VORLAGE ZU ABSCHNITT 3.11 DES BANDES 5B

Die Kontenprüfung

Rechte, nicht Namen: von der Zahl der Konten bis zu den vier kritischen Rechten, und die Rückverfolgung eines einzelnen Menschen durch jedes System, das ihm je einen Zugang gegeben hat.

Kategorie: Arbeitsblatt (mit Register in Excel). Bezug im Buch: Abschnitt 3.11 (Das Problem, Das Prinzip, Was die Norm sagt, Rahmen in Deutschland, Österreich und der Schweiz); Norm: Klauseln 5.3, 7.5, 8.1 und 9.1 sowie Maßnahmen A.5.15 bis A.5.18, A.6.5 und A.8.2 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 28. September 2026.

Haus		**Stand (Datum)**	
System		**Geprüft von**	

So nutzen Sie diese Vorlage

1. Beginnen Sie nicht mit der Benutzerliste und lassen Sie keine Liste unterschreiben. Zählen Sie die aktiven Konten, vergleichen Sie sie mit der Zahl der Beschäftigten, folgen Sie der Differenz zu Funktionskonten, Sammelkonten und Protokollen: vier Schritte, eine Stunde.
2. Lassen Sie sich von der Abteilungsleitung drei Rollenkürzel erklären. Übersetzen Sie die Rollen in Klartext, ein Satz je Rolle; zählen Sie die Konten mit den vier kritischen Rechten und fragen Sie, wer sie hat und warum.
3. Werten Sie Nutzung aus, nicht Personen: «Wurde dieses Recht in sechs Monaten benutzt?», nicht «Was hat Frau X in der Nacht des vierten April getan?». Schreiben Sie vorher die Zweckbindung auf, binden Sie die Auswertung an eine Rolle, beteiligen Sie dann die Gremien.
4. Verfolgen Sie bei einem Austritt oder Wechsel den einzelnen Menschen durch jedes System, in dem er je ein Konto hatte (Teil 4 dieses Blattes). Der Auditor beurteilt nicht, ob die Person vertrauenswürdig ist, sondern ob die Rechte zur Funktion passen und ob ihre Vergabe nachvollziehbar ist.

Spalte «Im Buch»: verlangt = von Norm oder Recht verlangt, wie der Band es nennt; Methode = Vorgehen dieses Bandes, keine Anforderung. Das Register zum Blatt liegt als Excel-Datei bei.

1 Die Zahl der Konten und die Differenz

Aktive Konten insgesamt		**Beschäftigte**	
Differenz (Konten minus Beschäftigte)		**davon Funktionskonten**	
davon Testkonten		**davon Schnittstellenkonten**	
davon Sammelkonten		**davon Konten von Menschen, die es im Haus nicht mehr gibt**	

Niemand hatte im Fall des Bandes je gezählt: einhundertdreiundvierzig aktive Konten bei siebenundachtzig Beschäftigten. Diese eine Zahl ist der schnellste Einstieg in jedes Audit dieses Themas (Beispiel aus Abschnitt 3.11; für Ihr Haus nicht übernehmen).

2 Die Rollen in Klartext

Kürzel	Ein Satz in der Sprache des Hauses: «darf …» (was jemand tun kann, nicht welche Tabelle er sieht)	Inhaber (Zahl)	Zuletzt benutzt (6 Monate)	Wer braucht es wirklich?

Ein Hotel hat selten mehr als zwanzig Rollen; die Übersetzung kostet einen Vormittag mit dem Anbieter. Die Probe, ob sie gelungen ist, dauert eine Minute: Man gibt sie einer Etagenleiterin zu lesen. Die Übersetzung ist dokumentierte Information und ändert sich mit jedem Systemupdate; eine veraltete ist gefährlicher als keine (7.5). Beispiele im Band: «darf gebuchte Umsätze nach dem Tagesabschluss korrigieren», «darf Zimmerpreise ändern», «darf Gästeprofile löschen», «darf Berichte über alle Häuser sehen».

