ICT Berufsbildung
Formation professionnelle
Formazione professionale

ICT-Berufsbildung Schweiz

WEGLEITUNG zur

Prüfungsordnung über die

Höhere Fachprüfung für ICT Security Expert

vom 14. August 2017

Die Prüfungskommission erlässt gestützt auf Ziffer 2.11 der Prüfungsordnung über die Höhere Fachprüfung **ICT Security Expert** folgende Wegleitung:

1 EINLEITUNG

Gestützt auf Ziffer 2.21 Bst. a der Prüfungsordnung über die Höhere Fachprüfung ICT Security Expert vom dd.mmm.2017 erlässt die Prüfungskommission folgende Wegleitung zur genannten Prüfungsordnung.

1.1 Zweck der Wegleitung

Die Wegleitung ergänzt und präzisiert die Bestimmungen der Prüfungsordnung. Die Wegleitung wird durch die Prüfungskommission erlassen, periodisch überprüft und bei Bedarf angepasst.

1.2 Gesetzliche Grundlagen

- Bundesgesetz über die Berufsbildung (Berufsbildungsgesetz, BBG)
- Verordnung über die Berufsbildung (Berufsbildungsverordnung, BBV)

1.3 Prüfungssekretariat und Ansprechstelle

Die Geschäftsstelle erledigt für alle Sprachregionen die mit den Fachprüfungen verbundenen administrativen Aufgaben und ist die Ansprechstelle für diesbezügliche Fragen:

ICT-Berufsbildung Schweiz
Aarbergergasse 30
3011 Bern
Tel.: +41 58 360 55 50
Email: info@ict-berufsbildung.ch
www.ict-berufsbildung.ch

1.4 Erläuterungen zur Berufspraxis (Ziff. 3.31 der PO)

a) Die geforderten Praxisjahre müssen im Zeitpunkt der Prüfung erreicht sein.

b) Unter hauptberuflicher Praxis wird eine Tätigkeit zu 100% verstanden. Teilzeitpensen werden pro rata angerechnet, d.h. die erforderliche Praxisdauer verlängert sich entsprechend.

1.5 Kompetenzbeschreibung

Die Kompetenzbeschreibungen aller für den Erwerb des eidgenössischen Diploms vorausgesetzten Kompetenzen sind in der Kompetenzen-Datenbank der Trägerschaft hinterlegt. (www.ict-berufsbildung.ch).

2 BERUFSBILD

Das Berufsbild ist in Ziffer 1.2 der Prüfungsordnung dargestellt.

3 ZULASSUNGSBEDINGUNGEN

Die Zulassungsbedingungen sind in Ziffer 3.3 der Prüfungsordnung dargestellt.

4 PRÜFUNG

4.1 Prüfungsteile, Prüfungsdauer und Gewichtung

	Prüfungsteil	Art der Prüfung	Dauer	Gewichtung des Prüfungsteils
1	Portfolioarbeit Expertengespräch zum Portfolio	schriftlich mündlich	Vorgängig ca. 40 Minuten	2
2	Fallstudien	schriftlich	ca. 120 Minuten	1
3	Fallsimulationen	praktisch	ca. 300 Minuten	2

4.2 Beschreibung der Prüfungsteile

Prüfungsteil 1, Portfolio und Expertengespräch

Alle Kandidatinnen und Kandidaten führen ein Portfolio, in welchem sie die Theorie mit der Praxis verknüpfen. Das Portfolio ist eine reflektierte und kommentierte Sammlung von Materialien verschiedener Art, in welcher die Kandidatinnen und Kandidaten das erworbene theoretische Wissen durch eine Transferleistung auf praktische Beispiele im Arbeitsalltag anwenden. Im Portfolio müssen in den Handlungskompetenzbereichen verschiedene Handlungskompetenzen bearbeitet werden (Anhang A). Die detaillierten inhaltlichen und formalen Vorgaben für das Portfolio sind im Leitfaden «Portfolioarbeit» festgelegt. Das individuelle Portfolio dient als Basis für das Expertengespräch, in welchem die Kandidatinnen und Kandidaten Fragen der Expertinnen und Experten ihrer Arbeit beantworten.

Prüfungsteil 2, Fallstudien

Die Kandidatinnen und Kandidaten erhalten realitätsnahe Fälle zur schriftlichen Bearbeitung. Die Auswahl der Fälle erfolgt so, dass eine Auswahl aus Handlungskompetenzen aus allen Handlungskompetenzbereichen überprüft wird (Anhang A).

Prüfungsteil 3, Fallsimulationen

Die Kandidatinnen und Kandidaten bearbeiten an mehreren Posten alleine wie auch im Team verschiedene Situationen, die der beruflichen Realität nahe kommen. Die Lösung der Fallsimulationen findet unter Beobachtung statt und wird anschliessend ausgewertet und beurteilt. Im Rahmen der Fallsimulationen werden auch verschiedene Haltungen überprüft, wobei der Teamfähigkeit, der Kommunikationsfähigkeit und dem Urteilsvermögen ein besonderes Gewicht beigemessen wird. Die detaillierten inhaltlichen und formalen Vorgaben für die Fallsimulationen sind im Leitfaden «Fallsimulationen» festgelegt.

4.3 Beurteilungskriterien

Die inhaltlichen und formalen Vorgaben für die Beurteilung der Prüfung wird in den Leitfäden «Portfolioarbeit» und «Fallsimulationen» festgelegt.

4.4 Notengebung

Die Notengebung in Ziffer 1.2 der Prüfungsordnung dargestellt.

5 ORGANISATION DER PRÜFUNG

Vor der Prüfung	12 Monate	Abgabe von Informationen zu Inhalt und Form der Portfolioarbeit und Start
	5 Monate	Ausschreibung der Prüfungstermine Beginn der Anmeldung, Öffnen des Anmeldefensters auf der Webseite.
	4 Monate	Anmeldeschluss
	3 Monate	Zulassungsentscheid
	3 Monate	Einreichen der Portfolioarbeit
	6 Wochen	Aufgebot zur mündlichen und schriftlichen Prüfung
	4 Wochen	Rücktrittsbegehren eingereicht.
	Das Aufgebot zur mündlichen und schriftlichen Prüfung beinhaltet keine Aussage darüber, wie die Portfolioarbeit beurteilt wurde.	
Prüfung	Teilnahme an den Prüfungsteilen 1, 2 und 3	
Nach der Prüfung	Die Mitteilung der Resultate an die Kandidatinnen und Kandidaten erfolgt spätestens 5 Wochen nach dem letzten Prüfungstag.	

