Leiter der Informationssicherheit

FF09 IT-Infrastruktur, Betrieb und Sicherheit · ISCO-08 1330 · CBS 0533 IKT-Manager · Dienstalter lead · Auch bekannt als: CISO, Leiter der Informationssicherheit

Trägt die oberste Verantwortung für die Informationssicherheit, legt Richtlinien und die Risikobereitschaft fest und legt gegenüber dem Vorstand und den Aufsichtsbehörden Rechenschaft über den Sicherheitsstatus ab.

Der Chief Information Security Officer leitet den Sicherheitsbereich einer Organisation, verteilt Ressourcen und entscheidet, welche Risiken akzeptiert werden. Im Gegensatz zum Sicherheitsbeauftragten verfügt diese Position über ein Mandat und ein Budget, und im Gegensatz zum IT-Leiter liegt ihr Hauptaugenmerk auf der Risikokontrolle und nicht auf der Systemverfügbarkeit. Bei der Auswahl wird großes Gewicht auf technisches Wissen und Normenkenntnisse gelegt, während die Rolle in der Praxis häufig an Führungspräsenz scheitert: Ein CISO muss in der Lage sein, eine Investition durchzusetzen und in Krisenzeiten mit Vorständen und Vorgesetzten zu kommunizieren, ohne die Fakten zu beschönigen.

Kennzahlen für dieses Profil

26 Fähigkeiten · 4 Zu bewertende Kompetenzen · 3 Ausschlusskriterien · Schwerpunkt: Digitales, Daten und KI 47%, Führung und Organisation 20%, Kognitive Fähigkeiten und Problemlösung 10%

1 Zu messende Kompetenzen

Dies sind die Verhaltens- und Fähigkeitskonstrukte in diesem Profil. Zu jedem wird angezeigt, welcher hrmforce-Fragebogen es misst.

Zu messende Kompetenzen	Zielniveau	hrmforce-Instrument	Messmethode	Verhaltensanker auf Zielniveau
Genauigkeit und Liebe zum Detail Kompetenz (50-Framework): Genauigkeit	N5	Big Fifty, 360 Feedback	Persönlichkeitsfragebogen	Legt die Standards für Vollständigkeit und Richtigkeit fest, lässt Beispiele prüfen und weist Teams auf strukturelle Nachlässigkeiten hin.
Integrität und Zuverlässigkeit Kompetenz (50-Framework): Integrität	N5	Big Fifty (Integritätsskala), 360 Feedback, Strukturiertes Interview	Persönlichkeitsfragebogen	Legt die Integritätsstandards der Organisation fest, setzt diese auch gegenüber einflussreichen Parteien durch und erläutert die daraus resultierenden Entscheidungen öffentlich.

Zu messende Kompetenzen	Zielniveau	hrmforce-Instrument	Messmethode	Verhaltensanker auf Zielniveau
Disziplin und Einhaltung von Verpflichtungen Kompetenz (50-Framework): Fachgebiet	N5	Big Fifty, 15PF, 360 Feedback	Persönlichkeitsfragebogen	Verankert den Standard für die zuverlässige Einhaltung von Arbeitsvereinbarungen und richtet sich an alle Mitarbeiter auf jeder Ebene, die diesen Standard vernachlässigen.
Stressresistenz Kompetenz (50-Framework): Stressresilienz	N5	Big Fifty, 15PF, Mental Resilience (4C)	Persönlichkeitsfragebogen	Sorgt dafür, dass die Organisation auch in Krisenzeiten funktionsfähig bleibt, trifft Entscheidungen unter hoher Unsicherheit und setzt Maßstäbe für besonnenes Handeln unter Druck.

2 Vollständiges Kompetenzprofil

Alle Kompetenzen in diesem Profil, sortiert nach Gewichtung. Der unter jeder Kompetenz angegebene Verhaltensanker bezieht sich auf das Zielniveau.

