schwachstellen und aktiven Angriffskampagnen.

6.2 Entscheidungsprozess

Die Entscheidung über eine anlassbezogene Prüfung trifft idealerweise die für Informationssicherheit verantwortliche Stelle gemeinsam mit dem fachlichen Leistungsverantwortlichen (Business Owner) sowie, je nach Kritikalität, unter Einbezug von Risikomanagement, Datenschutz oder BCM. Massgebend ist die Frage, wie relevant das Signal für die eigene Organisation ist, auch über mittelbare Abhängigkeiten, und welche Klärung oder Reaktion angemessen ist: eine vertiefte Prüfung, eine gezielte Nachweisanforderung oder zunächst die weitere Beobachtung.

> **Reaktionszeiten und Eskalation**
>
> Bei schwerwiegenden Sicherheitsvorfällen beim Leistungserbringer empfiehlt sich eine sofortige erste Reaktion: Direkte Kommunikation aufnehmen, eigene Exposition einschätzen sowie erforderliche Schutzmassnahmen treffen. Zeitpunkt und Umfang einer anlassbezogenen Prüfung werden, sofern vertraglich möglich, so festgelegt, dass sie zur laufenden Vorfallbewältigung passen.

7 Prüfplanung in der Praxis

7.1 Der jährliche Kontroll- und Prüfplan

Grundlage ist ein Jahresplan, der die wesentlichen Systeme und bezogenen Leistungen, ihre Risikokategorie sowie geplante Prüfmassnahmen, Zeitpunkte und Zuständigkeiten dokumentiert. Er ist kein bürokratisches Dokument, sondern ein operatives Steuerungsinstrument.

Wesentliche Grundsätze für den Prüfplan:

- Risikoorientierung: Ressourcen fliessen primär in Prüfungen mit hohem Risikoniveau und hohem Nachweisbedarf; geringe Risiken erhalten schlanke Instrumente.
- Abdeckung: Der im Prüfprogramm festgelegte Prüfrhythmus bildet den Regelfall. Können geplante Prüfungen nicht durchgeführt werden, werden die entstehende Nachweislücke, verfügbare ergänzende Nachweise und erforderliche vorübergehende Massnahmen beurteilt. Wesentliche Abweichungen werden nach Abschnitt 3.1 entschieden und mit einem neuen Prüftermin versehen.
- Neuzugänge: Neue Dienstleister werden vor der Beauftragung risikogerecht beurteilt. Vor der Übernahme kritischer Leistungen oder dem Beginn der Datenbearbeitung werden die erforderlichen Sicherheitsnachweise und Freigaben eingeholt. Die erste vertiefte Prüfung der Betriebswirksamkeit folgt nach Aufnahme des Betriebs in einem risikobasiert festgelegten Zeitraum.
- Flexibilität: Der Plan wird jährlich fortgeschrieben und unterjährig, etwa quartalsweise, auf neue Risikosignale überprüft. Anlassbezogene Prüfungen ersetzen oder ergänzen geplante Massnahmen.

7.2 Vorbereitung, Durchführung und Nachbereitung

Jede professionelle Prüfung folgt einem dreiteiligen Grundschema, dessen Umfang sich nach Werkzeug und Risiko richtet. Auf Seiten der prüfenden Organisation sind typischerweise mehrere Funktionen einzubinden: die für Informationssicherheit verantwortliche Stelle (Planung, fachliche Leitung), der fachliche Leistungsverantwortliche (Business Owner) für Kontextkenntnis und Entscheidkompetenz sowie bei formalen Audits gegebenenfalls die interne Revision oder externe Prüfer. Auf Seiten des Leistungserbringers sind Ansprechpartner aus IT, Informationssicherheit und operativem Betrieb einzuplanen. Die frühzeitige Klärung dieser Beteiligten ist Teil der Vorbereitung und vermeidet Verzögerungen in der Durchführung.