5.1 Prüfungsakten

Die Portfolioarbeit, die Aufgaben, Lösungsblätter, Präsentationsmittel, Notenunterlagen und Bewertungen der Prüfungen werden Bestandteil der Prüfungsakten. Die Experten/Expertinnen sind zu Stillschweigen über die eingereichten Unterlagen und Bewertungen verpflichtet. Die Vertraulichkeit ist gewährleistet.

5.2 Internetauftritt der ICT-Berufsbildung Schweiz

Die Website von ICT-Berufsbildung Schweiz enthält alle relevanten Informationen und Dokumente zur Prüfung. Die Informationen zu den Kompetenzinhalten, die in der Kompetenzen-Datenbank enthalten sind, sind für die gezielte Vorbereitung unentbehrlich:
www.ict-berufsbildung.ch

5.3 Informationen für Kandidierende

Auf der Homepage des SBFI finden sich weitere Informationen für Kandidierende.
https://www.sbfi.admin.ch/sbfi/de/home/themen/hbb/allgemeine-informationen-ep/kandidierende-und-absolvierende.html

- Merkblatt: Nachteilsausgleich für Menschen mit Behinderung
- Merkblatt: Akteneinsichtsrecht
- Merkblatt: Beschwerden gegen Nichtzulassung zur Prüfung und Nichterteilung des eidg. Fachausweises bzw. Diploms

5.4 Fachliteratur

Literaturhinweise werden im Beschwerdefall in der Regel nicht als Beweismittel berücksichtigt.

6 ERLASS

BERN, 14.08.2017

Daniel Jäggli	*Mario Rusca*
Präsident der Prüfungskommission	Prüfungsleiter

ANHANG A: QUALIFIKATIONSPROFIL

INHALTSVERZEICHNIS

– **Handlungskompetenzen**

Übersicht der Handlungskompetenzen

Handlungskompetenzbereiche		Handlungskompetenzen								
a	Verankern der Sicherheitsstrategie	a1: Informationssicher-heitsgrundlagen erarbeiten	a2: Informations sicherheit in der Geschäftsleitung und im Verwaltungsrat verankern	a3: Führung und Steuerung der Informationssicher heit managen	a4: Sicherheitsor ganisation etablieren	a5: Informationssicher-heitsspezialisten fachlich führen				
b	Etablieren des Informationssicherheits-Managementsystems (ISMS)	b1: ISMS führen	b2: Prozesse etablieren	b3: Risiken managen	b4: Informationssicher-heitsanforderungen in allen Prozessen integrieren	b5: Sicherheitsvorgaben definieren	b6: Sicherheitsüber-prüfung sicherstellen	b7: Security im Outsourcing überwachen	b8: Performance messen	b9: Informationsspezi-fische Anforderungen an Personensicher-heitsüberprüfung definieren
c	Führen des Sicherheitsprogramms	c1: ICT-Security-Architektur erarbeiten	c2: Produkt- / Service-Portfolio managen	c3: Portfoliomanagement Security-Programm erstellen	c4: Business Case entwickeln	c5: Information-sicherheitslö-sungen evaluieren	c6: Umsetzung der beschlossenen Massnahmen sicherstellen	c7: Projekte leiten	c8: Innovationen in die Informationssicherheit integrieren	
d	Managen von Stakeholdern	d1: Tragfähiges trusted Netzwerk unterhalten	d2: Stakeholder fachlich beraten	d3: Informationssicher-heitscompliance einfordern	d4: Projekte begleiten	d5: Sicherheits-aspekte in Proofs of Concept sicherstellen				
e	Schaffen von Awareness	e1: Awarenesskampagne durchführen	e2: Sicherheits-kommunikation intern und extern sicherstellen							
f	Bewältigen von Ereignissen	f1: Business-Impact-Analyse sicherstellen	f2: Notfallorganisation für Security Incidents sicherstellen	f3: Security Incident managen	f4: Integrieren von Informatiksicherheits-aspekten im Business Continuity Management sicherstellen					
g	Sichern von Informationen	g1: Klassifizierung von Informationen sicherstellen	g2: Datensicherheit bei der Übertragung sicherstellen	g3: Datensicherheit bei der Speicherung und Archivierung sicherstellen						

A) Verankern der Sicherheitsstrategie

Beschreibung des Handlungskompetenzbereichs:
ICT Security Experts erarbeiten die Informationssicherheitsstrategie für ihr Unternehmen auf der Basis des Informationsrisikoappetits der Geschäftsleitung und des Verwaltungsrats. Sie definieren die Bedrohungsszenarien und den Sollzustand, analysieren die Abweichungen und leiten daraus die strategischen Ziele ab, um sie zu schliessen. Sie fordern die Verabschiedung der Informationssicherheitsstrategie durch die Geschäftsleitung und den Verwaltungsrat ein. Anschliessend definieren sie die Informationssicherheits-Governance und setzen diese um.

Sie verankern die Informationssicherheit in der Organisation und führen die Sicherheitsorganisation. Dazu gehört die Definition der Rolle des Steuerungsgremiums in Abstimmung mit der Organisation und die Bestimmung der Mitglieder. Sie definieren die Ausbildung der Rollenträger der Sicherheitsorganisation, führen deren Ausbildung durch und überprüfen den Reifegrad der Sicherheit in der Organisation.

ICT Security Experts können ein Team von Informationssicherheitsspezialisten im fachlichen Bereich führen, identifizieren Wissenslücken und legen Ausbildungspläne fest. Weiter gewährleisten sie konstanten Erfahrungs- und Wissensaustausch zwischen den Informationssicherheitsspezialisten.