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
V	Problemanalyse Führt hartnäckige organisatorische Probleme auf einige wenige Grundursachen zurück und legt die Analysemethode fest, die andere Teams anwenden werden.	N5	5	ja	Assessment-Center	Competency Check, Ability Scan
V	Strategisches Denken Entwickelt Szenarien für das gesamte Unternehmen, wägt Unsicherheiten explizit ab und legt gemeinsam mit der Geschäftsleitung die strategische Agenda fest.	N5	5	nein	Assessment-Center	Ability Scan, Competency Check
K	Governance und Compliance Erarbeitet den Governance-Rahmen der Organisation, legt Mandate und Aufsichtsregelungen fest und legt gegenüber externen Aufsichtsgremien Rechenschaft über die Einhaltung der Vorschriften ab.	N5	5	nein	Wissenstest	Wissenstest (kundenspezifisch)
V	Risikomanagement Erstellt das Risikorahmenwerk der Organisation, legt gemeinsam mit der Geschäftsleitung die Risikobereitschaft fest und berichtet dem Aufsichtsgremium darüber.	N5	5	nein	Wissenstest	Wissenstest (kundenspezifisch), Competency Check
V	Zugangs- und Identitätsmanagement Legt die Zugriffsrichtlinien der Organisation fest und ist für die Kontrolle der Berechtigungen bei Audits zuständig.	N5	5	ja	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
V	Bedrohungs- und Risikoanalyse Führt eigenständig eine Bedrohungsanalyse einer Anwendung durch, priorisiert Risiken und berät hinsichtlich Maßnahmen unter Angabe von Kosten und Wirkung.	N4	5	ja	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test
G	Genauigkeit und Liebe zum Detail Legt die Standards für Vollständigkeit und Richtigkeit fest, lässt Beispiele prüfen und weist Teams auf strukturelle Nachlässigkeiten hin.	N5	4	nein	Persönlichkeitsfragebogen	Big Fifty, 360 Feedback
G	Integrität und Zuverlässigkeit Legt die Integritätsstandards der Organisation fest, setzt diese auch gegenüber einflussreichen Parteien durch und erläutert die daraus resultierenden Entscheidungen öffentlich.	N5	4	nein	Persönlichkeitsfragebogen	Big Fifty (Integritätsskala), 360 Feedback, Strukturiertes Interview
V	Rechenschaftspflicht gegenüber Vorgesetzten und Interessengruppen Rechenschaftsberichte über Unternehmensergebnisse und Vorfälle gegenüber dem Aufsichtsrat, den Medien oder der Politik sowie die Verknüpfung sichtbarer strategischer Anpassungen mit diesen Ereignissen.	N5	4	nein	Assessment-Center	Competency Check, 360 Feedback
G	Disziplin und Einhaltung von Verpflichtungen Verankert den Standard für die zuverlässige Einhaltung von Arbeitsvereinbarungen und richtet sich an alle Mitarbeiter auf jeder Ebene, die diesen Standard vernachlässigen.	N5	4	nein	Persönlichkeitsfragebogen	Big Fifty, 15PF, 360 Feedback

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
G	Stressresistenz Sorgt dafür, dass die Organisation auch in Krisenzeiten funktionsfähig bleibt, trifft Entscheidungen unter hoher Unsicherheit und setzt Maßstäbe für besonnenes Handeln unter Druck.	N5	4	nein	Persönlichkeitsfragebogen	Big Fifty, 15PF, Mental Resilience (4C)
V	Informationssicherheit im Arbeitsprozess Legt die Richtlinien zur Informationssicherheit fest und überwacht organisationsweit, ob die Prozesse den festgelegten Anforderungen entsprechen.	N5	4	nein	Wissenstest	Wissenstest (kundenspezifisch)
V	Nutzung von Cloud-Plattformen Legt die Cloud-Strategie des Unternehmens fest und entscheidet, welche Workloads wo platziert werden.	N5	4	nein	Wissenstest	Wissenstest (kundenspezifisch)
K	Sensibilisierung für Informationssicherheit Entwirft das Sensibilisierungsprogramm des Unternehmens, misst dessen Wirkung und passt den Ansatz auf der Grundlage der gemessenen Ergebnisse an.	N5	4	nein	Wissenstest	Wissenstest (kundenspezifisch)
V	Entwicklung von Richtlinien Legt den strategischen Kurs für einen Bereich fest, vernetzt die Beteiligten in der Kette und lässt die Auswirkungen systematisch bewerten.	N5	4	nein	Portfolio oder Nachweise	Portfolio, Competency Check
V	Reaktion auf Sicherheitsvorfälle Begrenzt eigenständig den Schaden während eines Vorfalls, sichert Beweismittel und liefert einen nachvollziehbaren Ablauf der Ereignisse.	N4	4	nein	Simulation	Wissenstest (kundenspezifisch), Arbeitsproben-Test

