Ein System, vier Blickwinkel

Ein Objektblatt je Gegenstand, eine Zutrittsliste je Raum und die Fragen an ein kombiniertes Audit: integriert wird der Gegenstand, nicht das Handbuch.

Kategorie: Arbeitsblatt. Bezug im Buch: Abschnitt 4.11 (Das Prinzip, sieben Regeln und Datenschutz, Operative Synthese); Norm: Klauseln 4.4, 5.2, 7.5, 8.1 und 9.2 der ISO/IEC 27001:2022 mit Änderung 1:2024 und Referenzmaßnahmen des Anhangs A (Fassung 2022); kombinierte und integrierte Audits nach ISO/IEC 17021-1, Auditzeit Informationssicherheit nach ISO/IEC 27006-1. Rechtsstand des Bandes: 28. September 2026.

Haus / Standort		**Ausgefüllt von**	
Gegenstand		**Stichtag**	

So nutzen Sie diese Vorlage

1. Wählen Sie einen Raum, holen Sie alle Beschreibungen, die die Systeme dazu enthalten, und füllen Sie das Objektblatt (Abschnitt 2) aus: eine Beschreibung mit vier Blickwinkeln statt vier Beschreibungen.
2. Vergleichen Sie die Zutrittslisten je Raum (Abschnitt 3) und tragen Sie die Fernzugänge ein (Abschnitt 4). Integration heißt nicht, alles in ein Dokument zu schreiben, sondern dieselben Tatsachen nur einmal aufzuschreiben.
3. Benennen Sie für jedes Objektblatt einen Eigentümer: Wer integriert, ohne Eigentümer zu benennen, erzeugt Papier ohne Verantwortung.

Spalte «Im Buch»: verlangt = von Norm, Regelwerk oder Recht verlangt, wie der Band es nennt (Quelle in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Anwendung in Schritten

Nr.	Schritt	Grund (aus dem Band)	Im Buch
1	Einen Raum wählen, alle Beschreibungen der Systeme dazu holen und die Zutrittslisten vergleichen.	Im Fall kamen sieben Dokumente aus vier Ordnern und zwei Laufwerken auf den Tisch, drei musste die Systemverantwortliche suchen.	Methode dieses Bandes
2	Die Fernzugänge der Anlagenbauer erfragen und aufschreiben, seit wann sie offen sind.	Diese Zugänge entstehen bei der Inbetriebnahme, sind nirgends dokumentiert und überleben jeden Systemwechsel.	Methode dieses Bandes
3	Objektblätter für die zwanzig bis dreißig wesentlichen Gegenstände anlegen, mit je einem Eigentümer; eine Zutrittsliste je Raum führen, die dem Schliessplan vorangeht; die drei Notfallpläne zu einem mit Kapiteln zusammenführen.	Die Liste gehört dorthin, wo die Schlüssel ohnehin herausgegeben werden, und besteht aus Name, Grundlage und Datum, nicht aus einer Datenbank.	Methode dieses Bandes
4	Das interne Audit auf Gegenstände ausrichten und mit der Zertifizierungsstelle das kombinierte Audit besprechen.	Jedes Haus hat drei bis fünf solcher Räume wie den Technikraum des Bades.	Methode dieses Bandes
5	Überwachen: je Raum die Zahl der Personen mit Zutritt gegen die Zahl der unterwiesenen Personen; die Zahl der dauerhaft offenen Fernzugänge.	Beispiel aus Abschnitt 4.11: vierzehn Schlüsselinhaber gegen vier unterwiesene Personen, zehn Personen ohne Unterweisung (Abschnitt 3).	Methode dieses Bandes

2 Das Objektblatt: acht Angaben, eine Seite je Gegenstand

Angabe	Eintrag	Angabe	Eintrag
1 Was es ist		5 Welche Gefahren bestehen	
2 Wo es ist		6 Welche Prüfungen und Intervalle gelten	
3 Wer verantwortlich ist (Eigentümer)		7 Welche Anbieter beteiligt sind	
4 Wer Zutritt oder Zugriff hat		8 Was im Notfall zu tun ist	

3 Zutrittsliste je Raum und Gegenüberstellung

Raum	Name	Grundlage (unterwiesen am / Vertrag vom)	Datum

Raum	Personen mit Zutritt (Schliessplan)	Unterwiesene Personen	Personen mit Zutritt ohne Unterweisung
Beispiel aus Abschnitt 4.11: Technikraum des Bades	14	4	10

Beispiel aus Abschnitt 4.11: zehn Personen können einen Raum betreten, für den sie nicht unterwiesen sind (14 minus 4); nach der Umstellung waren es sechs Schlüsselinhaber, die übrigen mit Zugang im Notfall über den Schlüsseltresor mit Protokoll.

