Online-Schulung · 3 Stunden · Bescheinigung

Wer darf was – und warum noch?

Konten und Rechte nachvollziehbar beantragen, freigeben, ändern und entziehen – und eine Rezertifizierung durchführen, die fachlich entschieden und belegbar ist.

In fast jeder Organisation haben Beschäftigte mehr Rechte, als sie brauchen – nicht durch Regelverstöße, sondern weil Rechte einzeln vergeben und nie zurückgenommen werden. Diese Schulung vermittelt den Lebenszyklus von Konten und Berechtigungen so, dass Fachbereich, Personalwesen und IT zusammenarbeiten.

ISO/IEC 27001 verlangt im Anhang A geregelte Zugriffskontrolle, Identitätsmanagement, die Verwaltung privilegierter Zugangsrechte und die regelmäßige Überprüfung von Zugangsrechten; der BSI-Baustein ORP.4 beschreibt das Verfahren.

Der Lebenszyklus in vier Schritten

- **Beantragen mit Zweck**
- **Fachlich freigeben**
- **Bei Wechsel anpassen**
- **Fristgerecht entziehen**

Berechtigungen
6 Module
15 Lektionen
180 Minuten

- **Teilnahme-bescheinigung**
- **6 Begleit-unterlagen**
- **15 Infografiken**



So entsteht ein Rechtebestand. Lektion 1.1 zeigt vier Jahre einer Mitarbeiterin: Eintritt, Vertretung, Projekt, Wechsel – jede Vergabe begründet, keine je zurückgenommen. Ergebnis: 17 Rechte, davon 5 erforderlich, und ein Funktionstrennungskonflikt, den niemand beschlossen hat.

Listen, die entschieden werden

Fachliche Rollennamen, Herkunft und letzte Nutzung statt technischer Gruppen – erst damit wird aus Bestätigen Entscheiden.

Der Wechsel im Griff

Der riskanteste Vorgang: Bestand ziehen, neue Rolle festlegen, Differenz im selben Vorgang entziehen.

Besondere Konten geregelt

Privilegierte Konten, Dienstkonten, Externe und Notfallzugriffe – jedes mit Verantwortlichem und Ablauf.

6	15	46	180	6	75 %
Module	Lektionen	Quizfragen	Minuten Mindest-bearbeitungszeit	Begleitunterlagen	Bestehensgrenze

Schulung ansehen →

Angebot anfordern →

Herausgeber: Sachverständigenbüro Schulte, Düsseldorf. Die Schulung folgt den Anforderungen von ISO/IEC 27001 (Anhang A, Zugangssteuerung) und dem BSI-IT-Grundschutz-Baustein ORP.4. **Normtexte werden nicht wiedergegeben**; maßgeblich sind die gültigen Originaldokumente sowie das Berechtigungskonzept Ihrer Organisation. Rechtsstand November 2026. Keine Rechtsberatung.

Woran Berechtigungsmanagement scheitert.

Der Wechsel ohne Rücknahme. Neue Rechte werden beantragt, weil die Person sie braucht. Die alten entzieht niemand: Der abgebende Bereich ist nicht mehr zuständig, der aufnehmende kennt sie nicht. So entstehen Rechteansammlung und Funktionstrennungskonflikte – ohne dass jemand sie beschlossen hat.

Gesperrt statt entzogen. Nach dem Austritt wird das Konto deaktiviert, die Rechte bleiben daran bestehen. Bei Reaktivierung ist es sofort wieder voll wirksam, und in jeder Auswertung zählt es als bestehender Zugriff.

Die Liste, die durchgewinkt wird. Eine Rezertifizierung mit technischen Gruppennamen ist nicht prüfbar. Der Prüfende bestätigt – nicht aus Nachlässigkeit, sondern weil die Frage so nicht beantwortbar ist.