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
V	Aus Fehlern und Vorfällen lernen Analysiert eigene Fehler sowie die des Teams, erörtert die Ursachen offen in der Arbeitsbesprechung und passt die Vereinbarungen entsprechend an.	N4	3	nein	Situational Judgement Test	360 Feedback, Competency Check
V	Aktueller Fachstand und Fachliteratur Erfasst Quellen und Leitlinien systematisch, bewertet deren Qualität und passt die eigene Arbeitsweise an neue Erkenntnisse an.	N4	3	nein	Portfolio oder Nachweise	Portfolio, Wissenstest (kundenspezifisch)
V	Erstellung technischer Dokumentationen Verfasst die vollständige Dokumentation für ein System oder einen Prozess, testet diese mit einem Laien und pflegt die verschiedenen Versionen.	N4	3	nein	Arbeitsproben-Test	Arbeitsproben-Test, Portfolio
V	Prozessautomatisierung Beschreibt einen Prozess in einzelnen Schritten, automatisiert die wiederholbaren Schritte und integriert Prüfungen auf Fehler und Ausnahmen.	N4	3	nein	Arbeitsproben-Test	Arbeitsproben-Test, Portfolio
V	Funktions- und Anwendungsmanagement Verwaltet eigenständig eine Anwendung, priorisiert Änderungswünsche gemeinsam mit den Anwendern und testet neue Versionen, bevor diese in Betrieb genommen werden.	N4	3	nein	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
V	Störungsmanagement und Fehlerbehebung Leitet eine Untersuchung zu einer unbekannten Störung ein, stellt den Betrieb wieder her und dokumentiert Ursache und Lösung zur späteren Wiederverwendung.	N3	3	nein	Arbeitsproben-Test	Arbeitsproben-Test, Wissenstest (kundenspezifisch)
V	Datenklassifizierung und -aufbewahrung Legt die Klassifizierung und die Aufbewahrungsfrist für einen Informationsfluss fest und überprüft, ob die Bereinigung wie geplant erfolgt.	N4	2	nein	Wissenstest	Wissenstest (kundenspezifisch), Arbeitsproben-Test
K	Grundkenntnisse im Bereich Netzwerke Leitet anhand von Symptomen ab, in welcher Netzwerkschicht ein Problem vorliegt, und untermauert dies durch eigene Messungen.	N3	2	nein	Wissenstest	Wissenstest (kundenspezifisch)
V	IT-Lieferanten- und Vertragsmanagement Führt Besprechungen mit Lieferanten zu Leistung und Kosten durch, dokumentiert Vereinbarungen und greift ein, wenn Vereinbarungen nicht eingehalten werden.	N3	1	nein	Strukturiertes Interview	Strukturiertes Interview, Portfolio
V	Systemadministration und -überwachung Führt geplante Wartungsaufgaben und Aktualisierungen gemäß dem Runbook durch und meldet Abweichungen bei den Überwachungssignalen.	N2	1	nein	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test

3 Stufen nach Dienstalter

Dasselbe Profil unter Berücksichtigung der Dienstaltersanpassung für die Berufsgruppe. Die Zielstufen sind auf 1 bis 5 begrenzt.

Skill	lead
Problemanalyse	N5
Strategisches Denken	N5
Governance und Compliance	N5
Risikomanagement	N5
Zugangs- und Identitätsmanagement	N5
Bedrohungs- und Risikoanalyse	N4
Genauigkeit und Liebe zum Detail	N5
Integrität und Zuverlässigkeit	N5
Rechenschaftspflicht gegenüber Vorgesetzten und Interessengruppen	N5
Disziplin und Einhaltung von Verpflichtungen	N5
Stressresistenz	N5
Informationssicherheit im Arbeitsprozess	N5
Nutzung von Cloud-Plattformen	N5
Sensibilisierung für Informationssicherheit	N5
Entwicklung von Richtlinien	N5
Reaktion auf Sicherheitsvorfälle	N4
Aus Fehlern und Vorfällen lernen	N4
Aktueller Fachstand und Fachliteratur	N4
Erstellung technischer Dokumentationen	N4
Prozessautomatisierung	N4
Funktions- und Anwendungsmanagement	N4
Störungsmanagement und Fehlerbehebung	N3
Datenklassifizierung und -aufbewahrung	N4
Grundkenntnisse im Bereich Netzwerke	N3
IT-Lieferanten- und Vertragsmanagement	N3
Systemadministration und -überwachung	N2

4 Die Kompetenzskala

Ebene	Bezeichnung	Autonomie	Komplexität	Umfang	Kenntnis עעfang
N1	**Geführt**	arbeitet unter Aufsicht und befolgt Anweisungen	Routine, jeweils eine Variable nach der anderen	eigene Aufgabe	Grundlegendes Verständnis der Terminologie
N2	**Anwendung**	arbeitet selbstständig innerhalb festgelegter Rahmenbedingungen	vertraute Situationen mit geringen Abweichungen	die eigene Rolle	praktische Kenntnisse, wendet Standardverfahren an
N3	**Beherrscht**	legt den eigenen Ansatz fest und holt proaktiv Input ein	mehrere Variablen, gewisse Mehrdeutigkeiten	eigenes Team oder eigener Prozess	fundierte Kenntnisse, wägt Alternativen ab
N4	**Fortgeschritten**	leitet andere an und entscheidet über die Vorgehensweise	komplex, mit widersprüchlichen Interessen	mehrere Teams oder eine Abteilung	fundierte Kenntnisse, berät andere
N5	**Führung**	legt den Standard und die Richtlinien fest	strategisch, unter hoher Unsicherheit	Organisation, Wertschöpfungskette oder Berufsfeld	Autorität, fördert die Entwicklung des Berufsstandes

5 Verhaltensanker pro Kompetenz

Die Ankerpunkte befinden sich bei N1, N3 und N5. N2 und N4 sind bewusst nicht als Ankerpunkte festgelegt: Die Bewerter interpolieren zwischen diesen Punkten gemäß der O*NET-Konvention.

