Information Security Manager mit eidg. Diplom

Berufsbegleitender Lehrgang
digicomp.ch/d/ICTSED

What’s in it?

120723

Weshalb ein eidgenössisches Diplom für Information Security Managers?

Der Schutz vor Cyberattacken auf Firmen- und Verwaltungsnetze ist ein entscheidender Erfolgsfaktor für Unternehmen und Verwaltungen. Dabei ist es nicht einfach, geeignetes Fachpersonal für die Aufgaben im Bereich ICT Security zu finden. ICT-Berufsbildung Schweiz hat deshalb das Projekt «Information Security Manager» initiiert und schafft damit in Zusammenarbeit mit dem Informatiksteuerungsorgan des Bundes (ISB) und Wirtschaftsvertretern einen hochpositionierten und anerkannten Diplom-Abschluss für Personen, die mit dem Management der Informatiksicherheit befasst sind.

Digicomp ist Bildungspartner von ICT-Berufsbildung Schweiz
Als Bildungspartner von ICT-Berufsbildung Schweiz, stellt Digicomp eine Prüfungsvorbereitung für die Teilnehmenden zur Verfügung, die die eidgenössische Diplomprüfung «Information Security Manager» absolvieren möchten.

Arbeitsgebiet eines Information Security Manageren
Information Security Managers arbeiten für private Unternehmen und öffentliche Institutionen im Bereich der Informationssicherheit. Entsprechend gross ist die Bandbreite der organisatorischen Zuordnungen. Unabhängig von der Organisationsgrösse deckt ihre Tätigkeit den Gesamtkontext der Informationssicherheit in der Organisation ab. Dank ihrem vertieften Verständnis der Tätigkeitsbereiche und Prozesse der Organisation arbeiten sie in sicherheitsrelevanten Bereichen mit den verschiedensten Stakeholdern zusammen. Zu ihnen gehören Geschäftsleitung und Verwaltungsrat, Fachexperten, Fachbereichs- und Prozessverantwortliche und externe Dienstleister. Information Security Managers reduzieren das Informationssicherheitsrisiko der Organisation auf das Niveau, das die Geschäftsleitung und Verwaltungsrat vorgibt. Sie erkennen allfällige Lücken in der Sicherheitsstrategie und erarbeiten Massnahmen, mit denen diese Lücken geschlossen werden können. Sie beraten den Krisenstab der Organisation in allen Belangen der ICT-Sicherheit. Sie schaffen auf allen Stufen ein Sicherheitsbewusstsein, indem sie adäquate Sensibilisierungskampagnen erarbeiten und durchführen.

Mehrwert eines Information Security Manager
Der Information Security Manager trägt dazu bei, dass Informationen besser vor unerlaubten Zugriffen geschützt werden. Insbesondere der Informations- und Kommunikationstechnologie kommt in allen Lebensbereichen eine wachsende Bedeutung zu. Damit steigt auch die Verwundbarkeit von Wirtschaft und Gesellschaft. Sie tragen dazu bei, die Gesellschaft für das Thema zu sensibilisieren.

ICT-Sicherheit ist ein Standortfaktor für die Schweiz und stärkt das Image der Schweiz als verlässliches Land. Information Security Managers leisten einen wichtigen Beitrag dazu.