3 Die vier kritischen Rechte

Recht	Konten mit diesem Recht (Zahl)	Namen und Funktion dem Direktor bekannt?	In sechs Monaten benutzt von (Zahl der Konten)	Grund, wenn nicht entzogen
Nachträgliche Korrektur von Umsätzen				
Änderung von Preisen und Konditionen				
Zugriff auf vollständige Gästeprofile einschließlich Notizen				
Vergabe von Rechten selbst				

Mit diesen vier Rechten sind Geld oder Vertraulichkeit unmittelbar verbunden; wer nur sie sauber führt, hat den größten Teil des Risikos im Griff. Die Direktion braucht kein Fachwissen, sondern weiß, wer sie hat. Das Beispiel des Bandes: ein Recht, das zwei Personen haben sollten, hatten neun (die beiden Nachtdienste, drei Empfangsmitarbeitende, der Vorgänger des Empfangsleiters, ein Sammelkonto, zwei Konten des Anbieters).

4 Rückverfolgung eines einzelnen Menschen durch jedes System

Funktion (nicht Name, soweit entbehrlich)		**Eintritt / Wechsel / Austritt am**	
Systeme laut Eintrittsliste		**Systeme laut Abfrage in jedem System**	

Nr.	System	Konto (persönlich · Sammel · Funktion · Anbieter)	Rolle in Klartext	Kritisches Recht (welches)	Letzte Nutzung	Stand (aktiv · stillgelegt · entfernt)

Der Band beschreibt das Verfahren, nicht diese Tabelle: Rechte werden mit der Funktion vergeben und enden mit der Funktion; der Austritt ist der einfachste Fall, der Wechsel innerhalb des Hauses der schwierige, weil dabei nichts weggenommen wird, sondern etwas hinzukommt. Konten werden stillgelegt, nach drei Monaten ohne Zugriff entfernt; ein Konto, das nach dem Austritt seines Inhabers benutzt wird, ist ein meldepflichtiges Ereignis, auch wenn die Nutzung harmlos war (im Fall des Bandes: ein übernommenes Kennwort für einen Montagsbericht).