Kontext:
Die Informationssicherheitsstrategie bestimmt die Tätigkeit der ICT Security Experts. Sie definiert die Fähigkeiten und Kontrollen, die für die Einhaltung des Informationsrisikoappetits notwendig sind. Die Abweichungsanalyse identifiziert bestehenden Verbesserungsbedarf. Daraus leiten sich die strategischen Ziele ab, die diese Abweichungen behandeln und aus diesen Zielen die Tätigkeit der ICT Security Experts.

Ein zentraler Erfolgsfaktor einer Informationssicherheitsstrategie ist die Ausrichtung der Informationssicherheitsstrategie an allen Informationssicherheitsaspekten des Unternehmens. Dies bedeutet, dass die ICT Security Experts die Prozesse, die Wertschöpfungskette, die schützenswerten Assets und die Strategie der Unternehmung kennen müssen. Die Informationssicherheitsstrategie ist dann in die Unternehmensstrategie einzubetten.

Die Geschäftsleitung und der Verwaltungsrat haben die zentrale Rolle bei der Verankerung der Sicherheitsstrategie. Sie definieren den Informationssicherheitsrisikoappetit und verankern die Informationssicherheitsprogramme. Die ICT Security Experts sorgen für ein gemeinsames Verständnis der Risikoszenarien und der damit verbundenen Risiken. Die ICT Security Experts achten bei der Umsetzung auf eine breite Abstützung im Unternehmen.

Damit die Sicherheit als ein Kulturelement der Organisation wahrgenommen und von allen gelebt wird, muss eine Sicherheitsorganisation etabliert werden. Die ICT Security Experts tragen dafür die organisatorische und fachliche Verantwortung. Sie stellen sicher, dass die Rollenträger ihre Aufgaben, Verantwortlichkeiten und Kompetenzen im Bereich Informationssicherheit kennen und die Sicherheitskultur (vor)leben.

Die Informationssicherheitsspezialisten müssen fachlich stets auf dem aktuellen Stand sein. Nur so können Sicherheitsereignisse vermieden oder ihre Auswirkung vermindert werden. Die ICT Security Experts garantieren dies mit Ausbildung und konstantem gegenseitigem Erfahrungs- und Informationsaustausch. Dies führt zu einer besseren Akzeptanz der Informationssicherheitsspezialisten im Unternehmen.

Der Handlungskompetenzbereich A ist die Basis für die Handlungskompetenzbereiche B - Etablieren des Informationssicherheits-Managementsystems (ISMS) und C - Führen des Sicherheitsprogramms.

A) Verankern der Sicherheitsstrategie (Übersicht)

Berufliche Handlungskompetenzen	**Wichtige Themen / Inhalte**	**Leistungskriterien**
A1 – Informationssicherheits-grundlagen erarbeiten	Inhalt/Elemente einer Informationssicherheitsstrategie, Industrielle Informatik	ICT Security Experts sind fähig: - eine Unternehmensstrategie zu analysieren - die Implikationen der regulatorischen Vorgaben für die Unternehmung abzuleiten - die Bedrohungsszenarien mit Relevanz für die Organisation zu definieren - die Risiken zu analysieren - eine Informationssicherheitsstrategie auf der Basis des Risikoappetits der Geschäftsleitung und des Verwaltungsrats zu erarbeiten - eine Gap-Analyse durchzuführen - eine Informationssicherheits-Governance zu definieren und umzusetzen - adressatengerecht zu präsentieren - ICT Security-Verantwortlichkeiten zu definieren (RACI: Responsible, Accountable, Consulted and Informed) - ein ICT-Sicherheitsdispositiv zu erstellen und in der Organisation zu verankern - den Reifegrad der Sicherheit in der Organisation zu ermitteln - den Inhalt von Security-Publikationen an ihr Team weiterzugeben - unterstellte Mitarbeitende fachlich zu unterstützen - eine Community von Informationssicherheitsspezialisten zu etablieren und den konstanten Erfahrungs- und Wissensaustausch zu gewährleisten - den eigenen Weiterbildungsbedarf und jenen des Teams zu erkennen und Massnahmen umzusetzen
A2 – Informationssicherheit in der Geschäftsleitung und im Verwaltungsrat verankern	Präsentationstechnik	
A3 – Führung und Steuerung der Informationssicherheit managen		
A4 – Sicherheitsorganisation etablieren		
A5 – Informationssicherheits-spezialisten fachlich führen	Führungskompetenz	

B) Etablieren des Informationssicherheits-Managementsystems (ISMS)

Beschreibung des Handlungskompetenzbereichs:
ICT Security Experts stellen den Managementsupport für das ISMS sicher und steuern den Plan-Do-Check-Act-Regelkreis. Sie gestalten und führen Prozesse zur Steuerung und Implementierung der Informationssicherheit. Für die Prozessüberwachung definieren sie geeignete Kennzahlen, messen und bewerten diese.

Sie beobachten die Entwicklung im Bereich neuer Technologien und das sicherheitsrelevante Umfeld. Sie ermitteln und dokumentieren Bedrohungen, erkennen interne Schwachstellen und leiten daraus den Handlungsbedarf ab. Sie überprüfen die Liste der dokumentierten Sicherheitsrisiken regelmässig auf ihre Aktualität, führen Interviews mit Stakeholdern zu deren Einschätzung der Risikobeurteilung und rapportieren Auswirkungen und Gefahrenpotenziale an die Geschäftsleitung und den Verwaltungsrat.

Sie unterstützen die Prozessverantwortlichen bei der Umsetzung der Sicherheitsanforderungen für deren Prozesse. Zusammen mit den Prozess-, Weisungs- und Projektverantwortlichen definieren sie die Sicherheitsvorgaben und integrieren sie in die entsprechenden Vorgabedokumente. Sie veranlassen Sicherheitsüberprüfungen durch interne und externe Auditoren. Sie kategorisieren Schwachstellen, veranlassen deren Kontrolle und führen erforderliche Wiederholungsüberprüfungen und Retests durch.

Sie definieren mit den HR-Verantwortlichen die Anforderungen an die Personensicherheitsüberprüfung (PSÜ), erstellen ein PSÜ-Dokument, legen den Prozess fest und schulen die HR-Mitarbeitenden in der Umsetzung des PSÜ-Prozesses.

