§ 4 InSiFPrV — Prüfungsbereich „Informationssicherheit gewährleisten“

Informationssicherheits-Fortbildungsprüfungsverordnung
Stand: 01.11.2024 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

Im Prüfungsbereich „Informationssicherheit gewährleisten“ hat die zu prüfende Person nachzuweisen, dass sie in der Lage ist, Bedrohungs- und Risikoszenarien zu analysieren, Sicherheitsmaßnahmen zu planen, einzuleiten und zu dokumentieren sowie den sicheren Betrieb von IT-Systemen zu gewährleisten. In diesem Rahmen wird aus den Inhalten der folgenden Qualifikationsschwerpunkte geprüft:

1. Qualifikationsschwerpunkt „Bedrohungs- und Risikoszenarien analysieren“:

   a) Durchführen von Risiko- und Schwachstellenanalysen in Bezug auf die Informationssicherheit anhand von Vorgaben,

   b) Mitwirken bei der Erstellung von Datenschutz-Folgenabschätzungen im Hinblick auf mögliche Datenschutzverletzungen,

   c) Analysieren von IT-Infrastrukturen, von Netzwerkkommunikation, von Protokolldaten, von Softwareverhalten und von System- und Softwarekonfigurationen sowie Ableiten von risikominimierenden Schutz- und Gegenmaßnahmen sowie

   d) Identifizieren und Analysieren von Schadsoftware und deren Verbreitungswegen sowie Dokumentieren der Analyseergebnisse,
2. Qualifikationsschwerpunkt „Sicherheitsmaßnahmen planen“:

   a) Mitwirken bei der Entwicklung eines Konzepts zur Informationssicherheit,

   b) Definieren von Notfallsystemen in Absprache mit den jeweiligen Fachabteilungen und Ansprechpartnern,

   c) Erstellen von Rechte- und Rollenkonzepten zur Einhaltung von Datenschutzbestimmungen und zur Gewährleistung der Datensicherheit,

   d) fachliches Unterstützen bei der Erstellung datenschutzrelevanter Dokumente,

   e) Mitwirken bei der Erstellung und Einführung eines Informationssicherheitsmanagementsystems,

   f) fachliches Beraten bei der Entwicklung von Testkonzepten, insbesondere zur Koordination und Durchführung von Schwachstellen- und Penetrationstests,

   g) Bereitstellen von aktuellen IT-Sicherheitsinformationen und Aufbereiten sicherheitsrelevanter Erkenntnisse,

   h) Informieren von Anwenderinnen und Anwendern über Regularien der Informationssicherheit, insbesondere zur Datenklassifizierung sowie zum Umgang mit IT-Ausstattung und mit Daten sowie

   i) Sicherstellen der Einhaltung der Regularien zur Informationssicherheit,
3. Qualifikationsschwerpunkt „Sicheren Betrieb gewährleisten“:

   a) Umsetzen der Vorgaben eines Sicherungs- und Wiederherstellungskonzepts sowie Testen der Funktionalität des Sicherungs- und Wiederherstellungskonzepts,

   b) Konfigurieren von Soft- und Hardware der Sicherheitsinfrastruktur zur Gewährleistung der Informationssicherheit anhand definierter Sicherheitsrichtlinien,

   c) Durchführen von Notfallübungen und Dokumentieren der Ergebnisse,

   d) Erstellen und Umsetzen von Schulungskonzepten zur Sicherstellung des Datenschutzes und der Datensicherheit, insbesondere im Hinblick auf die Sensibilisierung der Mitarbeitenden,

   e) Überprüfen der Einhaltung von Sicherheitsvorgaben, auch im Bereich von Kritischen Infrastrukturen,

   f) fortlaufendes Bewerten von Sicherheitsrisiken und Ableiten von Sicherheitsmaßnahmen aus den ermittelten Sicherheitsrisiken,

g) fortlaufendes Berichten und Dokumentieren des Status von Maßnahmen zur Sicherstellung der Informationssicherheit,

h) Mitwirken bei der Planung und Durchführung von Sicherheitsaudits sowie bei der Bewertung und Behandlung von Schwachstellen und Sicherheitsvorfällen,

i) Mitwirken bei der Überprüfung und der Analyse von Anwendungssoftware im Hinblick auf die Gefährdung der Informationssicherheit,

j) Gewährleisten der Sicherheit vernetzter Systeme und Geräte durch die Umsetzung von Ende-zu-Ende-Verschlüsselungen sowie durch die Integration sicherer Geräteauthentifizierungen und digitaler Identitäten,

k) Mitwirken beim Einsatz von Lösungen zur Sicherheitsüberwachung unter Berücksichtigung rechtlicher Aspekte,

l) Organisieren und Durchführen von Penetrationstests im laufenden Betrieb sowie

m) Unterstützen bei der Implementierung eines datenbasierten Security-Information-and-Event-Managements sowie Analysieren, Auswerten und Interpretieren von aktuellen und vergangenen sicherheitsrelevanten Ereignissen,

4. Qualifikationsschwerpunkt „Sicherheitsmaßnahmen einleiten, dokumentieren und evaluieren“:

a) Erkennen und Dokumentieren von IT-Sicherheitsvorfällen sowie Informieren der verantwortlichen Stellen über IT-Sicherheitsvorfälle,

b) Auswählen, Durchführen und Evaluieren von Tests der Sicherheitsinfrastruktur, Dokumentieren der Evaluationsergebnisse, einschließlich Hinweisen auf Schwachstellen in der Sicherheitsinfrastruktur sowie Einleiten von Maßnahmen zur Verbesserung der Sicherheitsinfrastruktur,

c) Gewährleisten der Qualitätssicherung, insbesondere durch Dokumentieren der IT-Sicherheitsmaßnahmen,

d) Archivieren datenschutzrelevanter und IT-sicherheitsrelevanter Unterlagen nach betrieblichen und rechtlichen Vorgaben, insbesondere von Verträgen, Richtlinien und Dokumentationen,

e) Einleiten von Notfallmaßnahmen bei akuten Bedrohungssituationen sowie

f) Einleiten von Prozeduren zum Wiederanlauf von Systemen gemäß Notfallhandbuch sowie Testen und Sicherstellen der Funktionalität der wiederangelaufenen Systeme,

5. Qualifikationsschwerpunkt „Organisatorische und rechtliche Vorgaben“:

a) Ermitteln von Anforderungen an Datensicherheitskonzepte,

b) Mitwirken bei der Entwicklung von Datensicherheitskonzepten,

c) Berücksichtigen und Umsetzen von Datensicherheitskonzepten,

d) Identifizieren und Bewerten von Risiken sowie Einleiten von Maßnahmen zur Minimierung von Risiken sowie

e) Sicherstellen der Einhaltung organisatorischer und rechtlicher Vorgaben sowie

6. Qualifikationsschwerpunkt „Projektunterstützung und -koordination“:

a) Unterstützen der Projektleitung durch Übernehmen und Umsetzen von Teilprojekten,

b) organisatorisches Begleiten von Projekten, insbesondere Erstellen von Projektplänen und Planen des Mitarbeitendeneinsatzes,

c) Mitwirken bei der Aufwandsanalyse und -kalkulation von Projekten,

d) projektbegleitendes Beraten von Kunden sowie Unterstützen und Beraten von Kunden in der Roll-out-Phase,

e) Mitwirken beim Projektcontrolling, bei der Nachverfolgung von Aufgaben und beim Aufbereiten von Statusberichten sowie

f) Planen und Umsetzen von projektbezogenen Schulungs- und Trainingsmaßnahmen.