Bildungspartner ICT Berufsbildung Schweiz

Handlungskompetenzfelder eines Information Security Manager im Überblick

Veranken der Sicherheits-strategie	A1: Informations-sicherheitsgrund-lagen erarbeiten	A2: Informations-sicherheit in der Geschäfts-leitung und im Verwaltungsrat verankern	A3: Führung und Steuerung der Informations-sicherheit managen	A4: Sicherheits-organisation etablieren	A5: Informations-sicherheitsspe-zialisten fachlich führen
Etablieren des Informationssi-cherheits-Management-systems (ISMS)	B1: ISMS führen	B2: Prozesse etablieren	B3: Risiken managen	B4: Informations-sicherheitsan-forderungen in allen Prozessen integrieren	B5: Sicherheits-vorgaben defi-nieren
	B6: Sicherheits-überprüfung sicherstellen	B7: Security im Outsourcing überwachen	B8: Performance messen	B9: Informa-tionsspezifische Anfoderungen an Personensicher-heitsüberprüfung definieren	
Führen des Sicherheits-programms	C1: ICT-Security-Architektur er-arbeiten	C2: Produkt-/ ServicePortfolio managen	C3: Portfolio-management-Security-Programm erstellen	C4: Business Case entwickeln	C5: Informations-sicherheitslösun-gen evaluieren
	C6: Umsetzung der beschlosse-nen Massnah-men sicherstellen	C7: Projekte leiten	C8: Innovationen in die Informa-tionssicherheit integrieren		
Managen von Stakeholdern	D1: Tragfähiges trusted Netzwerk unterhalten	D2: Stakeholder fachlich beraten	D3: Informations-sicherheitscom-pliance einfor-dern	D4: Projekte begleiten	D5: Sicherheits-aspekte in Proofs of Concept sicherstellen
Schaffen von Awareness	E1: Awareness-kampagne durchführen	E2: Sicherheits-kommunikation intern und extern sicherstellen			
Bewältigen von Ereignissen	F1: Business-Impact-Analyse sicherstellen	F2: Notfallor-ganisation für Security Incidents sicherstellen	F3: Security Inci-dent managen	F4: Integration von Informatiksicherheits-aspekten im Business Continuity Manage-ment sicherstellen	
Sichern von Informationen	G1: Klassifizie-rung von Infor-mationen sicher-stellen	G2: Datensicher-heit bei der Übertragung sicherstellen	G3: Datensicher-heit bei der Speicherung und Archivierung sicherstellen		

Information Security Manager mit eidg. Diplom
Buchungsmöglichkeiten

Digicomp bietet folgende zwei Weiterbildungsformate an:

Variante 1: Kompakt-Vorbereitung
Das Kurspaket des Kompaktlehrgangs (siehe Seite 8), deckt die wichtigsten Handlungskompetenzen des Information Security Manager ab. Mit der 4-tägigen Prüfungsvorbereitung stellen wir sicher, dass Sie zielgerichtet auf die eidgenössische Diplomprüfung vorbereitet werden.

Variante 2: Individueller Weg
Als Alternative bieten wir Ihnen ein breites, modulares Kursportfolio an, aus dem Sie sich die individuell benötigten Kompetenzen zusammenstellen können. Die Handlungskompetenzen mit den dazu passenden Modulen, die Sie sich individuell zusammenstellen können, finden Sie in dieser Broschüre ab Seite 10. So bereiten Sie sich entsprechend Ihrer bestehenden Kompetenzen gezielt auf die eidg. Diplomprüfung zum Information Security Manager vor.

Zielgruppen
Der Information Security Manager richtet sich an leitende Mitarbeitende privater Unternehmen und öffentlicher Institutionen, die für das Management der Informationssicherheit verantwortlich sind und sich vorbereiten wollen auf den Abschluss zum Information Security Manager mit eidgenössischem Diplom.

Nutzen & Lernziele
- ★ Verankerung der Sicherheitsstrategie in Ihrem Unternehmen
- ★ Etablieren eines Informationssicherheitsmanagementsystems
- ★ Führen eines Sicherheitsprogramms in Ihrem Unternehmen
- ★ Managen von Stakeholdern
- ★ Schärfen des Sicherheitsbewusstseins in Ihrem Unternehmen
- ★ Bewältigen von Ereignissen und Sichern von Informationen
- ★ Erkennen und Bewerten von Risiken
- ★ Definieren und Koordinieren von Schutzmassnahmen
- ★ Sicherstellung der Wirksamkeit von Abwehrmassnahmen
- ★ Kennen und Verstehen der neuen Anforderungen des nDSG

Um diese Tätigkeiten professionell ausführen zu können, sind Sie mit Ihrer Organisation und deren Produkte, Prozesse und Informationen vertraut und in der Lage, eine angemessene Informationssicherheit zu gewährleisten. Sie erkennen und bewerten die Risiken, definieren und koordinieren Schutzmassnahmen und stellen die Wirksamkeit der Abwehrmassnahmen sicher.

Diplomträger
Der Verein ICT-Berufsbildung Schweiz hat die Trägerschaft inne. Digicomp verantwortet die vorbereitenden Trainings.