Kontext:
Ein ISMS kann die gesamte Informationssicherheit einer Organisation steuern. Das ISMS muss laufend überprüft und angepasst werden. Die ICT Security Experts müssen sicherstellen, dass Prozesse auf dem aktuellsten Stand gemäss Anforderungen des ISMS sind.

Das Wissen der ICT Security Experts muss jederzeit auf dem aktuellsten Stand sein (Bedrohungsentwicklung, Technologien, Standards, Regulatorien, Gesetze und Mitbewerber). Nur so können sie auf die Entwicklungen reagieren und die geforderte Informationssicherheit der Organisation gewährleisten.

Applikationen, Systeme und Informationen werden regelmässig einer Sicherheitsüberprüfung unterzogen. Dadurch können Schwachstellen erkannt, behoben und wiederum die Sicherheit erhöht werden. Weiter werden neue Funktionen vor Inbetriebnahme einer Sicherheitsprüfung unterzogen. Ausgelagerte Dienstleistungen müssen darauf überprüft werden, ob sie die Sicherheitsanforderungen erfüllen. Auf dieser Basis lassen sich allfällige Massnahmen ableiten.

Mit Kennzahlen kann der Sicherheitsstand einer Organisation gemessen werden. Zu diesem Zweck stimmen ICT Security Experts regelmässig die Kennzahlen mit den Stakeholdern ab.

Der Handlungskompetenzbereich B baut auf HKB A - Verankern der Sicherheitsstrategie auf.

B) Etablieren des Informationssicherheits-Managementsystems (ISMS) (Übersicht)

Berufliche Handlungskompetenzen	**Wichtige Themen / Inhalte**	**Leistungskriterien**
B1 – ISMS führen	ISO 27001 Methodik	ICT Security Experts sind fähig: - ein ISMS zu erstellen. Dazu gehört, den Umfang des ISMS zu definieren, eine Risikoanalyse durchzuführen, einen Risikobehandlungsplan zu erstellen, ein Kontrollsystem der Massnahmen zu definieren sowie Sicherheitsmassnahmen und Prozesse zu implementieren - ein ISMS zu steuern, zu kontrollieren und aufrechtzuerhalten, die Wirksamkeit der Massnahmen und Prozesse zu überprüfen und wenn nötig anzupassen - die kontinuierliche Verbesserung des ISMS sicherzustellen - strategische ICT-Risiken zu kennen und zu detaillieren - Prozesse zu definieren und einzuführen - Stakeholder für die Umsetzung der Prozesse zu schulen - Kennzahlen zu überwachen und bei Abweichungen von Zielwerten zu reagieren - Reviews zur Prozessverbesserung durchzuführen, aus den Ergebnissen Massnahmen abzuleiten und umzusetzen - sich laufend über sicherheitsrelevante Themen wie neue Technologien, Angriffsszenarien und Mitbewerber zu informieren und neue Erkenntnisse in interne Regelwerke und ins Risikomanagement einfliessen zu lassen - Sicherheitsanforderungen an Prozesse zu definieren, mit dem Prozess-Verantwortlichen abzustimmen und zu finalisieren - Sicherheitsvorgaben zu definieren, in Vorgabedokumente wie Weisungen und Prozessdokumentation einzuarbeiten und die Kontrolle zu definieren - aufgrund der Risikoanfälligkeit Applikationen, Systeme und Vorhaben zu bestimmen, die geprüft werden sollen - Schwachstellen zu kategorisieren und zur Korrektur zu adressieren - Sicherheitsüberprüfung im Outsourcing-Bewilligungsprozess zu integrieren und durchzuführen - Service Level Reports und Auditbericht über Drittlieferanten zu beurteilen und daraus Massnahmen abzuleiten - Sicherheitslevels pro Personeneinsatzgebiet zu definieren - Überprüfungsart oder Methodik pro Anforderung und Level zu definieren - ein Personensicherheitsüberprüfungs-Dokument und den entsprechenden Prozess zu erstellen - HR-Mitarbeitende für die Umsetzung des PSÜ-Prozesses zu schulen
B2 – Prozesse etablieren		
B3 – Risiken managen		
B4 – Informationssicherheitsanforderungen in allen Prozessen integrieren		
B5 – Sicherheitsvorgaben definieren	Industrielle Informatik Robotics IoT AI Cloud	
B6 – Sicherheits-überprüfung sicherstellen	ISO 27002 IT-Grundschutz Penetrationstest Codereview	
B7 – Security im Outsourcing überwachen		
B8 –Performance messen		
B9 – Informations-spezifische Anforderungen an Personensicherheitsüberprüfung definieren		

C) Führen des Sicherheitsprogramms

Beschreibung des Handlungskompetenzbereichs:
ICT Security Experts erstellen eine organisationsweite IT-Sicherheitsarchitektur. Sie identifizieren die Abweichungen zwischen der Ist- und Sollarchitektur und leiten daraus die technischen Anforderungen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen ab.

Sie planen und konzipieren das Security Produkte-/Service-Portfolio und entwickeln es weiter. Projekte im Bereich Informationssicherheit werden aus der Informationssicherheitsstrategie abgeleitet. Für geplante Neuanschaffungen von Produkten / Services erbringen sie einen Wirtschaftlichkeitsnachweis
Sie leiten Projekte im Bereich Information Security, beobachten den Markt und evaluieren neue Produkte und Prozesse.

Kontext:
Die Informationssicherheitsarchitektur bildet die Sicherheitsziele der Unternehmung ab und dient als Basis für die Projektorganisation. Für die Erstellung verwenden ICT Security Experts ein Architekturmodell in Abstimmung mit den verschiedenen Stakeholdern.

Das Produkt- und Serviceportfolio ist ständig weiterzuentwickeln. Für das Security-Programm der Organisation bedeutet dies, das Portfolio stets auf die Geschäftsprozesse abzustimmen. Die ICT Security Experts sorgen dabei für Transparenz über die Investitionen in ihrem Bereich.

Der Handlungskompetenzbereich C baut auf
dem Handlungsbereich A – Verankern der Sicherheitsstrategie auf.