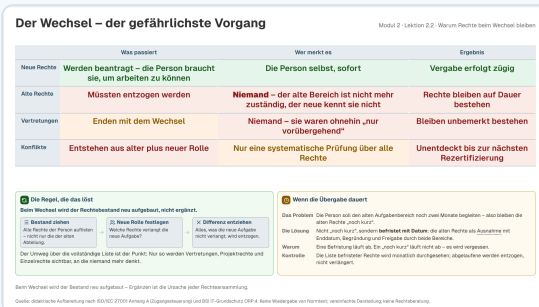
Konten ohne Person. Dienstkonten ohne Verantwortlichen, Zugänge von Dienstleistern ohne Ablaufdatum, Notfallzugänge ohne Meldepflicht. Sie fallen aus allen Prozessen heraus – und finden sich in nahezu jeder Prüfung.

Was die Schulung dagegen setzt

Getrennte Rollen für Antrag, Freigabe, Umsetzung und Kontrolle. Den Wechsel als Neuaufbau statt als Ergänzung. Rezertifizierungslisten, die fachlich lesbar sind, mit vier Entscheidungen statt einer. Und eine Fallwerkstatt mit zwölf echten Fällen.

BEZUGSRAHMEN

ISO/IEC 27001 Anhang A · Zugriffskontrolle · Identitätsmanagement · Privilegierte Zugangsrechte · BSI ORP.4 · Funktionstrennung



Der Wechsel – der gefährlichste Vorgang

Modul 2 · Lektion 2.2 · Warum Rechte beim Wechsel bleiben

	Was passiert	Wer merkt es	Ergebnis
Neue Rechte	Werden beantragt – die Person braucht sie, um arbeiten zu können	Die Person selbst, sofort	Vergabe erfolgt zügig
Alte Rechte	Müssten entzogen werden	**Niemand** – der alte Bereich ist nicht mehr zuständig, der neue kennt sie nicht	Rechte bleiben auf Dauer bestehen
Vertretungen	Enden mit dem Wechsel	Niemand – sie waren ohnehin „nur vorübergehend"	Bleiben unbemerkt bestehen
Konflikte	Entstehen aus alter plus neuer Rolle	Nur eine systematische Prüfung über alle Rechte	Unentdeckt bis zur nächsten Rezertifizierung

Die Regel, die das löst

Beim Wechsel wird der Rechtebestand neu aufgebaut, nicht ergänzt.

- Bestand ziehen – Alle Rechte der Person aufnehmen – nicht nur die der alten Abteilung.
- Neue Rolle festlegen – Welche Rechte verlangt die neue Aufgabe?
- Differenz entziehen – Alles, was die neue Aufgabe nicht verlangt, wird entzogen.

Der Umweg über die vollständige Liste ist der Punkt: Nur so werden Vertretungen, Projektrechte und Einzelrechte sichtbar, an die niemand mehr denkt.

Wenn die Übergabe dauert

Das Problem	Die Person soll den alten Aufgabenbereich noch zwei Monate begleiten – also bleiben die alten Rechte „noch kurz".
Die Lösung	Nicht „noch kurz", sondern **befristet mit Datum**: die alten Rechte als Ausnahme mit Enddatum, Begründung und Freigabe durch beide Bereiche.
Warum	Eine Befristung läuft ab. Ein „noch kurz" läuft nicht ab – es wird vergessen.
Kontrolle	Die Liste befristeter Rechte wird monatlich durchgesehen; abgelaufene werden entzogen, nicht verlängert.

Beim Wechsel wird der Bestand neu aufgebaut – Ergänzen ist die Ursache jeder Rechtesammlung.

Quelle: didaktische Aufbereitung nach ISO/IEC 27001 Anhang A (Zugangssteuerung) und BSI IT-Grundschutz ORP.4. Keine Wiedergabe von Normtext; verein

Lektion 2.2: Der Wechsel ist riskanter als der Austritt. Neue Rechte kommen sofort, alte bleiben – und die Konflikte entstehen aus der Summe.

Fragen, die Prüfer und Aufsicht stellen

1. Wie lange dauert es vom Austritt bis zum tatsächlichen Entzug?
2. Wer hat dieses Recht fachlich freigegeben – und zu welchem Zweck?
3. Wie viele Rechte wurden in der letzten Rezertifizierung entzogen?
4. Wer verantwortet dieses Dienstkonto, und wann wurde sein Kennwort gewechselt?
5. Welche Funktionstrennungskonflikte bestehen – und wie sind sie behandelt?