Voraussetzung für die Zulassung zur Prüfung

Zur Prüfung Information Security Manager mit eidgenössischem Diplom wird zugelassen, wer:

- ★ einen Tertiärabschluss im Informatikbereich (eidg. Fachausweis; eidg. Diplom; Diplom HF; Bachelor; Master) oder eine gleichwertige Qualifikation besitzt und über mindestens drei Jahre Berufspraxis im Bereich der ICT-Sicherheit verfügt

oder

- ★ einen Tertiärabschluss in einem anderen Bereich (eidg. Fachausweis; eidg. Diplom; Diplom HF; Bachelor; Master) oder eine gleichwertige Qualifikation besitzt und über mindestens vier Jahre Berufspraxis im Bereich der ICT-Sicherheit verfügt

oder

- ★ einen Abschluss der Sekundarstufe II im Informatikbereich oder eine gleichwertige Qualifikation besitzt und über mindestens sechs Jahre Berufspraxis im Bereich der ICT-Sicherheit verfügt

oder

- ★ einen Abschluss der Sekundarstufe II in einem anderen Bereich (eidg. Fähigkeitszeugnis; gymnasiale Maturität; Fachmittelschulausweis; Fachmaturität) oder eine gleichwertige Qualifikation besitzt und über mindestens acht Jahre Berufspraxis im Bereich der ICT-Sicherheit verfügt

und

- ★ einen aktuellen Nachweis erbringt, dass kein mit der Berufstätigkeit unvereinbarer Eintrag im Zentralstrafregister vorliegt

Bitte beachten Sie, dass sich die Berufserfahrung auf die von ICT Berufsbildung definierten Handlungskompetenzen bezieht: Sie müssen entsprechend Berufserfahrung, basierend auf Management-Kompetenzen vorweisen können, keine technischen Kompetenzen.

Zwingend: Klären Sie VOR Ihrer Kursanmeldung ab, ob Sie zur eidgenössischen Prüfung zugelassen sind. Andernfalls riskieren Sie, dass erst nach Besusch der Prüfungsvorbereitung, bei Anmeldung zur Diplomprüfung, Ihre Zulassung abgelehnt wird. Damit eine verbindliche Aussage über Ihre Prüfungszulassung gemacht werden kann, benötigt ICT-Berufsbildung folgende Dokumente:

- ★ Vorabklärung Prüfungszulassung Information Security Manager
- ★ Lebenslauf
- ★ Arbeitszeugnisse, in denen die geforderte Berufspraxis ersichtlich ist (von der aktuellen Stelle genügt eine Stellenbeschreibung mit der Bestätigung, dass Sie in dieser Funktion arbeiten)
- ★ Zeugnis/Diplom des höchsten Abschlusses

Für den Besuch der Prüfungsvorbereitungskurse beachten Sie bitte die Kursvoraussetzungen der einzelnen Kurse.

Kompakt-Vorbereitung | Variante 1

Kurspaket: Information Security Manager mit eidg. Diplom (ICTSED)

Im Kurspaket bereiten Sie sich auf die Kernthemen der Prüfung vor. Profitieren Sie von einem attraktiven Bundlepreis.

Details & Inhalt

1. Onboarding (1 Stunde)
2. IT & Cybersecurity Risk Management (1 Tag)
- ★ Einführung Cybersecurity Risk Management
- ★ Die Auswirkungen von Cyber-Bedrohungen
- ★ Risikomanagement als Teil eines umfassenderen Cyber-Sicherheits-Management-Ansatzes
- ★ Erfüllung von Cyber-Sicherheitsstandards
- ★ Risikomanagement-Strategie
- ★ Bewährte Praxis

3. ISO/IEC 27001 Lead Implementer (4 Tage)
- ★ Einführung in ISO/IEC 27001 und Initiierung eines ISMS
- ★ Planung der Einführung eines ISMS
- ★ Implementierung eines ISMS
- ★ ISMS-Überwachung, kontinuierliche Verbesserung und Vorbereitung auf das Zertifizierungsaudit

4. ISO/IEC 27001 Lead Implementer Brush-up (0.5 Tage)

5. ISO 27001 in der Praxis (0.5 Tage)
- ★ Warum haben wir uns für die ISO 27001 entschieden?
- ★ Wie sind wir vorgegangen?
- ★ Learnings und Empfehlungen

6. Projektmanagement-Grundlagen für IPMA Level D (3 Tage, ohne Prüfung)
- ★ Definition Projekt / Projektmanagement
- ★ Vorgehensmodelle Projektmanagement
- ★ Projektportfoliomanagement
- ★ Initiieren von Projekten
- ★ Planen von Projekten
- ★ Ausführen und Überwachen von Projekten
- ★ Abschluss von Projekten