C) Führen des Sicherheitsprogramms (Übersicht)

Berufliche Handlungskompetenzen	**Wichtige Themen / Inhalte**	**Leistungskriterien**
C1 – ICT Security-Architektur erarbeiten	Architekturmodelle	ICT Security Experts sind fähig: - die Ist-Situation von IT-System- und Applikationslandschaft zu analysieren und Gefährdungssituation zu bewerten, - Anforderungen an ein technisches Sollmodell der IT-System- und Applikationslandschaft zu skizzieren - eine Abweichungsanalyse zwischen Ist und Soll zu erstellen und mit den entsprechenden Stakeholdern abzustimmen - aus Abweichungen die technischen Anforderungen der Schutzmassnahmen zu definieren - mit den Stakeholdern abgestimmte technische Schutzlösungen abzuleiten - Neuanforderungen an Produkte und Services zu beurteilen - Projekte aufgrund von transparenten Kriterien zu priorisieren - ein Information Security-Budget mitzugestalten - Risiken von Neuanschaffungen abzuschätzen - Projekte im Bereich Information Security zu planen, durchzuführen und Produkte zu evaluieren
C2 – Produkt- / Service-Portfolio managen		
C3 – Portfolio-management Security-Programm erstellen		
C4 – Business Case entwickeln		
C5 – Informationssicherheitslösungen evaluieren		
C6 – Umsetzung der beschlossenen Massnahmen sicherstellen		
C7 – Projekte leiten	Projektmethodik Projektmanagement-Software	
C8 – Innovationen in die Informations-sicherheit integrieren	Research Portale (z.B. Gartner) Konferenzen für Informationssicherheit Ethik	

D) Managen von Stakeholdern

Beschreibung des Handlungskompetenzbereichs:
ICT Security Experts pflegen zum Austausch über informationssicherheitsrelevante Themen ein tragfähiges und zuverlässiges Beziehungsnetzwerk im Bereich Informationssicherheit.

In der Organisation beantworten sie zielgruppengerecht sicherheitsrelevante Fragen. Sie beraten bei Projekten, analysieren und bewerten diese bezüglich Informationssicherheitsrisiken. Sie leiten die Sicherheitsanforderungen an ein Produkt aus den Geschäftsanforderungen ab. Gleichzeitig legen sie die minimale Integration eines Produktes in die bestehende Sicherheitsarchitektur für den Proof of concept (PoC) fest. Sie erstellen den Security-Prüfplan und arbeiten bei der Prüfung für den PoC mit. Den Sign-off definieren sie und führen ihn durch.

Zum Stakeholder Management gehört auch, dass sie sicherheitsrelevante Tätigkeiten auf die Einhaltung der Compliance kontrollieren. Die Ergebnisse dokumentieren und rapportieren sie der Compliance Organisation.

Kontext:
Nur eine Verankerung der Informationssicherheit in der gesamten Organisation schützt optimal vor Sicherheitsereignissen. Dies bedingt ICT Security Experts, die sicherheitsrelevanten Fragen kompetent und nachvollziehbar beantworten können.

Gleichzeitig müssen im ganzen Unternehmen neue Produkte und Prozesse auf die Einhaltung der Informationssicherheit überprüft werden. Der Integration eines neuen Produktes in die bestehende Sicherheitsarchitektur kommt eine zentrale Rolle zu. Die ICT Security Experts integrieren die Produkte in die bestehende Sicherheitsarchitektur.

Der Austausch mit anderen Fachleuten im Bereich Informationssicherheit erlaubt es, Wissen und Erfahrungen auszutauschen. ICT Security Experts wissen um die Bedeutung dieses Netzwerkes, bauen es auf und pflegen es.

Der Handlungskompetenzbereich D steht in Bezug zu den Handlungskompetenzbereichen A - Verankern der Sicherheitsstrategie, B - Etablieren des Informationssicherheits-Managementsystems (ISMS) und C - Führen des Sicherheitsprogramms.

D) Managen von Stakeholdern (Übersicht)

Berufliche Handlungskompetenzen	**Wichtige Themen / Inhalte**	**Leistungskriterien**
D1 – Tragfähiges Netzwerk unterhalten		ICT Security Experts sind fähig: - ein Beziehungsnetzwerk im Bereich Informationssicherheit aufzubauen und zu pflegen - mit externen Informationssicherheitsorganisationen zusammenzuarbeiten - Fragestellungen von Stakeholder zu erfassen und zielgruppengerecht zu beantworten - Auditresultate bezüglich Compliance zu dokumentieren und zu rapportieren - bei Projekten aus anderen Bereichen bezüglich Informationssicherheit zu beraten - Projekte aus anderen Bereichen bezüglich Informationssicherheit zu analysieren, zu bewerten und die Ergebnisse zu kommunizieren - den Security-Sign-off in Projekten aus anderen Bereichen zu definieren und vorzunehmen - Sicherheitsanforderungen an ein Produkt aus den funktionalen Geschäftsanforderungen abzuleiten - eine minimale Integration eines Produktes in die bestehende Sicherheitsarchitektur für den Proof of concept (PoC) festzulegen. - bei der Erstellung des Security-Prüfplans und bei der und beim PoC mitarbeiten und den Testbericht reviewen. - Leistungsverträge bezüglich Informationssicherheit mit Kunden und Lieferanten zu vereinbaren und zu überprüfen
D2 – Stakeholder fachlich beraten	Governance und Prozesse im Unternehmen ISO 2700x	
D3 – Einhaltung der Informationssicherheitsvorschriften einfordern	Gesetze Regulatorien interne Vorgaben/Prozesse AKV-Prinzip	
D4 – Projekte begleiten	IoT AI Robotics Industrial Control Systems	
D5 – Sicherheitsaspekte in Proofs of Concept festlegen	Service Level Agreement	

E) Schaffen von Awareness

Beschreibung des Handlungskompetenzbereichs:
ICT Security Experts sensibilisieren die Mitarbeitenden, die Geschäftsleitung und den Verwaltungsrat für ICT-Sicherheitsaspekte. Sie planen interne Sensibilisierungskampagnen, stimmen diese mit bestehenden Programmen ab und werten sie aus. Die Zielgruppen bestimmen die Inhalte und Kommunikationskanäle. Die ICT Security Experts formulieren die Inhalte und bereiten diese didaktisch auf. Sie überprüfen die Teilnahme der Mitarbeitenden an Schulungen. Sie werten die Schulungen aus und informieren den Auftraggeber über das Ergebnis der Schulung.