Die Schulung beantwortet jede dieser Fragen mit einer Vorlage – und mit geschulten Beteiligten, deren Teilnahme dokumentiert ist.

Die IT gibt nicht fachlich frei

Sie kennt die Aufgabe nicht und steht unter dem Zeitdruck des Anrufers – die Freigabe gehört in den Fachbereich.

Sperren ist nicht Entziehen

Erst der technische Entzug beendet den Zugriff; die Sperrung ist die Sofortmaßnahme.

Ohne Entzüge kein Ergebnis

Eine Rezertifizierung mit 100 % Bestätigungen hat nichts geprüft – die Entzugsquote misst das Verfahren.

Ablauf, Nutzen und Inhalte

Die sechs Module

1 Grundprinzipien und Rollen
Minimalprinzip, Kenntnis nur bei Bedarf; wer beantragt, freigibt, umsetzt und kontrolliert. · 20 Min.

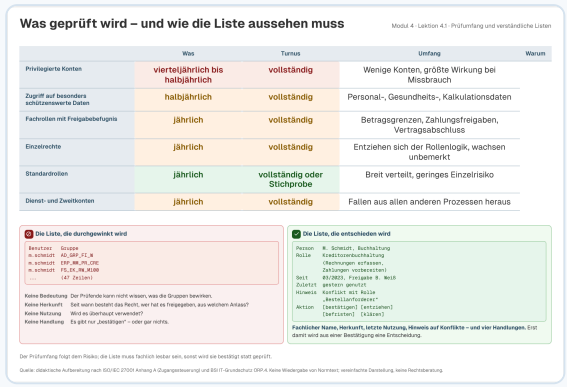
2 Eintritt, Wechsel, Austritt
Auslösung aus dem Personalsystem, Neuaufbau beim Wechsel, Sperrung, Entzug und Löschung mit Fristen. · 35 Min.

3 Rollen und besondere Konten
Rollenmodell und Einzelrechte, privilegierte Konten, Dienstkonten, Externe und Notfallzugriff. · 30 Min.

4 Rezertifizierung
Prüfumfang nach Risiko, lesbare Listen, vier Entscheidungen, Entzug und Abschlusskontrolle. · 35 Min.

5 Fallwerkstatt
Zwölf Fälle aus einem echten Rechtebestand: entscheiden, begründen, Konflikte auflösen, dokumentieren. · 45 Min.

6 Abschluss
Sechs Kennzahlen mit den Handlungen, die daraus folgen, und ein persönlicher Maßnahmenplan. · 15 Min.



Lektion 4.1: Prüfumfang nach Risiko – und der Unterschied zwischen der Liste, die durchgewinkt wird, und der, die entschieden wird.

Fallwerkstatt

Zwölf Zeilen aus einem echten Rechtebestand: ehemalige Beschäftigte, ein Doppelkonto, überhöhte Rechte aus Projekt und Vertretung, ein Dienstkonto ohne Verantwortlichen, ein Externer ohne Ablaufdatum, ein ungeregelter Notfallzugang und zwei Funktionstrennungskonflikte. Ergebnis: elf begründete Entscheidungen und vier Folgemaßnahmen.

Für wen

IT-Administration, Anwendungsverantwortliche, Führungskräfte mit Freigabebefugnis, Schnittstellen zum Personalwesen, ISB und interne Kontrollverantwortliche. Vorausgesetzt wird ein Grundverständnis von Benutzerkonten und Anwendungen.

Sechs Begleitunterlagen – dazu 46 Lernkontrollfragen, bestanden ab 75 %

Muster eines Berechtigungskonzepts — B1

Modul 1

Geltung, Grundsätze, Rollen, Kontenarten, Fristen, Ausnahmen, Nachweise – von der Leitung freizugeben.

Rollen- und Verantwortungsmatrix — B2

Modul 1/3

Welche Rolle was erlaubt, wer sie freigibt und welche Kombinationen unvereinbar sind.

Checklisten Eintritt, Wechsel, Austritt — B3

Modul 2

Drei Abläufe zum Abhaken – mit vollständiger Bestandsaufnahme beim Wechsel.