7. Security Awareness im Unternehmen (0.5 Tage)
- ★ Strategische Planung von Security-Awareness-Massnahmen
- ★ Beispiele für methodische Trainingsansätze und -konzepte
- ★ Beispiele für ganzheitliche Security-Awareness-Programme
- ★ Nachhaltige Kommunikationsmethoden und -kanäle
- ★ Erfolgsmessung von Security-Awareness-Massnahmen/KPIs

8. Das neue Schweizer Datenschutzgesetz (1 Tag)
- ★ Datenschutzgrundsätze
- ★ Geltungsbereich
- ★ Personendaten Kategorien
- ★ Profiling
- ★ Informationspflichten (Cookies, Profiling-Tools etc.)
- ★ Einwilligung (Clickwrapping)
- ★ Meldepflichten (Prozess Data breaches)
- ★ Grundsätze der IT-Sicherheit (Privacy by Default und Privacy by Design)
- ★ Sanktionen (Bussen)
- ★ Betroffenenrechte (Prozessbeschreibungen)
- ★ Verhaltenskodex und Zertifizierungsverfahren
- ★ Spezialfragen: Cloud Computing und Auslandspeicherung, Auftragsdatenverarbeitung

9. Entwicklung Datenschutzkonzept / Datenschutz-Managementsystem DSMS (1 Tag)
- ★ Verzeichnis der Bearbeitungstätigkeiten
- ★ Datenschutz-Folgeabschätzung
- ★ Datenschutzerklärung

10. Cloud Service Governance für Manager (1 Tag)
- ★ Cloud Services – Service-Modelle, Architektur-Modelle und die Cloud Referenzarchitektur
- ★ Cloud Services im Business-Kontext und Governance
- ★ Cloud und der Daten-Lebenszyklus; rechtliche Anforderungen bezüglich Cloud Security
- ★ Security Zertifizierungen und Attestierungen im Cloud-Umfeld
- ★ Kryptographie und Key Management in Clouds; Cloud Access Security Broker (CASB)
- ★ Cloud Services und Business Continuity, Desaster Recovery
- ★ Risiken von Cloud Services und der sichere Weg in die Cloud
- ★ Cloud Security Operations, Security Incident Management, Security Testing und Forensik in Cloud Services

11. Cybersecurity – Technical Overview (2 Tage)
- ★ Differenzierung Informationssicherheit, ICT-Sicherheit, Cyber-Sicherheit; IT-Security und OT-Security, Safety & Security
- ★ Lebenszyklus von Daten
- ★ Technology-Levels – Abstraktionsstufen zwischen Geschäftsprozess und IT / Technik
- ★ Sicherheitsarchitekturen – Sicherheitsmodelle
- ★ Computersysteme – Client/Server; Prozessor-Architekturen
- ★ Kryptographie
- ★ Netzwerk-Grundlagen: das OSI-Modell vom Physical Layer bis zum Application Layer
- ★ Sicherheit im Netzwerk, Physische Sicherheit
- ★ Identity- und Access-Management (IAM)
- ★ Security-Assessment und Testing
- ★ Software Development Security

12. Security Governance und -Management (2 Tage)
- ★ Information Security Governance
- ★ ICT Security Organisation
- ★ ICT Security Architektur
- ★ Information Security Metrics, Reporting
- ★ Information Security Business Case, Return on Security Investment
- ★ Information Security Incident Management

13. Prüfungsvorbereitung (4 Tage)

Code: ICTSED
Information Security Manager mit eidg. Diplom
Dauer: 21 Tage | Preis: CHF 18'800.– zzgl. 8.1% MWST

Individueller Weg | Variante 2

Verankern der Sicherheitsstrategie

Module

★ Information Security Manager 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.

★ Information Security Manager verankern die Informationssicherheit in der Organisation und führen die Sicherheitsorganisation. Dazu gehören die Definition der Rolle des Steuerungsgremiums in Abstimmung mit der Organisation sowie 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.

★ Information Security Manager 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.