Intern und extern informieren sie über Sicherheitsaspekte mit Medien wie Newsletter und Onlinepublikationen.

Kontext:
Das Schaffen von Awareness stellt eine zentrale Aufgabe von ICT Security Experts dar.
Eine Schlüsselrolle kommt der Sensibilisierung der Geschäftsleitung und des Verwaltungsrates zu, denn sie entscheiden, welche Risiken die Sicherheitsstrategie umfasst und auf welches Niveau sie gebracht werden sollen. Mit Mitarbeitenden Sensibilisierung gelingen die Etablierung des Informationssicherheits-Managementsystems (ISMS) und das Führen des Sicherheitsprogramms.

Sensibilisierung muss bei allen Mitarbeitenden geschaffen werden. Dieser Prozess ist nie abgeschlossen und bedarf stets neuer kommunikativer Anstrengungen. Die Sensibilisierung darf sich nicht nur im Wissen niederschlagen, sondern die Mitarbeitenden müssen sie auch im Arbeitsalltag umsetzen.

Der Handlungskompetenzbereich E steht in Bezug zu den Handlungskompetenzbereichen A - Verankern der Sicherheitsstrategie, B - Etablieren des Informationssicherheits-Managementsystems (ISMS) und C - Führen des Sicherheitsprogramms. In all diesen Handlungskompetenzbereichen spielt Sensibilisierung eine zentrale Rolle.

E) Schaffen von Awareness (Übersicht)

Berufliche Handlungskompetenzen	**Wichtige Themen / Inhalte**	**Leistungskriterien**
E1 – Awareness-kampagne durchführen	Didaktik Kommunikation	ICT Security Experts sind fähig: - Sensibilisierungskampagnen und Sicherheitskommunikation mit dem Auftraggeber zu definieren - Sensibilisierungskampagnen mit einem vorhandenen Sensibilisierungsprogramm abzustimmen - Themen, Zielpublikum, Zeitraum, Hilfsmittel, Messgrösse und Kommunikationskanal festzulegen - für Sensibilisierungskampagnen die Inhalte zu didaktisieren und entsprechend dem gewählten Kommunikationskanal zielgruppengerecht aufzubereiten - Schulungen bei den Zielgruppen zu planen und durchzuführen - Ergebnisse von Schulungen auszuwerten und dem Auftraggeber zu rapportieren - aus Bewertungen von Schulungen Verbesserungen für die Sensibilisierungsausbildung zu erkennen
E2 – Sicherheitskommunikation intern und extern sicherstellen	Kommunikation mit Medien	

F) Bewältigen von Ereignissen

Beschreibung des Handlungskompetenzbereichs:
ICT Security Experts analysieren die allgemeine Sicherheitslage mit Fokus auf die eigene Organisation.
Im Falle eines Sicherheitsereignisses ermitteln, analysieren und dokumentieren sie die Auswirkung auf die Organisation. Sie leiten Massnahmen ein, um die Auswirkungen zu reduzieren. Sie informieren die Stakeholder und Geschäftsprozessverantwortlichen über die entsprechenden Konsequenzen.

Sie beraten und unterstützen den Krisenstab zur Bewältigung des Sicherheitsereignisses bei der Entscheidungsfindung. Nach Abschluss des Sicherheitsereignisses evaluieren sie die Bewältigung und beurteilen den entstandenen Schaden. Sie identifizieren Optimierungsmöglichkeiten in der Sicherheitsorganisation, den Sicherheitsprozessen oder der Sicherheitsarchitektur.
Sie setzen diese Optimierungsmöglichkeiten in Kooperation mit den entsprechenden Personen um.

Weiter stellen sie die Integration von Sicherheitsaspekten im Business Continuity Management (BCM) sicher.

Kontext:
Die Effizienz bei der Bewältigung eines Sicherheitsereignisses entscheidet über das Schadensausmass. Sämtliche Massnahmen sind zu koordinieren. Die ICT Security Experts haben dabei die Funktion der Koordinations- und Ansprechstelle für Geschäftsleitung, Verwaltungsrat und die Mitarbeitenden.

Der Handlungskompetenzbereich F steht in Bezug zu allen anderen Handlungskompetenzbereichen, denn die Bewältigung eines Sicherheitsereignisses baut auf den anderen Handlungskompetenzbereichen auf.

F) Bewältigen von Ereignissen (Übersicht)

Berufliche Handlungskompetenzen	**Wichtige Themen / Inhalte**	**Leistungskriterien**
F1 – Business Impact Analyse sicherstellen		ICT Security Experts sind fähig: - Bestandsaufnahmen über Bedrohungen von wichtigen Prozessen, Produkten, Infrastrukturen usw. zu erstellen und zu unterhalten (BIA) - Schwachstellen in wichtigen Prozessen, Produkten und Infrastrukturen zu erkennen - Abhängigkeiten von Risiken auf der Basis einer BIA zu beurteilen - Handlungsbedarf für die Sicherheitsorganisation abzuleiten - die allgemeine Sicherheitslage mit Fokus auf das Gefahrenpotenzial für die eigene Organisation zu analysieren und Sofortmassnahmen zu erarbeiten - die Auswirkung eines Ausfalls von Informationsdiensten zu ermitteln und zu analysieren und zu dokumentieren - Massnahmen aus der Auswirkung (Schaden) abzuleiten und zu priorisieren - Stakeholder und Geschäftsprozessverantwortliche über die relevanten Abhängigkeiten im Geschäftsprozess zu informieren - den Krisenstab zu beraten und in der Entscheidungsfindung zu unterstützen - die Lösung eines Sicherheitsereignisses festzulegen und den entstandenen Schaden zu beurteilen - Optimierung für weitere mögliche Sicherheitsereignisse zu identifizieren und Verbesserungen in der Sicherheitsorganisation, Sicherheitsprozessen und/oder in der Sicherheitsarchitektur vorzunehmen - zu überprüfen, ob die Sicherheitsaspekte im BCM berücksichtigt sind
F2 – Notfallorganisation für Sicherheitsereignisse sicherstellen	Sicherheitsanbieter, Sicherheitsblogs und Sicherheitsbehörden, z.B. MELANI	
F3 – Sicherheitsereignisse managen	Kriminalistik / Jus Forensik Zusammenarbeit mit Ermittlungen und Strafverfolgung	
F4 – Integrieren von Informatiksicherheitsaspekten im Business Continuity Management sicherstellen	BCM-Prozesse ISO2700x	