Rezertifizierungsvorlage — B4

Modul 4

Eine Zeile je Berechtigung mit Herkunft, letzter Nutzung, Entscheidung und Begründung.

Ausnahmen und Notfallzugriffe — B5

Modul 3/5

Konflikt, Begründung, kompensierende Maßnahme, Entscheidung und Frist – in einer Vorlage.

Kennzahlenblatt — B6

Modul 6

Sechs Kennzahlen mit Zielwert, Istwert und der Handlung, die daraus folgt.

So läuft es ab

1 Plätze buchen
Sie teilen uns die Zahl der Teilnehmenden mit; wir richten Ihr Unternehmen im Schulungsportal ein.

2 Einladen
Teilnehmende werden im Portal angelegt und erhalten ihren persönlichen Zugang per E-Mail.

3 Lernen
Sechs Module in drei Einheiten von je 60 Minuten, mit Lernkontrollen nach jeder Lektion.

4 Fälle bearbeiten
Die Fallwerkstatt führt durch zwölf Fälle bis zur dokumentierten Entscheidung.

5 Nachweisen
Abschlussprüfung ab 75 Prozent, Bescheinigung als PDF, Auswertung im Portal.

Was Sie erhalten

Zugang je Teilnehmer
Persönlicher Link, Fortschritt wird gespeichert, Bearbeitung in mehreren Sitzungen möglich.

Teilnahmebescheinigung
PDF mit fortlaufender Nummer, Inhalten, Dauer und Prüfadresse zur Online-Verifikation.

Sechs Begleitunterlagen
Berechtigungskonzept, Rollenmatrix, Prozesschecklisten, Rezertifizierungsvorlage, Ausnahmenprotokoll, Kennzahlenblatt.

Auswertung im Portal
Stand je Teilnehmer, Abschlüsse, Bescheinigungen und Wiederholungsintervalle auf einen Blick.

Anbindung an Ihr ISMS
Abschlüsse lassen sich automatisch als Schulungsnachweise in das ISMS-Werkzeug **Vercora** übertragen – mit Bescheinigungsnummer, Datum und Prüfadresse.

Ihr Ansprechpartner

Herausgeber

Heinrich Markus Schulte
IT-Sachverständiger · CISA, CISM, CIPP/E, CEH
Schwerpunkte: NIS-2, DORA, CRA, ISMS

> *„Die Frage ist nie, ob ein Recht schadet, sondern welche Aufgabe es heute verlangt. Wer sie bei jedem Antrag stellt, braucht die übrigen Regeln seltener."*

Angebot anfordern →

Schulung ansehen →

Sachverständigenbüro Schulte
Grünberger Weg 9 · 40627 Düsseldorf
+49 211 93375777
sachverstaendiger@itschulte.de
itschulte.de

Weitere Schulungen aus demselben Haus

Interne ISMS-Audits — 420 Min.
ISO/IEC 27001 Abschnitt 9.2 · ISO 19011
Audits planen, Nachweise bewerten und Feststellungen schreiben, die standhalten.

Risiken bewerten und behandeln — 420 Min.
ISO/IEC 27001 6.1.2/6.1.3 · ISO/IEC 27005 · BSI 200-3
Szenarien formulieren, bewerten, behandeln und der Leitung entscheidungsreif vorlegen.

NIS-2-Geschäftsleitungsschulung — 180 Min.
§ 38 Abs. 3 BSIG · BSI-Curriculum
Die gesetzlich geforderte Schulung der Geschäftsleitung zu Risikomanagement, Pflichten und Haftung.

Incident Response & Playbooks — 420 Min.
NIST SP 800-61 · ISO/IEC 27035 · § 32 BSIG
Vorfälle erkennen, melden, eindämmen und auswerten – mit fünf szenariobasierten Playbooks.

Die Schulung vermittelt die betriebliche Praxis des Berechtigungsmanagements. **Normtexte werden nicht wiedergegeben**; maßgeblich sind die jeweils gültigen Originaldokumente sowie das Berechtigungskonzept, die Fristen und die Freigaberegeln Ihrer Organisation. Die Bescheinigung bestätigt die Teilnahme; sie ist keine Zertifizierung und kein Prüftestat. Rechtsstand November 2026. Keine Rechtsberatung.