Die einzeln buchbaren Vorbereitungsmodule

ISO/IEC 27001:2022 Foundation – 2 Tage, CHF 2200.– (inkl. Prüfungsvoucher)
Sie wollen mehr über Informationssicherheit erfahren? Dann lernen Sie die ISO/IEC 27001:2022 kennen und verstehen. Ihr Wissen dokumentieren Sie mit der abschliessenden Zertifizierung ISO/IEC 27001 Foundation.
Weitere Infos: www.digicomp.ch/d/IS27F

ISO/IEC 27001:2022 Lead Implementer – 4.5 Tage, CHF 4900.– (inkl. Prüfungsvoucher)
Sie planen ein Informationssicherheitsmanagementsystem aufzusetzen und zu betreiben? Dann lernen Sie von unseren Profis, wie Sie dies effizient und effektiv angehen und dokumentieren Sie Ihr Wissen mit der abschliessenden Zertifizierung.
Weitere Infos: www.digicomp.ch/d/IS27I

ISO/IEC 27001:2022 Lead Auditor – 4.5 Tage, CHF 4900.– (inkl. Prüfungsvoucher)
Sie wollen ISO/IEC 27001 Audits professionell durchführen? Lernen Sie die anerkannten Audit-Grundsätze, -Verfahren und -Techniken kennen und dokumentieren Sie Ihr Wissen mit der abschliessenden Zertifizierung.
Weitere Infos: www.digicomp.ch/d/IS27A

Die Handlungskompetenzen

Veranken der Sicherheitsstrategie	A1: Informationssicherheitsgrundlagen erarbeiten	A2: Informationssicherheit in der Geschäftsleitung und im Verwaltungsrat verankern	A3: Führung und Steuerung der Informationssicherheit managen	A4: Sicherheitsorganisation etablieren	A5: Informationssicherheitsspezialisten fachlich führen

Individueller Weg | Variante 2

Etablieren des Informationssicherheits-Managementsystems (ISMS)

Module

★ Information Security Manager stellen den Managementsupport für das Informationssicherheitsmanagementsystem (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.

★ Information Security Manager beobachten die Entwicklung im Bereich neuer Technologien und des sicherheitsrelevanten Umfelds. 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.

★ Information Security Manager 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 und kategorisieren Schwachstellen, veranlassen deren Kontrolle und führen erforderliche Wiederholungsüberprüfungen sowie Retests durch.

★ Information Security Manager 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.

Die einzeln buchbaren Vorbereitungsmodule

ISO/IEC 27001:2022 Foundation – 2 Tage, CHF 2200.– (inkl. Prüfungsvoucher)
Sie wollen mehr über Informationssicherheit erfahren? Dann lernen Sie die ISO/IEC 27001:2022 kennen und verstehen. Ihr Wissen dokumentieren Sie mit der abschliessenden Zertifizierung ISO/IEC 27001 Foundation.
Weitere Infos: www.digicomp.ch/d/IS27F

ISO/IEC 27001:2022 Lead Implementer – 4.5 Tage, CHF 4900.– (inkl. Prüfungsvoucher)
Sie planen ein Informationssicherheitsmanagementsystem aufzusetzen und zu betreiben? Dann lernen Sie von unseren Profis, wie Sie dies effizient und effektiv angehen und dokumentieren Sie Ihr Wissen mit der abschliessenden Zertifizierung.
Weitere Infos: www.digicomp.ch/d/IS27I

ISO/IEC 27001:2022 Lead Auditor – 4.5 Tage, CHF 4900.– (inkl. Prüfungsvoucher)
Sie wollen ISO/IEC 27001 Audits professionell durchführen? Lernen Sie die anerkannten Audit-Grundsätze, -Verfahren und -Techniken kennen und dokumentieren Sie Ihr Wissen mit der abschliessenden Zertifizierung.
Weitere Infos: www.digicomp.ch/d/IS27A

Security Governance und -Management – 2 Tage, CHF 2200.–
Der Chief Information Security Officer muss interdisziplinäre Erwartungen und Bedürfnisse im Unternehmen erfüllen – zu möglichst tiefen Kosten. Wie die Balance zwischen Prävention, Detektion und Reaktion effizient gelingt, lernen Sie in diesem Kurs.
Weitere Infos: www.digicomp.ch/d/ICTMAG

Die Handlungskompetenzen

Etablieren des Informationssicherheits-Managementsystems (ISMS)	B1: ISMS führen	B2: Prozesse etablieren	B3: Risiken managen	B4: Informationssicherheitsanforderungen in allen Prozessen integrieren	B5: Sicherheitsvorgaben definieren
	B6: Sicherheitsüberprüfung sicherstellen	B7: Security im Outsourcing überwachen	B8: Performance messen	B9: Informationsspezifische Anfoderungen an Personensicherheitsüberprüfung definieren	

Individueller Weg | Variante 2

Führen des Sicherheitsprogramms

Module

★ Information Security Manager 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.