G) Sichern von Informationen

Beschreibung des Handlungskompetenzbereichs:
Der ICT Security Expert definiert das Regelwerk zur Datenklassifizierung in Absprache mit den Dateneignern. Er erstellt auf dieser Basis das Datenmanagementkonzept. In diesem Konzept werden die Aspekte Datenübertragung, Datenspeicherung und Datenzugriffe definiert. Dabei werden die rechtlichen Grundlagen hinsichtlich Datenschutz und die branchenspezifischen, regulatorischen Vorgaben berücksichtigt.

Kontext:
Als Folge der zunehmenden Vernetzung von IT-Systemen und der sich verändernden Wertschöpfungsketten ist die Daten- und Informationsmenge nahezu unbegrenzt. Diese Daten und Informationen fallen lokal, dezentral und in Cloudlösungen von Dritten an und werden dort gespeichert.

Für eine Organisation sind sowohl intern als auch extern generierte Daten und Informationen von Bedeutung. Dies führt zu Schnittstellen, die einer technischen Lösung (Übertragung, Speicherung) bedürfen. Weiter müssen die Daten bezüglich der Kriterien Verfügbarkeit, Echtheit, Verbindlichkeit und Vertraulichkeit klassifiziert werden. Dabei gilt es, die rechtlichen Grundlagen der involvierten Länder zu befolgen.

Der Handlungskompetenzbereich G fliesst in alle anderen Handlungskompetenzbereiche ein, im speziellen in den Handlungskompetenzbereich B.

G) Sichern von Informationen (Übersicht)

Berufliche Handlungskompetenzen	**Wichtige Themen / Inhalte**	**Leistungskriterien**
G1 – Klassifizierung von Informationen sicherstellen		ICT Security Experts sind fähig: - Vorgaben für das Datenmanagement zu formulieren - die rechtlichen Grundlagen bei der Verwaltung von Daten und Informationen sicherzustellen - ein Datenmanagementkonzept auf die Kriterien Verfügbarkeit, Echtheit, Verbindlichkeit und Vertraulichkeit von Daten und Informationen zu prüfen - ein Klassifizierungskonzept zu erstellen - das Einhalten der Vorgaben für das Datamanagement sicherzustellen - Verschlüsselungstechnik und deren Anwendung situativ anzuordnen - Speicherung, Archivierungstechnologien und Kassation auf ihre Sicherheitsaspekte zu überprüfen
G2 – Datensicherheit bei der Übertragung sicherstellen	Datenschutzbestimmungen Verschlüsselung	
G3 - Datensicherheit bei der Speicherung und Archivierung sicherstellen		

– Haltungen

Haltungen	Leistungskriterium	A	B	C	D	E	F	G
Selbständigkeit	HKB A und B alle Leistungskriterien HKB D: - Auditresultate bezüglich Compliance zu dokumentieren und zu rapportieren - Projekte aus anderen Bereichen bezüglich Informationssicherheit analysieren, bewerten und die Ergebnisse kommunizieren	x	x		x			
Kommunikationsfähigkeit	HKB A: - adressatengerecht präsentieren - eine Informationsstrategie auf der Basis des Risikoappetits der Geschäftsleitung und des Verwaltungsrates erarbeiten - den Reifegrad der Sicherheit in der Organisation zu ermitteln - den Inhalt von Security-Publikationen an ihr Team weiterzugeben - unterstellte Mitarbeitende fachlich zu unterstützen - eine Community von Informationssicherheitsspezialisten etablieren und den konstanten Erfahrungs- und Wissensaustausch gewährleisten HKB B: - Prozesse definieren und einführen - Sicherheitsanforderungen an Prozesse definieren, mit dem Prozessverantwortlichen abstimmen und finalisieren HKB C: - aus Abweichungen die technischen Anforderungen der Schutzmassnahmen zu definieren - mit den Stakeholdern abgestimmte technische Schutzlösungen abzuleiten HKB D: - ein Beziehungsnetzwerk im Bereich Informationssicherheit aufbauen und pflegen	x	x	x	x	x	x	

Haltungen	Leistungskriterium	A	B	C	D	E	F	G
	- bei Projekten aus anderen Bereichen bezüglich Informationssicherheit beraten HKB E: - für Sensibilisierungskampagnen die Inhalte didaktisieren und entsprechend dem gewählten Kommunikationskanal zielgruppengerecht aufbereiten - Schulungen bei den Zielgruppen planen und durchführen HKB F: - die Auswirkungen eines Ausfalls von Informationsdiensten ermitteln und analysieren - Stakeholder und Geschäftsprozessverantwortliche über die relevanten Abhängigkeiten im Geschäftsprozess informieren - den Krisenstab beraten und in der Entscheidungsfindung unterstützen							
Loyalität	HKB A und B alle Leistungskriterien	x	x					
Urteilsvermögen	HKB A: - die Bedrohungsszenarien mit Relevanz für die Organisation definieren - die Risiken analysieren HKB B alle Leistungskriterien HKB C: - Projekte im Bereich Information Security planen, durchführen und evaluieren HKB D: - Fragestellungen von Stakeholdern erfassen und zielgruppengerecht beantworten	x	x	x	x		x	