Skill	N1	N3	N5
Problemanalyse Teilt ein Problem in einzelne Teile auf, trennt Ursachen von Wirkungen und gibt an, welche Informationen erforderlich sind, um weiterzukommen.	Gibt genau an, was bei einer Störung abweicht und welche Daten fehlen, und meldet dies dem Vorgesetzten.	Gliedert eine wiederholt auftretende Beschwerde in mögliche Ursachen auf, prüft diese anhand eigener Daten und benennt die wahrscheinlichste Ursache.	Führt hartnäckige organisatorische Probleme auf einige wenige Grundursachen zurück und legt die Analysemethode fest, die andere Teams anwenden werden.
Strategisches Denken Analyse von Entwicklungen im Umfeld, auf dem Markt und im technologischen Bereich sowie Ableitung strategischer Optionen und Alternativen daraus für die langfristige Ausrichtung einer Organisation oder einer Einheit.	Erhebt auf Anfrage Daten zum Markt und zur Konkurrenz und fasst die wichtigsten Entwicklungen für die Führungskraft zusammen.	Stellt Kennzahlen, Kundensignale und Trends gegenüber und nennt zwei oder drei strategische Optionen mit ihren jeweiligen Konsequenzen.	Entwickelt Szenarien für das gesamte Unternehmen, wägt Unsicherheiten explizit ab und legt gemeinsam mit der Geschäftsleitung die strategische Agenda fest.

Skill	N1	N3	N5
Governance und Compliance Kenntnis darüber, welche Gesetze, Verhaltenskodizes und internen Vorschriften für den eigenen Bereich gelten und wie Aufsicht, Befugnisse und Rechenschaftspflicht in der Organisation geregelt sind.	Nennt die wichtigsten Regeln für die eigene Arbeit und recherchiert im Zweifelsfall die geltende Vorgehensweise.	Prüft die Arbeitsmethoden auf Übereinstimmung mit gesetzlichen Vorschriften und internen Regeln und meldet Abweichungen mit Begründung an den zuständigen Vorgesetzten.	Erarbeitet den Governance-Rahmen der Organisation, legt Mandate und Aufsichtsregelungen fest und legt gegenüber externen Aufsichtsgremien Rechenschaft über die Einhaltung der Vorschriften ab.
Risikomanagement Risiken in der Arbeit, bei Projekten oder in Richtlinien identifizieren, deren Eintrittswahrscheinlichkeit und Auswirkungen abwägen, Kontrollmaßnahmen auswählen und regelmäßig überprüfen, ob diese Maßnahmen funktionieren.	Meldet unsichere oder risikobehaftete Situationen im eigenen Arbeitsbereich über den vereinbarten Meldeweg.	Erstellt eine Risikoliste mit Angaben zu Wahrscheinlichkeit, Auswirkung und Maßnahmen pro Risiko und überprüft diese regelmäßig gemeinsam mit den Beteiligten.	Erstellt das Risikorahmenwerk der Organisation, legt gemeinsam mit der Geschäftsleitung die Risikobereitschaft fest und berichtet dem Aufsichtsgremium darüber.
Zugangs- und Identitätsmanagement Erteilt Zugriffsrechte je nach Rolle und Bedarf, überprüft regelmäßig, wer auf welche Daten zugreifen darf, und entzieht die Rechte bei Änderungen oder beim Ausscheiden.	Bearbeitet Zugriffsanfragen gemäß dem festgelegten Rollenschema und protokolliert jede Änderung.	Entwirft Rollen und Berechtigungen für eine Anwendung, führt regelmäßige Überprüfungen durch und korrigiert übermäßige Zugriffsrechte.	Legt die Zugriffsrichtlinien der Organisation fest und ist für die Kontrolle der Berechtigungen bei Audits zuständig.
Bedrohungs- und Risikoanalyse Ermittelt Risiken, Schwachstellen und Folgen für ein System oder einen Prozess, wägt die Eintrittswahrscheinlichkeit gegen die Auswirkungen ab und benennt geeignete Maßnahmen.	Führt anhand einer vorgegebenen Liste von Bedrohungen eine Risikoanalyse durch und übermittelt das Ergebnis an den Fachspezialisten.	Führt eigenständig eine Bedrohungsanalyse einer Anwendung durch, priorisiert Risiken und berät hinsichtlich Maßnahmen unter Angabe von Kosten und Wirkung.	Ermittelt die Risikobereitschaft und die Analysemethode des Unternehmens und legt dem Vorstand das Sicherheitsrisikobild dar.
Genauigkeit und Liebe zum Detail Arbeitet sorgfältig, überprüft die eigene Arbeit auf Fehler und hält sich an die Vereinbarungen bezüglich der Vollständigkeit und Richtigkeit der Daten.	Überprüft die eigene Arbeit anhand einer Checkliste und korrigiert festgestellte Fehler, bevor die Arbeit weitergeleitet wird.	Baut Kontrollmomente in den eigenen Prozess ein, verfolgt Fehler und verhindert deren Wiederholung durch Anpassung der Vorgehensweise.	Legt die Standards für Vollständigkeit und Richtigkeit fest, lässt Beispiele prüfen und weist Teams auf strukturelle Nachlässigkeiten hin.