Die Frage, wer prüft, ist dabei keine Formalie. Kontrollen der zweiten Linie, in der Regel durch die für Informationssicherheit verantwortliche Stelle, und Prüfungen der dritten Linie durch die interne Revision unterscheiden sich in Auftrag, Unabhängigkeit und Berichtsweg. Externe Prüfer gehören nicht automatisch zur dritten Linie: Massgebend ist, in wessen Auftrag und mit welchem Berichtsweg sie tätig sind. Ein im Auftrag der Informationssicherheit tätiger externer Prüfer erweitert deren Kapazität, übernimmt aber nicht die Rolle der internen Revision. Für Prüfungen der internen Revision bleiben deren Auftrag, Planung, Freigabe und Berichtsweg vorbehalten. ISO 19011 betont einen unabhängigen und nachweisbasierten Ansatz: Wer die Leistungsbeziehung fachlich mitverantwortet oder den Vertrag ausgehandelt hat, sollte deren Wirksamkeit nicht abschliessend selbst beurteilen. Bei formalen Audits in den Kategorien 3 und 4 ist die organisatorische Trennung von Steuerung und Prüfung deshalb Teil der Prüfqualität und nicht bloss eine Frage der Ressourcenzuteilung.

Die drei Phasen im Überblick:

- Vorbereitung: Definition von Scope und Kriterien; Einholung relevanter Unterlagen; Erstellung von Leitfäden und Checklisten; Kommunikation mit dem Leistungserbringer (Terminankündigung, Dokumentenanforderung). Gut investierte Vorbereitungszeit reduziert den Durchführungsaufwand erheblich.
- Durchführung: Strukturierte Prüfung anhand der vorbereiteten Kriterien; kontinuierliche Kommunikation von Feststellungen; dokumentierte Nachweise (Protokolle, Screenshots, Dokumente als Evidenz).
- Nachbereitung: Erstellung eines Berichts oder Protokolls; Abstimmung der Befunde; verbindlicher Massnahmenplan mit Fristen und Verantwortlichkeiten; Nachverfolgung der Umsetzung und, soweit risikorelevant, der Wirksamkeit.

> **Der Massnahmenplan als zentrales Instrument**
>
> Abweichungen und risikorelevante Feststellungen werden bewertet. Der Massnahmenplan hält erforderliche Massnahmen, Verantwortliche und Fristen fest. Offene Punkte werden nachverfolgt, Verzögerungen eskaliert. Bei kritischen Abweichungen wird risikogerecht zwischen Dokumentennachweis, Nachtest und erneuter vertiefter Prüfung gewählt. Ein geschlossenes Ticket ist noch kein Wirksamkeitsnachweis. Für die Umsetzung bleibt das zuständige Management verantwortlich; eine begründete Akzeptanz verbleibender Risiken wird gesondert dokumentiert.

7.3 Vertragliche Absicherung externer Dienstleisterprüfungen

Prüfungen bei externen Dienstleistern brauchen eine vertragliche Grundlage. Ohne sie bleibt die Prüfung auf das beschränkt, was der Dienstleister freiwillig vorlegt. Gesetzliche Prüfbefugnisse und interne Prüfmandate bleiben davon unberührt. Prüfrechte, Meldepflichten, Nachweispflichten und Kostenregelungen müssen im Vertrag oder einem Sicherheits-Anhang verankert sein, und zwar vor Vertragsbeginn. Nachträgliche Verhandlungen über Prüfrechte sind schwierig und setzen die prüfende Partei in eine schwächere Position. Die folgenden Inhalte sind Beispiele, die im Einzelfall zu verhandeln sind; ergänzend beschreibt das Whitepaper IT-Outsourcing & Governance dieser Reihe die vertraglichen Steuerungsinstrumente.