★ Information Security Manager 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.

Die einzeln buchbaren Vorbereitungsmodule

Cybersecurity – Technical Overview – 2 Tage, CHF 2200.–
In diesem Kurs eignen Sie sich das Verständnis für die technologischen Grundlagen der ICT- und Cyber-Sicherheit an und erlernen die notwendigen Kompetenzen für eine effektive Informationssicherheit.
Weitere Infos: www.digicomp.ch/d/ICTTEC

Cloud Service Governance für Manager – 1 Tag, CHF 1300.–
Der Chief Information Security Officer muss interdisziplinäre Erwartungen und Bedürfnisse im Unternehmen erfüllen – zu möglichst tiefen Kosten. Wie die Balance zwischen Prävention, Detektion und Reaktion effizient gelingt, lernen Sie in diesem Kurs.
Weitere Infos: www.digicomp.ch/d/CLSECU

Certified Information Systems Security Pro – 5 Tage, CHF 5190.–
Ziel dieses Kurses ist die Absolvierung der CISSP-Prüfung. Mit diesem Zertifikat erhöhen Sie Ihre Attraktivität für Arbeitgeber enorm. Sie helfen zudem mit, einen hohen Sicherheitsstandard zu garantieren und aufrechtzuerhalten.
Weitere Infos: www.digicomp.ch/d/SSP

Die Handlungskompetenzen

Führen des Sicherheitsprogramms	C1: ICT-Security-Architektur erarbeiten	C2: Produkt-/ServicePortfolio managen	C3: Portfoliomanagement-Security-Programm erstellen	C4: Business Case entwickeln	C5: Informationssicherheitslösungen evaluieren
	C6: Umsetzung der beschlossenen Massnahmen sicherstellen	C7: Projekte leiten	C8: Innovationen in die Informationssicherheit integrieren		

Individueller Weg | Variante 2

Managen von Stakeholdern

Module

★ Information Security Manager 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.

Die einzeln buchbaren Vorbereitungsmodule

Projektmanagement-Grundlagen für IPMA Level D – 3 Tage, CHF 2200.–
In diesem Kurs lernen Sie, wie Projekte initiiert, geplant, ausgeführt, überwacht und abgeschlossen werden. Neben den strukturellen Elementen lernen Sie auch kulturelle Aspekte zu berücksichtigen und bereiten sich vor auf die IPMA-Level-D-Zertifizierung.
Weitere Infos: www.digicomp.ch/d/PMEM

Projektmanagement für die Praxis – 4 Tage, CHF 3200.–
In diesem Kurs lernen Sie, wie Projekte initiiert, geplant, ausgeführt, überwacht und abgeschlossen werden. Neben den strukturellen Elementen lernen Sie auch kulturelle Aspekte zu berücksichtigen und bereiten sich vor auf die IPMA-Level-D-Zertifizierung.
Weitere Infos: www.digicomp.ch/d/PMEMFP

Die Handlungskompetenzen

Managen von Stakeholdern	D1: Tragfähiges trusted Netzwerk unterhalten	D2: Stakeholder fachlich beraten	D3: Informationssicherheitscompliance einfordern	D4: Projekte begleiten	D5: Sicherheitsaspekte in Proofs of Concept sicherstellen

Individueller Weg | Variante 2

Schaffen von Awareness

Module

★ Information Security Manager 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 Information Security Manager 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.

Die einzeln buchbaren Vorbereitungsmodule

Security Awareness im Unternehmen – 0.5 Tage, CHF 600.–
In diesem Kurs lernen Sie, wie Sie Ihr Unternehmen mit Hilfe Ihrer Mitarbeitenden gegen Sicherheits- und Betrugsfälle von aussen schützen können.
Weitere Infos: www.digicomp.ch/d/SAWG

Die Handlungskompetenzen

Schaffen von Awareness	E1: Awareness-kampagne durchführen	E2: Sicherheits-kommunikation intern und extern sicherstellen

Individueller Weg | Variante 2

Bewältigen von Ereignissen

Module

★ Information Security Manager 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.