Skill	N1	N3	N5
Integrität und Zuverlässigkeit Handeln im Einklang mit geltenden Standards und Vereinbarungen, auch ohne Aufsicht, sowie Transparenz hinsichtlich eigener Interessen, Fehler und zweifelhafter Fälle.	Hält sich an getroffene Vereinbarungen und Verhaltensregeln und meldet eigene Fehler dem Vorgesetzten.	Meldet von sich aus einen möglichen Interessenkonflikt und bittet um eine Überprüfung, bevor eine Entscheidung getroffen wird.	Legt die Integritätsstandards der Organisation fest, setzt diese auch gegenüber einflussreichen Parteien durch und erläutert die daraus resultierenden Entscheidungen öffentlich.
Rechenschaftspflicht gegenüber Vorgesetzten und Interessengruppen Erläuterung von Ergebnissen, Entscheidungen und Vorfällen gegenüber einem Aufsichtsrat, einem Betriebsrat, Kunden oder einer Aufsichtsbehörde unter Angabe von Fakten, Zusammenhängen und erkennbaren Konsequenzen für die Politik.	Liefert Fakten für einen Rechenschaftsbericht und überprüft diese auf Richtigkeit und Vollständigkeit.	Präsentiert dem Auftraggeber und dem Betriebsrat die Ergebnisse des Teams, nennt zudem, was nicht funktioniert hat und welche Schritte als Nächstes folgen werden.	Rechenschaftsberichte über Unternehmensergebnisse und Vorfälle gegenüber dem Aufsichtsrat, den Medien oder der Politik sowie die Verknüpfung sichtbarer strategischer Anpassungen mit diesen Ereignissen.
Disziplin und Einhaltung von Verpflichtungen Hält sich auch ohne Aufsicht an Vereinbarungen, Abläufe und Verpflichtungen und meldet rechtzeitig, wenn sich eine Verpflichtung als nicht erfüllbar erweist.	Erscheint zur vereinbarten Zeit mit der vereinbarten Arbeit und meldet etwaige Verzögerungen dem Vorgesetzten.	Verpflichtet sich nur zu dem, was machbar ist, behält den Überblick über die eigenen Verpflichtungen und informiert die Beteiligten, sobald eine Frist unter Druck gerät.	Verankert den Standard für die zuverlässige Einhaltung von Arbeitsvereinbarungen und richtet sich an alle Mitarbeiter auf jeder Ebene, die diesen Standard vernachlässigen.
Stressresistenz Liefert auch unter Zeitdruck, bei Widerständen oder unerwarteten Wendungen stets Arbeit von gleichbleibender Qualität und bewahrt im Umgang mit anderen einen sachlichen Ton.	Arbeitet auch bei steigendem Druck weiter an der aktuellen Aufgabe und fragt den Vorgesetzten, welche Aufgabe warten kann.	Arbeitet auch bei höchster Auslastung strukturiert weiter, hält Vereinbarungen mit Kunden klar fest und weist frühzeitig darauf hin, welche Ergebnisse gefährdet sind.	Sorgt dafür, dass die Organisation auch in Krisenzeiten funktionsfähig bleibt, trifft Entscheidungen unter hoher Unsicherheit und setzt Maßstäbe für besonnenes Handeln unter Druck.
Informationssicherheit im Arbeitsprozess Wendet im Arbeitsalltag Sicherheitsmaßnahmen an, wie z. B. den sicheren Austausch, die Klassifizierung und die Speicherung von Informationen, und weist auf riskante Arbeitspraktiken hin.	Hält sich an die Sicherheitsvorschriften für den Austausch und die Speicherung von Informationen und meldet einen vermuteten Vorfall unverzüglich.	Wägt Sicherheitsrisiken bei der Festlegung neuer Arbeitsvereinbarungen ab, passt Maßnahmen an und spricht Kollegen auf unsicheres Verhalten an.	Legt die Richtlinien zur Informationssicherheit fest und überwacht organisationsweit, ob die Prozesse den festgelegten Anforderungen entsprechen.