Haltungen	Leistungskriterium	A	B	C	D	E	F	G
	- Sicherheitsanforderungen an ein Produkt aus den funktionalen Business-Anforderungen ableiten HKB F: - die allgemeine Sicherheitslage mit Fokus auf das Gefahrenpotenzial für die eigene Organisation analysieren und Sofortmassnahmen erarbeiten - die Auswirkung eines Ausfalls von Informationsdiensten ermitteln und analysieren - die Lösung eines Sicherheitsereignisses festlegen und den entstandenen Schaden beurteilen - überprüfen, ob die Sicherheitsaspekte im BCM berücksichtigt sind - Massnahmen aus der Auswirkung eines Ereignisses ableiten und priorisieren							
Zukunftsorientierte Denkweise	HKB A: - den eigenen Weiterbildungsbedarf und jenen des Teams erkennen und Massnahmen umsetzen HKB B: - sich laufend über sicherheitsrelevante Themen wie neue Technologien, Angriffsszenarien und Mitbewerber informieren und neue Erkenntnisse in interne Regelwerke und ins Risikomanagement einfliessen lassen HKB C: - Anforderungen an ein technisches Sollmodell in den Bereichen IT-System- und Applikationslandschaft skizzieren HKB G: - Verschlüsselungstechnik und deren Anwendung situativ anordnen - Speicherung, Archivierungstechnologien und Kassation auf ihre Sicherheitsaspekte überprüfen	x	x	x				x

Haltungen	Leistungskriterium	A	B	C	D	E	F	G
Durchsetzungsvermögen	HKB A und B alle Leistungskriterien HKB E: - Themen, Zielpublikum, Zeitraum, Hilfsmittel, Messgrösse und Kommunikationskanal festlegen HKB F: - Massnahmen aus der Auswirkung eines Ereignisses ableiten und priorisieren - Stakeholder und Geschäftsprozessverantwortliche über die relevanten Abhängigkeiten im Geschäftsprozess informieren.	x	x			x	x	
Integrität	HKB A und B alle Leistungskriterien HKB D: - Leistungsverträge bezüglich Informationssicherheit mit Kunden und Lieferanten zu vereinbaren und zu überprüfen HKB G: - Speicherung, Archivierungstechnologien und Kassation auf ihre Sicherheitsaspekte überprüfen - ein Klassifizierungskonzept erstellen	x	x		x			x
Innovationsfähigkeit	HKB A: - den eigenen Weiterbildungsbedarf und jenen des Teams erkennen und Massnahmen umsetzen HKB B: - sich laufend über sicherheitsrelevante Themen wie neue Technologien, Angriffsszenarien und Mitbewerber informieren und neue Erkenntnisse in interne Regelwerke und ins Risikomanagement einfliessen lassen	x	x					

Haltungen	**Leistungskriterium**	**A**	**B**	**C**	**D**	**E**	**F**	**G**
Teamfähigkeit	HKB A und B alle Leistungskriterien HKB C: - Projekte im Bereich Information Security planen, durchführen und evaluieren HKB D: - ein Beziehungsnetzwerk im Bereich Informationssicherheit aufbauen und pflegen HKB F: - den Krisenstab beraten und in der Entscheidungsfindung unterstützen	x	x	x	x		x	
Vernetztes Denken	HKB A und B alle Leistungskriterien HKB C: - die Ist-Situation von IT System- und Applikationslandschaft analysieren und die Implikationen auf innere und äussere Bedrohungen feststellen - Anforderungen an ein technisches Sollmodell in den Bereichen IT-System- und Applikationslandschaft skizzieren HKB D: - eine minimale Integration eines Produktes in die bestehende Sicherheitsarchitektur für den Proof of concept (PoC) festlegen - bei der Erstellung des Security-Prüfplans und beim PoC mitarbeiten und den Testbericht reviewen	x	x	x	x			

Haltungen	Leistungskriterium	A	B	C	D	E	F	G
Systemisches Denken	HKB B: - ein ISMS zu erstellen. Dazu gehört, den Umfang des ISMS zu definieren, eine Risikoanalyse durchzuführen, einen Risikobehandlungsplan zu erstellen, ein Kontrollsystem der Massnahmen zu definieren sowie Sicherheitsmassnahmen und Prozesse zu implementieren - ein ISMS zu steuern, zu kontrollieren und aufrechtzuerhalten, die Wirksamkeit der Massnahmen und Prozesse zu überprüfen und wenn nötig anzupassen - die kontinuierliche Verbesserung des ISMS sicherzustellen - sich laufend über sicherheitsrelevante Themen wie neue Technologien, Angriffsszenarien und Mitbewerber informieren und neue Erkenntnisse in interne Regelwerke und ins Risikomanagement einfliessen lassen HKB C: - die Ist-Situation von IT System- und Applikationslandschaft analysieren und die Implikationen auf innere und äussere Bedrohungen feststellen HKB F: - die allgemeine Sicherheitslage mit Fokus auf das Gefahrenpotenzial für die eigene Organisation analysieren und Sofortmassnahmen erarbeiten - die Auswirkung eines Ausfalls von Informationsdiensten ermitteln und analysieren - die Lösung eines Sicherheitsereignisses festlegen und den entstandenen Schaden beurteilen - überprüfen, ob die Sicherheitsaspekte im BCM berücksichtigt sind - Massnahmen aus der Auswirkung eines Ereignisses ableiten und priorisieren HKB G: - ein Klassifizierungskonzept erstellen - Vorgaben für das Datenmanagement formulieren		x	x			x	x

Haltungen	**Leistungskriterium**	**A**	**B**	**C**	**D**	**E**	**F**	**G**
Lernfähigkeit	HKB A und B alle Leistungskriterien	x	x					
Verantwortungsbewusstsein	HKB A und B alle Leistungskriterien HKB C: - die Ist-Situation von IT System- und Applikationslandschaft analysieren und Implikationen auf die inneren und äusseren Bedrohungen feststellen, - Anforderungen an ein technisches Sollmodell in den Bereichen IT System- und Applikationslandschaft skizzieren - Projekte im Bereich Information Security planen, durchführen und evaluieren - eine Abweichungsanalyse zwischen Ist und Soll zu erstellen und mit den entsprechenden Stakeholdern abzustimmen - aus Abweichungen die technischen Anforderungen der Schutzmassnahmen zu definieren HKB F: - die allgemeine Sicherheitslage mit Fokus auf das Gefahrenpotenzial für die eigene Organisation etablieren - Massnahmen aus der Auswirkung eines Ereignisses ableiten und priorisieren HKB G: - ein Klassifizierungskonzept erstellen - Speicherung, Archivierungstechnologien und Kassation auf ihre Sicherheitsaspekte überprüfen	x	x	x			x	x