5 Prüffragen

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
1	Was darf diese Rolle? Lassen Sie drei Kürzel von der Abteilungsleitung erklären. _____	Die Leiterin hatte acht Quartale lang für ein Recht unterschrieben, das sie nicht beschreiben konnte; ein Kürzel ohne Beschreibung in Klartext ist eine Unterschrift ohne Text. Die Antwort auf diese drei Fragen ist das Audit.	**verlangt:** Zuweisung und Bekanntmachung von Rollen, Verantwortlichkeiten und Befugnissen (5.3); Zugriffsrechte, Bereitstellung, Überprüfung, Änderung, Entziehung (A.5.18).
2	Woher kommt die Information über die Rechte, und was geschieht, wenn jemand eine Abweichung meldet? _____	Die Regel des Hauses sagte, was zu tun ist (prüfen, unterschreiben), aber nicht, woraufhin geprüft wird, woher die Information kommt und was bei Abweichung geschieht: Regeln ohne diese Angaben erzeugen Unterschriften, und Unterschriften sehen aus wie Kontrolle.	**Methode** dieses Bandes.
3	Gibt es Sammelkonten? Wer nutzt sie? _____	Ein Protokolleintrag, der auf ein Sammelkonto zeigt, benennt niemanden; im Ereignisfall macht ein Sammelkonto alle verdächtig, die in der Schicht waren. In dem Fall: stilllegen, warten, entfernen.	**Methode** dieses Bandes.
4	Welche Konten des Anbieters gibt es? Wann wurden sie zuletzt benutzt, und sind sie befristet? _____	Ein dauerhaft aktives Supportkonto ohne Zweck, Umfang, Befristung und Protokollierung ist in jeder Prüfung eine Feststellung und im Ereignisfall die erste Spur des Forensikers.	**Methode** dieses Bandes.
5	Wer vergibt Rechte, und wer kontrolliert die Vergebenden? Geht die Rechteänderung monatlich als Auswertung an die Direktion? _____	In vielen Häusern hat eine Person am Empfang die Administratorrolle, weil sie sich auskennt, und niemand sieht ihr zu. Die privilegierten Rechte sind die Maßnahme, an der der Fall hängt.	**verlangt:** Privilegierte Zugriffsrechte: Vergabe und Nutzung einschränken und steuern (A.8.2).
6	Wie werden Rechte am Telefon vergeben, und wie wird das dokumentiert? _____	Rechte werden am Telefon vergeben, aus Hilfsbereitschaft, nie aus einem Antrag. Die Abhilfe: Jede Rechtevergabe erzeugt automatisch eine Mail an den Vorgesetzten des Empfängers.	**Methode** dieses Bandes.
7	Werden Rechte mit der Funktion vergeben und enden mit der Funktion? Wie läuft der Wechsel innerhalb des Hauses? _____	Eine Quartalsprüfung findet Abweichungen im Nachhinein, ein Prozess verhindert sie. Die laufende Abstimmung gehört dem Prozessverantwortlichen (Abteilungsleitung mit der IT); das interne Audit prüft unabhängig, ob sie stattfindet und wirkt.	**verlangt:** Steuerung der Prozesse; Eintritt, Wechsel und Austritt (8.1); Zuständigkeiten nach Beendigung oder Änderung eines Beschäftigungsverhältnisses (A.6.5).
8	Welcher Rhythmus gilt für die Prüfung, und wer hat ihn nach Risiko, Fluktuation und Vorfällen festgelegt? _____	Der Quartalsrhythmus ist die Wahl dieses Hauses; die Maßnahme zur Überprüfung der Zugriffsrechte schreibt keinen Dreimonatsrhythmus vor. Die wirksamste Prüfung findet am Tag des Austritts und am Tag des Wechsels statt.	**Methode** dieses Bandes.
9	Führt die Prüfung zu Änderungen, oder steht dort, warum keine nötig waren? Zeigt das Formular neben dem Namen das Recht im Klartext? _____	Die Überprüfung wird fast immer mit der Quartalsprüfung als umgesetzt geführt, der Nachweis besteht aus Unterschriften. Umgesetzt ist die Maßnahme erst, wenn die Prüfung zu Änderungen führt oder dokumentiert ist, warum keine nötig waren. Ein Verfahren, das in acht Quartalen keine Änderung hervorbringt, wird überprüft, nicht verstärkt.	**verlangt:** Überprüfung der Zugriffsrechte (A.5.18); Erklärung zur Anwendbarkeit.
10	Wie viele Konten haben die vier kritischen Rechte, und wie oft wird die Zahl erhoben? _____	Eine der wenigen Kennzahlen, die ein Hotel jederzeit exakt erheben kann.	**verlangt:** Festlegen, was überwacht und gemessen wird (9.1).
11	Wurde die Prüfung an einer Stichprobe selbst noch einmal durchgeführt? _____	Die interne Prüfung einer Rechteprüfung besteht darin, sie an einer Stichprobe zu wiederholen: die Leitung fragen, was die Aufgabe verlangt, das System fragen, was die Person darf, und beides nebeneinanderlegen.	**Methode** dieses Bandes.
12	Trennt das Berechtigungskonzept die Häuser? Wer in Haus A darf Daten aus Haus B sehen? _____	In zentral betriebenen Systemen lautet die Antwort technisch meist «alle, die die Rolle haben»; rechtlich sind es getrennte Verantwortliche, und ein Konzept, das Häuser nicht trennt, erzeugt eine Übermittlung zwischen Gesellschaften, die niemand vereinbart hat. Zuordnung der Rolle: Entscheidung des Hauses.	**Methode** dieses Bandes.
13	Ist die Zweckbindung der Protokollauswertung geschrieben, an eine Rolle gebunden, und sind die Gremien beteiligt? _____	Protokolle werden zur Aufklärung von Sicherheitsereignissen und zur Prüfung von Rechten ausgewertet, nicht zur Leistungsbeurteilung. Häuser, die diese Reihenfolge einhalten, bekommen ihre Vereinbarung in wenigen Wochen.	**verlangt:** Deutschland § 87 Abs. 1 Nr. 6 BetrVG (Mitbestimmung, soweit ein Betriebsrat besteht); Österreich je nach Eingriffstiefe Betriebsvereinbarung oder Zustimmung (insbesondere §§ 96, 96a ArbVG, § 10 AVRAG); Schweiz Art. 26 ArGV 3.
14	Welche Frist gilt für die Zugriffsprotokolle, und wer hat sie begründet? _____	Zugriffsprotokolle sind personenbezogene Daten und brauchen eine Frist nach Zweck und Risiko: lang genug für die Aufklärung, kurz genug, um keine Verhaltensakte zu erzeugen. Eine für alle Fälle geltende Frist nennen weder die Norm noch die Datenschutz-Grundverordnung; für Sonderfälle sind Mindestfristen im Einzelfall zu prüfen.	**verlangt:** Datenschutz-Grundverordnung (Rechtsstand dieses Bandes); Fristen im Einzelfall.