- Prüfrechte: Recht zur Durchführung von Prüfungen mit angemessener Ankündigungsfrist (z.B. 20 Arbeitstage), bei Vorfällen verkürzt; Zugang zu Räumlichkeiten, Systemen und Unterlagen
- Nachweispflichten: Pflicht zur Vorlage von Sicherheitsberichten, Penetrationstest-Reports und Zertifikatsnachweisen
- Meldepflichten: Unverzügliche Meldung von Sicherheitsvorfällen (z.B. Erstmeldung innerhalb von 24 Stunden, Ergänzung später), abgestimmt auf die eigenen Meldepflichten
- Subdienstleister: Durchgängige Prüf- oder Nachweismöglichkeiten auch bei wesentlichen Subdienstleistern, direkt, vermittelt oder gemeinsam
- Kostenregelung: Jede Partei trägt eigene Kosten; bei wesentlichen Mängeln trägt der Leistungserbringer auch die Prüfkosten

Prüfnachweise: Geeignet sind insbesondere das Dienstleisterinventar mit begründeter Einstufung, der risikobasierte Prüfplan mit dem Ist des Vorjahres, dokumentierte Auswertungen relevanter Nachweise mit Scope und Zeitraum, Entscheide zu wesentlichen Nachweislücken (Abschnitt 3.1) sowie Massnahmen mit Fristen, Verantwortlichkeiten und Belegen ihrer Umsetzung und risikorelevanten Wirksamkeit. Fehlen für einen Dienstleister der Kategorie 4 belastbare Nachweise zur Betriebswirksamkeit und ein Entscheid über diese Lücke, ist nicht belegt, dass sein Risiko bewusst getragen wird.

8 Häufige Schwachstellen und Praxistipps

Aus der Prüfungspraxis lassen sich typische Schwachstellen und Stolpersteine identifizieren, die Prüfprogramme in ihrer Wirksamkeit einschränken (Tabelle 3):

Schwachstelle	Praxistipp
Prüfungen ohne klare Scope-Definition liefern Ergebnisse mit unklarer Abdeckung, die schwer einzuordnen sind	Scope und Kriterien vor der Prüfung schriftlich festlegen und abstimmen; erforderliche Nachweise vorab definieren
Selbstdeklarationen werden nicht ausgewertet oder lösen keine Folgemassnahmen aus	Systematische Auswertung mit definierten Eskalationsschwellen; Auffälligkeiten lösen die definierte Risikobeurteilung und gegebenenfalls eine vertiefte Prüfung aus
Massnahmenpläne werden erstellt, aber nicht konsequent nachverfolgt	Feste Follow-up-Termine im Prüfplan; monatliche Statusberichte bei kritischen Abweichungen; risikogerechte Nachprüfung bei Nichtumsetzung
Prüfrechte fehlen im Vertrag oder sind zu unscharf formuliert	Standardisierte Musterklausel mit klar definiertem Umfang, Fristen und Kostenregelung, bereits ab Vertragsabschluss
Prüfungen stützen sich auf Vorgabedokumente und blenden die tatsächliche Anwendung aus	Betriebsnachweise über einen Zeitraum auswerten; Vor-Ort-Besuche und Interviews gezielt für Dienstleister mit hohem Risiko einplanen; Nachweise aus Dokumenten und Beobachtung kombinieren
Interne Ressourcen reichen für vertiefte Prüfungen nicht aus	Externes Prüfteam oder spezialisierte Prüfstellen beiziehen; vorhandene Assuranceberichte und Zertifizierungsberichte gezielt als ergänzende Evidenz auswerten; bei formalen Audits die Unabhängigkeit von der Steuerung sicherstellen

Schwachstelle	Praxistipp
Nachweislücken werden nicht benannt und gelten stillschweigend als Sicherheit	Lücken nach Abschnitt 3.1 dokumentieren und entscheiden lassen
Neue Risikosignale werden im Jahresplan nicht berücksichtigt	Prüfplan regelmässig, etwa quartalsweise, überprüfen; Entscheidungsprozess für anlassbezogene Prüfungen vorab definieren

Tabelle 3: Typische Schwachstellen und Praxistipps (eigene Darstellung)

9 Leitfragen für Leitungs- und Aufsichtsgremien

Die folgenden Fragen eignen sich für eine Standortbestimmung. Sie zielen nicht auf einzelne Prüfberichte, sondern darauf, ob die Organisation erklären kann, worauf ihre Beurteilung wesentlicher Dienstleister beruht.