Skill	N1	N3	N5
Nutzung von Cloud-Plattformen Richtet Dienste in einer Cloud-Umgebung ein und verwaltet diese, regelt Zugriffsrechte und Kosten und wählt je nach Anforderungen zwischen den verfügbaren Diensttypen aus.	Nutzt vorhandene Cloud-Dienste gemäß den Anweisungen und meldet ungewöhnliches Verhalten oder unerwartete Kosten an den Administrator.	Konfiguriert eigenständig Cloud-Dienste für eine Anwendung, richtet Berechtigungen und Backups ein und behält Kosten und Nutzung im Blick.	Legt die Cloud-Strategie des Unternehmens fest und entscheidet, welche Workloads wo platziert werden.
Sensibilisierung für Informationssicherheit Kennt die gängigsten Bedrohungen wie Phishing, Ransomware und Täuschungsversuche, erkennt deren Anzeichen und weiß, welche Maßnahmen in solchen Fällen zu ergreifen sind.	Erkennt eine offensichtliche Phishing-Nachricht, klickt nicht darauf und meldet die Nachricht über den dafür vorgesehenen Kanal.	Erläutert Kollegen, wie Bedrohungen funktionieren, beurteilt zweifelhafte Fälle eigenständig und passt das eigene Verhalten an neue Bedrohungen an.	Entwirft das Sensibilisierungsprogramm des Unternehmens, misst dessen Wirkung und passt den Ansatz auf der Grundlage der gemessenen Ergebnisse an.
Entwicklung von Richtlinien Entwickelt Strategien durch Problemanalyse, Abwägung von Optionen, Konsultation der Beteiligten und Ausarbeitung von Zielen, Instrumenten und Bewertungskriterien.	Sammelt unter Anleitung Zahlen und Dokumente für eine strategische Analyse und fasst die Ergebnisse kurz zusammen.	Erarbeitet eigenständig einen Politikvorschlag mit Optionen und erwarteten Auswirkungen und organisiert die Konsultation der beteiligten Parteien.	Legt den strategischen Kurs für einen Bereich fest, vernetzt die Beteiligten in der Kette und lässt die Auswirkungen systematisch bewerten.
Reaktion auf Sicherheitsvorfälle Reagiert auf einen Sicherheitsvorfall gemäß dem Runbook, indem er diesen eindämmt, Beweismittel sichert, Daten wiederherstellt und die zuständigen Stellen rechtzeitig informiert.	Meldet einen vermuteten Vorfall unverzüglich, rührt nichts an und befolgt die Anweisungen des Koordinators.	Begrenzt eigenständig den Schaden während eines Vorfalls, sichert Beweismittel und liefert einen nachvollziehbaren Ablauf der Ereignisse.	Leitet das unternehmensweite Einsatzteam, trifft Entscheidungen zur externen Kommunikation und verbessert das Runbook nach jeder Übung.
Aus Fehlern und Vorfällen lernen Untersucht nach einem Fehler oder Vorfall, was geschehen ist, benennt die Ursache, ohne die Schuld auf andere abzuwälzen, und passt die Arbeitsweise in diesem Punkt an.	Meldet einen eigenen Fehler unverzüglich dem Vorgesetzten und führt die Aufgabe gemäß der korrigierten Anweisung erneut aus.	Analysiert eigene Fehler sowie die des Teams, erörtert die Ursachen offen in der Arbeitsbesprechung und passt die Vereinbarungen entsprechend an.	Stellt sicher, dass Vorfälle unternehmensweit sicher gemeldet werden, lässt die Ursachen systematisch analysieren und lässt die daraus gewonnenen Erkenntnisse in Richtlinien und Standards einfließen.