4 Verzeichnis der Fernzugänge

Anbieter	Zweck	Zugangsweg	Freischaltung (auf Anforderung / dauerhaft)	Protokollierung

Regelfall ist der Zugang auf Anforderung; ein dauerhafter Zugang ist, wenn betrieblich nötig, begrenzt, protokolliert, regelmäßig ausgewertet und vertraglich unterlegt.

5 Prüffragen in der Reihenfolge des Abschnitts

Nr.	Frage	Befund	Grund (aus dem Band)	Im Buch
1	Gibt es für jeden wesentlichen Gegenstand ein Objektblatt mit den acht Angaben und einem Eigentümer?	☐ ja ☐ nein ☐ offen	Integriert wird der Gegenstand, nicht das Handbuch. Nichts in der Norm verlangt getrennte Dokumente je System; die Trennung stammt aus der Organisation der Häuser und dem Rhythmus der Audits.	Methode dieses Bandes; Anker 4.4 und 7.5
2	Gibt es eine Zutrittsliste je Raum, von einer Stelle geführt, mit Beschäftigten und Fremden, bei jedem Namen mit der Grundlage, auch für externe Techniker (Meldung von Personen als Vertragspflicht), und folgt der Schliessplan dieser Liste?	☐ ja ☐ nein ☐ offen	Unterweisung, persönliche Schutzausrüstung und Notfallplan richten sich an Personen; die Liste ist die Grundlage aller Schutzpflichten und zugleich die Liste der Informationssicherheit. In den meisten Häusern sind es zwei. Verträge führen Firmen auf, keine Menschen.	Methode dieses Bandes; Externe: verlangt (8.1); Schutzpflichten: Recht des Landes, Stand 28. September 2026
3	Gibt es einen Notfallplan mit Kapiteln, an einem Ort, mit einer ersten Nummer und der Verzweigung nach Art des Ereignisses?	☐ ja ☐ nein ☐ offen	Wer nachts allein ist, soll nicht entscheiden müssen, welches Managementsystem gerade zuständig ist; im Ernstfall liest niemand drei Pläne.	Methode dieses Bandes
4	Hat jeder Fernzugang einen Eintrag (Anbieter, Zweck, Zugangsweg, Freischaltung, Protokollierung), und ist ein dauerhafter Zugang begrenzt, protokolliert, regelmäßig ausgewertet und vertraglich unterlegt?	☐ ja ☐ nein ☐ offen	Die ältesten Zugänge eines Hauses führen fast immer in die Technik; die Wartungsverbindung überlebt Direktionen, Dienstleister und Betreiberwechsel.	Methode dieses Bandes; Referenzmaßnahmen Netze, Lieferantenbeziehungen (Anhang A, 2022)
5	Werden die gemeinsamen Elemente einmal geführt (Kontext und interessierte Parteien, Politik als ein Dokument mit vier Abschnitten, Rollen, Kommunikation, Lenkung der Dokumente, Schulung, Auditprogramm, Register der Feststellungen, Managementbewertung), und bleiben die fachlichen Kerne getrennt (Umweltaspekte, Gefährdungsbeurteilung, Risikobeurteilung der Informationssicherheit mit Erklärung zur Anwendbarkeit, Qualitätsprozesse)?	☐ ja ☐ nein ☐ offen	Die Normen folgen derselben Grundstruktur; vier Politiken in vier Ordnern vermitteln nichts.	verlangt (5.2: eine zum Zweck passende Politik); die Aufteilung: Methode dieses Bandes
6	Prüft das interne Audit Gegenstände (diesen Raum, diesen Dienstleister, diese Anlage) statt der Gliederung einer Norm?	☐ ja ☐ nein ☐ offen	Ein Gegenstandsaudit findet in zwei Stunden mehr als vier getrennte Audits in vier Tagen, weil es die Widersprüche zwischen den Systemen sieht.	verlangt (9.2: Auditprogramm nach Bedeutung der Prozesse); Gegenstandsprüfung: Methode
7	Ist die Integration nachweisbar (gemeinsame Politik, gemeinsame Bewertung, gemeinsames internes Audit, gemeinsame Dokumentenlenkung)?	☐ ja ☐ nein ☐ offen	Ein kombiniertes Audit ist kein Rabattmodell: Die Vorgaben erlauben, tatsächliche Integration bei der Auditzeit zu berücksichtigen. Wie viel, legt die Stelle nach den anwendbaren Regeln fest; für Informationssicherheit gilt ISO/IEC 27006-1.	verlangt (ISO/IEC 17021-1 mit dem verbindlichen Dokument über Audits integrierter Managementsysteme)
8	Hängt der Datenschutz an denselben Objektblättern (Verzeichnis der Verarbeitungstätigkeiten, Rechtsgrundlagen, Fristen, Auftragsverarbeiter), und hat ein Bereich mit besonders geschützten Daten getrennte Systeme, Zugriffe und Aufbewahrung?	☐ ja ☐ nein ☐ offen	Der Datenschutz ist keine Norm, sondern Recht und kein fünftes System. Gesundheitsdaten gehören zu den besonders geschützten Kategorien; bei Behandelnden kommt die berufsrechtliche Schweigepflicht hinzu.	Recht: DSGVO, revDSG, Schweigepflicht, Stand 28. September 2026; Objektblatt: Methode