Häufige Fehler (aus dem Band)

Nr.	Fehler	Was der Band daraus macht
1	Benutzerprüfung mit Rechteprüfung verwechselt	Eine Liste von Namen beantwortet, wer ein Konto hat, nicht, was es kann; nur die zweite Frage betrifft das Risiko.
2	Die Kürzel	Rollennamen überleben alle Menschen, die sie erklären könnten.
3	Die Pauschalvergabe bei Umstellungen	Rechte werden «mitgenommen»; ein fehlendes Recht fällt am ersten Tag auf, ein überflüssiges nie.
4	Die Sammelkonten	Bequem, weil sie Übergaben ersparen, und sie zerstören jede Nachvollziehbarkeit.
5	Die Konten des Anbieters	Sie gehören auf eine eigene Liste mit eigener Prüfung.
6	Die Zuständigkeit zwischen drei Abteilungen	Personal kennt Eintritte, die IT Rechte, der Betrieb Funktionen: Die Aufgabe liegt zwischen ihnen und deshalb nirgends.
7	Die Unterschrift ohne Grundlage	Wer bestätigt, was er nicht beurteilen kann, erzeugt einen Nachweis, der so viel wert ist wie das Wissen dahinter.
8	Das Prüfdesign nach einem Einzelfall	Maßnahmen, die aus einem Einzelfall entstehen, lösen den Einzelfall und blenden das Feld aus, in dem er stand.
9	Die papierbasierte Prüfung	Vierzehn Listen, zwei Wochen, ein Dokument über den Stand von vor zwei Wochen; im System bestätigt zeigt sich auch, wer wann bestätigt hat.
10	Die Zahl der Konten nie gezählt	Der schnellste Einstieg in das Audit.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch das Recht oder die Regelwerke, die für Ihr Haus gelten. Ein ausgefülltes Blatt ist kein Nachweis: Es zeigt, dass jemand hingesehen hat, nicht dass der Zustand besteht, den es beschreibt. Sie beurteilt keine Person und keine Leistung und ersetzt weder die Vereinbarung mit der Mitbestimmung noch eine arbeitsrechtliche Beratung. Die Rückverfolgung eines Menschen ist ein Prüfverfahren, kein Verdachtsverfahren. Die Rollenübersetzung ist so alt wie ihr letztes Systemupdate. Rechtsstand des Bandes: 28. September 2026.