Skill	N1	N3	N5
Aktueller Fachstand und Fachliteratur Verfolgt die Entwicklungen im eigenen Berufsfeld anhand von Fachliteratur, Leitlinien und Netzwerken und lässt relevante neue Erkenntnisse in die eigene Praxis einfließen.	Erfasst die erhaltenen beruflichen Informationen und ermittelt, welche Aspekte für die eigene Arbeit von Bedeutung sind.	Erfasst Quellen und Leitlinien systematisch, bewertet deren Qualität und passt die eigene Arbeitsweise an neue Erkenntnisse an.	Bewerten den Stand der Forschung, wägen widersprüchliche Forschungsergebnisse ab und legen fest, welche Leitlinien die Organisation künftig befolgen wird.
Erstellung technischer Dokumentationen Verfasst Handbücher, Supportdokumentationen und Entscheidungsprotokolle, denen ein Leser ohne Vorkenntnisse Schritt für Schritt folgen kann und die stets auf dem neuesten Stand bleiben.	Füllt eine Dokumentationsvorlage mit den einzelnen Schritten einer Aufgabe aus und lässt den Text von einem Kollegen überprüfen.	Verfasst die vollständige Dokumentation für ein System oder einen Prozess, testet diese mit einem Laien und pflegt die verschiedenen Versionen.	Legt den Dokumentationsstandard des Unternehmens fest und stellt sicher, dass die Dokumentation Bestandteil jeder Lieferung ist.
Prozessautomatisierung Analysiert einen wiederkehrenden Arbeitsprozess, entwickelt oder beauftragt die Automatisierung seiner einzelnen Schritte und überprüft, ob das Ergebnis zuverlässig bleibt.	Führt eine bestehende Automatisierung durch und meldet, wenn das Ergebnis von den Erwartungen abweicht.	Beschreibt einen Prozess in einzelnen Schritten, automatisiert die wiederholbaren Schritte und integriert Prüfungen auf Fehler und Ausnahmen.	Legt die Automatisierungsstrategie des Unternehmens fest und entscheidet, welche Prozesse automatisiert werden und welche nicht.
Funktions- und Anwendungsmanagement Stellt sicher, dass eine Anwendung funktionsfähig und für die Nutzer geeignet bleibt, indem er Anforderungen erfasst, Einstellungen verwaltet und Änderungen mit dem Anbieter abstimmt.	Bearbeitet Nutzeranfragen zu einer Bewerbung gemäß den Anweisungen und erfasst die Anfragen im dafür vorgesehenen Register.	Verwaltet eigenständig eine Anwendung, priorisiert Änderungswünsche gemeinsam mit den Anwendern und testet neue Versionen, bevor diese in Betrieb genommen werden.	Legt fest, wie das funktionale Management organisiert ist, und entscheidet über die Lebensdauer von Anwendungen.
Störungsmanagement und Fehlerbehebung Erfasst Störungen, ermittelt deren Ursache durch gezielte Maßnahmen, stellt den Betrieb wieder her und hält Melder sowie Beteiligte auf dem Laufenden.	Erfasst eine Störung lückenlos, durchläuft die Standardschritte und eskaliert den Fall, sobald die eigenen Maßnahmen nicht zum Erfolg führen.	Leitet eine Untersuchung zu einer unbekannten Störung ein, stellt den Betrieb wieder her und dokumentiert Ursache und Lösung zur späteren Wiederverwendung.	Entwirft den Vorfallmanagementprozess des Unternehmens, leitet die Reaktion auf größere Störungen und legt diese gegenüber der Geschäftsleitung und den Kunden Rechenschaft ab.

Skill	N1	N3	N5
Datenklassifizierung und -aufbewahrung Klassifiziert Informationen nach Vertraulichkeitsgrad und Wichtigkeit, ordnet ihnen Aufbewahrungsfristen zu und stellt sicher, dass die Löschung und Archivierung tatsächlich erfolgen.	Weist gemäß dem Schema eine Klassifizierungskategorie zu und leitet unklare Fälle an den Administrator weiter.	Legt die Klassifizierung und die Aufbewahrungsfrist für einen Informationsfluss fest und überprüft, ob die Bereinigung wie geplant erfolgt.	Entwirft die Klassifizierungs- und Aufbewahrungsrichtlinien der Organisation und berücksichtigt diese bei Audits und bei der Aufsicht.
Grundkenntnisse im Bereich Netzwerke Verfügt über ein umfassendes Verständnis der Funktionsweise von Netzwerken, einschließlich Adressierung, Routing, Ports und Namensauflösung, und kann angeben, wo Verbindungsprobleme auftreten können.	Erläutert, aus welchen Teilen eine Verbindung besteht, und führt eine vorgegebene Prüfung durch, beispielsweise einen Konnektivitätstest.	Leitet anhand von Symptomen ab, in welcher Netzwerkschicht ein Problem vorliegt, und untermauert dies durch eigene Messungen.	Verbreitet Netzwerkwissen innerhalb der Organisation, legt Gestaltungsgrundsätze fest und prüft Netzwerkentwürfe von Anbietern.
IT-Lieferanten- und Vertragsmanagement Verwaltet Vereinbarungen mit IT-Lieferanten hinsichtlich Lieferung, Leistung und Kosten, überwacht die Einhaltung der Vereinbarungen und spricht Abweichungen gegenüber den Lieferanten an.	Prüft Rechnungen und erbrachte Leistungen anhand des Vertrags und meldet Abweichungen an den Vertragsmanager.	Führt Besprechungen mit Lieferanten zu Leistung und Kosten durch, dokumentiert Vereinbarungen und greift ein, wenn Vereinbarungen nicht eingehalten werden.	Legt die Lieferantenrichtlinien des Unternehmens fest, schließt die wichtigsten Verträge ab und entscheidet über Kündigungen oder einen Wechsel.
Systemadministration und -überwachung Stellt den reibungslosen Betrieb der Systeme sicher, indem er Einstellungen, Updates und Berechtigungen verwaltet, Überwachungsmaßnahmen einrichtet und auf Signale reagiert, bevor die Nutzer davon betroffen sind.	Führt geplante Wartungsaufgaben und Aktualisierungen gemäß dem Runbook durch und meldet Abweichungen bei den Überwachungssignalen.	Verwaltet eigenständig eine Systemumgebung, legt Überwachungsschwellenwerte fest und beseitigt wiederkehrende Ursachen für Störungen.	Legt die Verwaltungs- und Überwachungsstandards der Organisation fest und entscheidet über die Gestaltung der Systemumgebung.