★ Information Security Manager 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.

Die einzeln buchbaren Vorbereitungsmodule

ISO/IEC 27001:2022 Foundation – 2 Tage, CHF 2200.– (inkl. Prüfungsvoucher)
Sie wollen mehr über Informationssicherheit erfahren? Dann lernen Sie die ISO/IEC 27001:2022 kennen und verstehen. Ihr Wissen dokumentieren Sie mit der abschliessenden Zertifizierung ISO/IEC 27001 Foundation.
Weitere Infos: www.digicomp.ch/d/IS27F

ISO/IEC 27001:2022 Lead Implementer – 4.5 Tage, CHF 4900.– (inkl. Prüfungsvoucher)
Sie planen ein Informationssicherheitsmanagementsystem aufzusetzen und zu betreiben? Dann lernen Sie von unseren Profis, wie Sie dies effizient und effektiv angehen und dokumentieren Sie Ihr Wissen mit der abschliessenden Zertifizierung.
Weitere Infos: www.digicomp.ch/d/IS27I

Security Governance und -Management – 2 Tage, CHF 2200.–
Der Chief Information Security Officer muss interdisziplinäre Erwartungen und Bedürfnisse im Unternehmen erfüllen – zu möglichst tiefen Kosten. Wie die Balance zwischen Prävention, Detektion und Reaktion effizient gelingt, lernen Sie in diesem Kurs.
Weitere Infos: www.digicomp.ch/d/ICTMAG

Die Handlungskompetenzen

Bewältigen von Ereignissen	F1: Business-Impact-Analyse sicherstellen	F2: Notfallorganisation für Security Incidents sicherstellen	F3: Security Incident managen	F4: Integration von Informatiksicherheitsaspekten im Business Continuity Management sicherstellen

Individueller Weg | Variante 2

Sichern von Informationen

Module

★ Der Information Security Manager definiert das Regelwerk zur Datenklassifizierung in Absprache mit den Dateneignern. Sie erstellen 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.

Die einzeln buchbaren Vorbereitungsmodule

Umsetzung des neuen Schweizer Datenschutzgesetz – 2 Tage, CHF 1900.–
Sie werden in die neuen datenschutzrechtlichen Anforderungen des revidierten Schweizer Datenschutzgesetzes eingeführt. Nach diesem Kurs verfügen Sie über die Handlungsfähigkeit, die datenschutzrechtlichen Bestimmungen in Ihrer Organisation umzusetzen.
Weitere Infos: www.digicomp.ch/d/NDSG

Die Handlungskompetenzen

Sichern von Informationen	G1: Klassifizierung von Informationen sicherstellen	G2: Datensicherheit bei der Übertragung sicherstellen	G3: Datensicherheit bei der Speicherung und Archivierung sicherstellen

Prüfungsinformationen

eidg. dipl.

Zweck der Prüfung
Die eidgenössische höhere Fachprüfung dient dazu, abschliessend zu prüfen, ob die Kandidatinnen und Kandidaten über die Kompetenzen verfügen, die zur Ausübung einer anspruchsvollen und verantwortungsvollen Berufstätigkeit als Information Security Manager erforderlich sind.

Die Eidg. Diplomprüfung besteht aus folgenden Teilen:
★ Portfolioarbeit (schriftlich, vorgängig erstellt)
★ Präsentation & Fachgespräch (mündlich, 30 bis 40 Minuten)
★ Fallstudien (schriftlich, 120 Minuten)
★ Fallsimulation (praktisch, 300 Minuten)

Prüfungsteil 1, Portfolioarbeit
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 mindestens vier Handlungskompetenzbereichen je mindestens zwei Handlungskompetenzen bearbeitet werden.

Prüfungsteil 2, Präsentation und Fachgespräch zum Portfolio
Die Kandidatinnen und Kandidaten präsentieren ihre Portfolioarbeit. Das individuelle Portfolio dient als Basis für das Fachgespräch, in welchem die Kandidatinnen und Kandidaten Fragen der Expertinnen und Experten ihrer Arbeit beantworten.

Prüfungsteil 3, 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.

Prüfungsteil 4, 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. Die Fallsimulationen dienen der Überprüfung von Haltungen, wie sie in der Wegleitung beschrieben sind. Mit diesem Prüfungsteil werden verschiedene Haltungen überprüft, wobei auf Teamfähigkeit, Kommunikationsfähigkeit und Urteilsvermögen ein besonderes Gewicht gelegt wird.