- Bei welchen wesentlichen Dienstleistern beruhen unsere Aussagen überwiegend auf ungeprüften Selbstauskünften?
- Welche Aussagen zur tatsächlichen Wirksamkeit können wir für welchen Zeitraum belegen?
- Reichen unsere Prüfressourcen für das, was unsere eigene Kategorisierung verlangt, und wer hat entschieden, was ungeprüft bleibt?
- Haben wir Prüf- und Nachweisrechte dort, wo wir sie am dringendsten bräuchten, auch bei Subdienstleistern?
- Ist für kritische Feststellungen nicht nur die Umsetzung, sondern auch die Wirkung der Massnahmen nachgewiesen?

Wo eine Antwort fehlt, liegt der erste Ansatzpunkt.

Fazit

Prüfergebnisse haben nur dann Wert, wenn sie die erforderlichen Entscheidungen tragen. Dafür müssen Prüfziele, Risikoprofil, Nachweise und Methoden zusammenpassen. Selbstdeklarationen, Dokumenten- und Nachweiskontrollen, Vor-Ort-Besuche und formale Audits leisten unterschiedliche Beiträge; keines dieser Werkzeuge garantiert allein eine bestimmte Nachweisqualität.

Wer risikobasiert prüft, konzentriert begrenzte Ressourcen auf wesentliche Fragen. Wo erforderliche Aussagen nicht ausreichend belegt werden können, bleiben Nachweislücken sichtbar und werden von der zuständigen Ebene entschieden. Und wer Feststellungen konsequent nachverfolgt, bis Umsetzung und risikorelevante Wirksamkeit belegt sind, schliesst den Regelkreis zwischen Erkenntnis und Verbesserung.

Entscheidend ist nicht die Zahl der Prüfungen, sondern ob ihre Nachweise eine belastbare Risikobeurteilung ermöglichen und wesentliche Nachweislücken bewusst behandelt werden.

Quellen

AICPA, SOC 2: Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy, Ausgabe 2022 (Stand 15. Oktober 2022).

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG, SR 235.1) vom 25. September 2020, insbesondere Art. 5 Bst. c und Art. 9.

IAASB, ISAE 3000 (Revised): Assurance Engagements Other than Audits or Reviews of Historical Financial Information, 2013; ISAE 3402: Assurance Reports on Controls at a Service Organization, 2009.

ISACA, IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit, 5. Ausgabe, 2026.

ISO 19011:2026, Guidelines for auditing management systems, 4. Ausgabe.

ISO/IEC 27001:2022 einschliesslich Amd 1:2024, Information security management systems. Requirements.

ISO/IEC 27002:2022, Information security controls.

ISO/IEC 27006-1:2024, Requirements for bodies providing audit and certification of information security management systems. Part 1: General.

ISO/IEC 27017:2026, Information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018:2025, Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors.

The Institute of Internal Auditors (IIA), Assurance and Advice in Support of Effective Governance: Three Lines Model, Statement of Position, Juli 2026.

Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO), insbesondere Art. 28.

Hinweis

Dieses Whitepaper gibt ausschliesslich meine persönliche fachliche Einschätzung wieder und steht nicht für eine Behörde oder Aufsicht. Es darf unverändert weitergegeben und mit Quellenangabe zitiert werden. Kommerzielle Verwertung und Bearbeitungen bedürfen meiner vorherigen Zustimmung.



Fragen und Austausch willkommen

carsten@carsten-beck.ch

Alle Beiträge der Reihe

carsten-beck.ch/publikationen

linkedin.com/in/carstenbeck-grc