6 Bewertungsmethoden und Validität

Bei den Validitätswerten handelt es sich um die korrigierten metaanalytischen Schätzungen von Sackett, Zhang, Berry und Lievens (2022) aus dem „Journal of Applied Psychology“, die die älteren Zahlen von Schmidt und Hunter (1998) ersetzen. Die Streuung ist ebenso wichtig wie der Mittelwert: Bei einer hohen Standardabweichung (SD) variiert die Validität stark je nach Kontext.

Messmethode	rho	SD	Was ist das?
Assessment-Center	**0.29**	**0.09**	Mehrere Übungen, mehrere Bewerter, bewertungsdimensionenbezogene Benotung.
Wissenstest	**0.40**	**0.13**	Test zur Überprüfung des deklarativen Fachwissens, der in der Regel kundenspezifisch zusammengestellt wird.
Arbeitsproben-Test	**0.33**	**0.09**	Der Bewerber führt unter standardisierten Bedingungen eine repräsentative Arbeitsprobe durch.
Persönlichkeitsfragebogen	**0.40**	**0.15**	Selbstauskunft zu Verhaltenspräferenzen. Unter hrmforce finden Sie den „Big Fifty“ und den „15PF“.
Portfolio oder Nachweise	-	-	Eine Sammlung früherer Arbeiten oder Ergebnisse, die anhand festgelegter Kriterien bewertet wurden.
Simulation	-	-	Simulierte Arbeitssituation, in der Regel digital, mit standardisierter Bewertung.
Situational Judgement Test	**0.12**	**0.11**	Szenario mit Antwortmöglichkeiten, das hinsichtlich Wissen oder Verhaltenstendenzen bewertet wird.
Strukturiertes Interview	**0.42**	**0.19**	Verhaltensorientiertes Vorstellungsgespräch mit festgelegten Fragen und einer Bewertungsskala pro Frage.

7 Assessment-Instrumente für diesen Beruf

hrmforce-Instrument	Kompetenzen	Was damit gemessen wird
Wissenstest (kundenspezifisch)	**14**	Fachwissenstest, individuell auf jeden Kunden zugeschnitten
Arbeitsproben-Test	**9**	Repräsentatives Arbeitsbeispiel unter standardisierten Bedingungen
Competency Check	**6**	Kompetenzbeurteilung auf Verhaltensebene
360 Feedback	**5**	Mehrere Bewertungen auf der Grundlage von Verhaltensankern
Portfolio	**5**	Bewertung bisheriger Arbeiten anhand festgelegter Kriterien
Big Fifty	**3**	Persönlichkeitsfragebogen, 150 Items, 25 Faktoren
Ability Scan	**2**	Eignungstest: Verbale, numerische und abstrakte Denkfähigkeiten
Strukturiertes Interview	**2**	Verhaltensorientiertes Vorstellungsgespräch mit fester Struktur
15PF	**2**	„Personality Profile“, eine kürzere Alternative zum „Big Fifty“
Big Fifty (Integritätsskala)	**1**	

hrmforce-Instrument	Kompetenzen	Was damit gemessen wird
Mental Resilience (4C)	**1**	Psychische Belastbarkeit gemäß dem 4C-Modell

8 So verwenden Sie dieses Profil

1. Stimmen Sie das Profil mit dem Personalverantwortlichen ab, bevor der erste Kandidat bewertet wird. Nachträglich vorgenommene Gewichtsanpassungen machen das Ergebnis nicht mehr vertretbar.
2. Wählen Sie die Bewertungsmethode pro Kompetenz aus der Spalte „Bewertungsmethode“ aus. Kombinieren Sie maximal drei Methoden pro Bewerber.
3. Führen Sie in einer zweistündigen Sitzung eine Kalibrierung der Bewerter anhand der Ankerwerte aus Kapitel 5 durch. Ankerwerte ohne Schulung der Bewerter sind kaum aussagekräftig.
4. Füllen Sie den Übereinstimmungsrechner aus und besprechen Sie die Lücken im Entwicklungsgespräch. Typ A und Typ G sind Auswahlkriterien, keine Entwicklungsziele für das erste Quartal.

Quelle: hrmforce Skills Framework 2.0, Version 2.0.0, erstellt am 2026-09-08. Zuordnungen zu ESCO v1.2.1, O*NET 31.0, Lightcast Open Skills, SFIA 9, DigComp 3.0, EntreComp, LifeComp, GreenComp, AILit, WEF Future of Jobs 2025, ISCO-08 sowie zur niederländischen CBS-Berufsklassifikation BRC 2014, Ausgabe 2025. Dieses Profil dient als Ausgangspunkt und stellt keinen Standard dar: Passen Sie es an Ihre eigene Organisation an, bevor Sie darauf basierend eine Auswahl treffen.