Diplomtitel und Veröffentlichung
Das eidgenössische Diplom wird auf Antrag der Prüfungskommission vom SBFI ausgestellt und von dessen Direktion und der Präsidentin oder dem Präsidenten der Prüfungskommission unterzeichnet.

Die Diplominhaberinnen und -inhaber sind berechtigt, folgenden geschützten Titel zu führen:
★ Information Security Manager mit eidgenössischem Diplom
★ Information Security Manager avec diplôme fédéral
★ Information Security Manager con diploma federale

Die englische Übersetzung lautet «Information Security Manager, Advanced Federal Diploma of Higher Education»

Die Namen der Diplominhaberinnen und -inhaber werden in ein vom SBFI geführtes Register eingetragen.

Wir sind gerne für Sie da: **T +41 44 447 21 21 – info@digicomp.ch**

Digicomp portrait

Ihre Ansprechpartnerin
für diesen Lehrgang:
Gabriela Wittwer
Kundenberaterin
+41 44 447 21 11
gabriela.wittwer@digicomp.ch

Die Digitalisierung zwingt Unternehmen zur Transformation, von der Strategie, über die Prozesse bis zur Kultur. Der Wandel betrifft sämtliche Unternehmensbereiche und Funktionen. Wir sind überzeugt: Zentral für die Gestaltung des Wandels sind die digitalen Kompetenzen der Mitarbeitenden. Denn es sind Menschen, die Unternehmen heute und in Zukunft gemeinsam erfolgreich machen.

Deshalb arbeitet Digicomp stetig an neuen Inhalten und Lernformen, um die Mitarbeitenden im Unternehmen für ständigen Wandel zu befähigen. Ob Videolearning, virtuelles Lernen, klassische Trainings, Coaching am Arbeitsplatz oder Workshops – Digicomp bietet für ihre Kursbesucher die passende Lernform für eine sofortige Praxisumsetzung an. Unsere Trainer sind erfahrene Praktiker mit didaktischer Ausbildung und Gespür für den richtigen Ton. Aktuelle Unterlagen, bestes Equipment und moderne didaktische Konzepte, sympathische Betreuung, heisser Kaffee, backfrische Gipfeli und knackige Früchte leisten den übrigen Teil, damit die Weiterbildung bei Digicomp zum Erfolg wird.

Dank topzentraler Lagen in Zürich, Bern, Basel, Lausanne und Genf sind alle Digicomp Bildungszentren ideal mit öffentlichen Verkehrsmitteln erreichbar. Unsere Teilnehmenden kommen also entspannt und schnell zum Schulungsort – ein weiterer wichtiger Beitrag für den nachhaltigen Lernerfolg.

Mit dieser ausschliesslich auf die Entwicklung digitaler Kompetenzen von Menschen fokussierten Strategie nimmt Digicomp in der Schweizer Bildungslandschaft mit jährlich über 25'000 Kursbesuchern einen führenden Platz ein. Wer sich weiterbilden und neue Ziele erreichen will, hat bei Digicomp die Auswahl aus über 1000 verschiedenen Kursthemen an sieben Standorten in der Schweiz – Dienstleistungen aus einer Hand sind auch über die Sprachgrenzen hinaus garantiert.

Digicomp – Digital Competence. Made of People.

How to find us

50 Kursräume an 5 zentralen Standorten in der Schweiz machen Digicomp leicht erreichbar. Treten Sie mit uns in Kontakt und erfahren Sie mehr!

Zürich
Digicomp Academy AG
Limmatstrasse 50
8005 Zürich
T +41 44 447 21 21
zuerich@digicomp.ch

Bern
Digicomp Academy AG
Bubenbergplatz 11
3011 Bern
T +41 31 313 22 22
bern@digicomp.ch

Basel
Digicomp Academy AG
Küchengasse 9
4051 Basel
T +41 61 278 33 33
basel@digicomp.ch

Lausanne
Digicomp Academy
Suisse Romande SA
Avenue de la Gare 50
1003 Lausanne
T +41 21 321 65 00
lausanne@digicomp.ch

Genève
Digicomp Academy
Suisse Romande SA
Rue de Monthoux 64
1201 Genève
T +41 22 738 80 80
geneve@digicomp.ch

Eager for more?

digicomp.ch