6 Häufige Fehler

Nr.	Häufiger Fehler	Was der Abschnitt dazu sagt	Bei uns
1	Vielfalt der Beschreibungen desselben Gegenstands	Vier Beschreibungen eines Raums sind drei zu viel. Keine sieht falsch aus, solange man sie einzeln liest; Widersprüche zeigen sich erst, wenn jemand die Blätter nebeneinanderlegt.	☐ trifft zu ☐ nicht zu
2	Widersprüchliche Zutrittslisten	Vier unterwiesene Personen in einem System, vierzehn Schlüsselinhaber in einem anderen: zehn Personen können einen Raum betreten, für den sie nicht unterwiesen sind.	☐ trifft zu ☐ nicht zu
3	Der Dienstleister, der in keiner Liste steht	Er arbeitet an einer Anlage mit Gefahrstoffen und einer Steuerung im Hausnetz und bekommt am Empfang einen Schlüssel; kein System kennt seine Techniker.	☐ trifft zu ☐ nicht zu
4	Drei Notfallpläne	Sie widersprechen einander nicht, aber im Ernstfall greift jeder zum Blatt seiner Abteilung: drei Meldeketten, zwei Sammelplätze.	☐ trifft zu ☐ nicht zu
5	Der offene Fernzugang	Seit sechs Jahren offen, damit der Anlagenbauer nachts eingreifen kann; beschrieben war er nur als Zeile in einer Lieferantenübersicht.	☐ trifft zu ☐ nicht zu
6	Die verpasste Einsicht aus der Kombination	Ein Angriff auf eine Gebäudeleittechnik ist ein Sicherheitsfall, kein Datenschutzfall; wer eine Dosierung verstellt, gefährdet Menschen.	☐ trifft zu ☐ nicht zu
7	Eine Systemverantwortliche betreut vier Systeme getrennt	Die Trennung war nicht ihre Entscheidung, sondern die Folge des Auditrhythmus: Ein Haus, das seine Systeme getrennt prüfen lässt, erzeugt getrennte Systeme.	☐ trifft zu ☐ nicht zu

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch die Normen der anderen Systeme noch die Regeln der Zertifizierung noch das Recht, das für Ihr Haus gilt (Gefahrstoff-, Arbeitnehmerschutz-, Chemikalien-, Datenschutzrecht). Sie rechnet keine Auditzeit und stellt keine Verkürzung in Aussicht; wie viel die Stelle berücksichtigt, legt sie nach den anwendbaren Regeln fest. Ein ausgefülltes Objektblatt ist kein Nachweis, dass die Maßnahmen wirken. Rechtsstand des Bandes: 28. September 2026.