Certified Information Systems Security Professional (CISSP)

ID CISSP **Preis** CHF 4'290.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

Jeder, der umfassendes Wissen auf sehr breiter Basis zur Informationssicherheit benötigt, wie

- erfahrene IT-Experten,
- Sicherheitsberater,
- Information Security Manager,
- Risk Manager,
- Sicherheitsbeauftragte,
- Führungskräfte in der IT / Sicherheit,
- Gutachter / Auditoren,
- Sicherheits- und IT-Architekten,
- Security- und IT-Analysten,
- Security- und IT-Designer,
- Security- und IT-Tester,
- Systemingenieure,
- Security Engineers,
- Netzwerkarchitekten und alle anderen, die ihr Wissen vertiefen und zertifizieren möchten.

Voraussetzungen

Mehrjährige Berufserfahrung in der IT und/oder Informationssicherheit wird empfohlen, um maximale Vorteile aus dem Kurs zu ziehen.

Voraussetzungen für eine erfolgreiche Zertifizierung

Erfolgreiches Bestehen des CISSP-Examens und 5 Jahre Berufserfahrung in mind. zwei der acht CISSP-CBK-Domänen, bestehende Qualifikationen (wie bspw. Universitätsabschlüsse und andere Zertifizierungen) werden angerechnet (Official ISC2 Approved List). Fehlende Berufserfahrung kann bis zu 5 Jahren nach bestandener Prüfung erworben werden, ohne das Examen erneut absolvieren zu müssen. Falls Sie aktuell nicht über die erforderliche Berufserfahrung verfügen, steht Ihnen dennoch die Zertifizierung offen: Sie können den Kurs und die Prüfung ablegen und werden dann als Associate of ISC2 geführt, dürfen mit Ihrem Zertifikat am Markt werben und die fehlende Berufserfahrung innerhalb von 5 Jahren einholen. Ihr Zertifikat wird danach automatisch in ein vollwertiges CISSP-Zertifikat umgewandelt, ohne dass Sie die Prüfung erneut ablegen müssen.

Kursinhalt

CISSP Common Body of Knowledge (CBK)

5-tägiger Intensivkurs über alle acht Domänen des CISSP CBK mit täglich jeweils acht Unterrichtsstunden Prüfungsvorbereitung und individueller Beratung jedes Teilnehmers.

Domain 1 - Security and Risk Management

- Sicherheitsanforderungen
- Compliance, Recht, Regulierung und Richtlinien
- Standards und Frameworks
- Risiko Management
- Business Continuity

Domain 2 - Asset Security

- Sicherheitsmodelle und Frameworks
- Schutz der Vermögenswerte
- Klassifikation

Domain 3 - Security Architecture and Engineering

- Verständnis der Sicherheitsmodelle
- Design und Schutzmassnahmen
- Kryptographie
- Physische Sicherheit

Domain 4 - Communication and Network Security

- Topologien
- Technologien
- Protokolle
- Angriffe
- Sicherheitsmassnahmen

Domain 5 - Identity and Access Management (IAM)

- Identitätskontrolle
- Zugriffskontrollmodelle

Domain 6 - Security Assessment and Testing

- Planung und Durchführung von Sicherheitstests
- Vulnerability Assessments
- Pentests

Domain 7 - Security Operations

- Sicherer Betrieb und Wartung
- Incidence Response
- Disaster Recovery Planning

Domain 8 - Software Development Security

- Entwicklung sicherer Software-Anwendungen
- Web-Anwendungen und mobile Anwendungen
- Malware und Angriffe auf Anwendungen
- IoT und ICS

Kursaufbau – Ihr 5 Tage Learning Path

Tag 1 – Security & Risk Management + Asset Security (Domains 1 & 2)

- Der Kurs startet mit den Grundlagen der CISSP Denkweise: Governance, Policies, Standards, Security Management Konzepte und Ethik.
- Sie erarbeiten sich konzeptionelles Risiko und Compliance Verständnis sowie BCP/DR Grundlagen.
- Im Anschluss folgt Asset Security mit Datenklassifizierung, Data Handling, Data Lifecycle und Privacy Grundlagen.
- Der Tag endet mit einem strukturierten Fragenblock (inkl. Szenariofragen).

Tag 2 – Security Architecture & Engineering (Domain 3)

- Sie tauchen in Security Architekturprinzipien, Sicherheitsmodelle, Trusted Concepts, Isolation und Assurance ein.
- Anschliessend behandeln Sie konzeptionelle Kryptografie Grundlagen, PKI und Key Management.
- Der Tag schliesst mit Physical/Environmental Security und Platform Security (inkl. TPM/HSM auf konzeptioneller Ebene).
- Auch dieser Kurstag endet mit einem Fragenblock zur Lernfestigung.

Tag 3 – Communication & Network Security + Identity & Access Management (Domains 4 & 5)

- Der Vormittag behandelt Secure Network Design, Segmentierung, sicherheitsrelevante OSI/TCP IP Aspekte, sichere Protokolle sowie VPN , TLS und Wireless Security Konzepte.
- Nachmittags folgt IAM: Authentifizierung/Autorisierung, Access Control Modelle (DAC, MAC, RBAC, ABAC), Federation/SSO (SAML, OIDC) sowie MFA und Identity Lifecycle Prozesse.
- Abschluss durch einen täglichen Fragenblock.

Tag 4 – Security Assessment & Testing + Security Operations (Domains 6 & 7)

- Sie lernen Strategien des Security Assessments, Audit Methoden, KPIs/Metriken und die Prozesssicht auf Vulnerability Management.
- Danach folgen Logging/Monitoring, Unterschiede zwischen VA, Penetration Testing und Audits sowie Reporting Ansätze.
- In Domain 7 vertiefen Sie Incident Response Lifecycle, Detection & Response, SOC Grundlagen, Forensics Basics sowie Change & Configuration Management.
- Der Tag endet mit einem Mini Mock: 30–40 realitätsnahe Prüfungsfragen inkl. Auswertung.

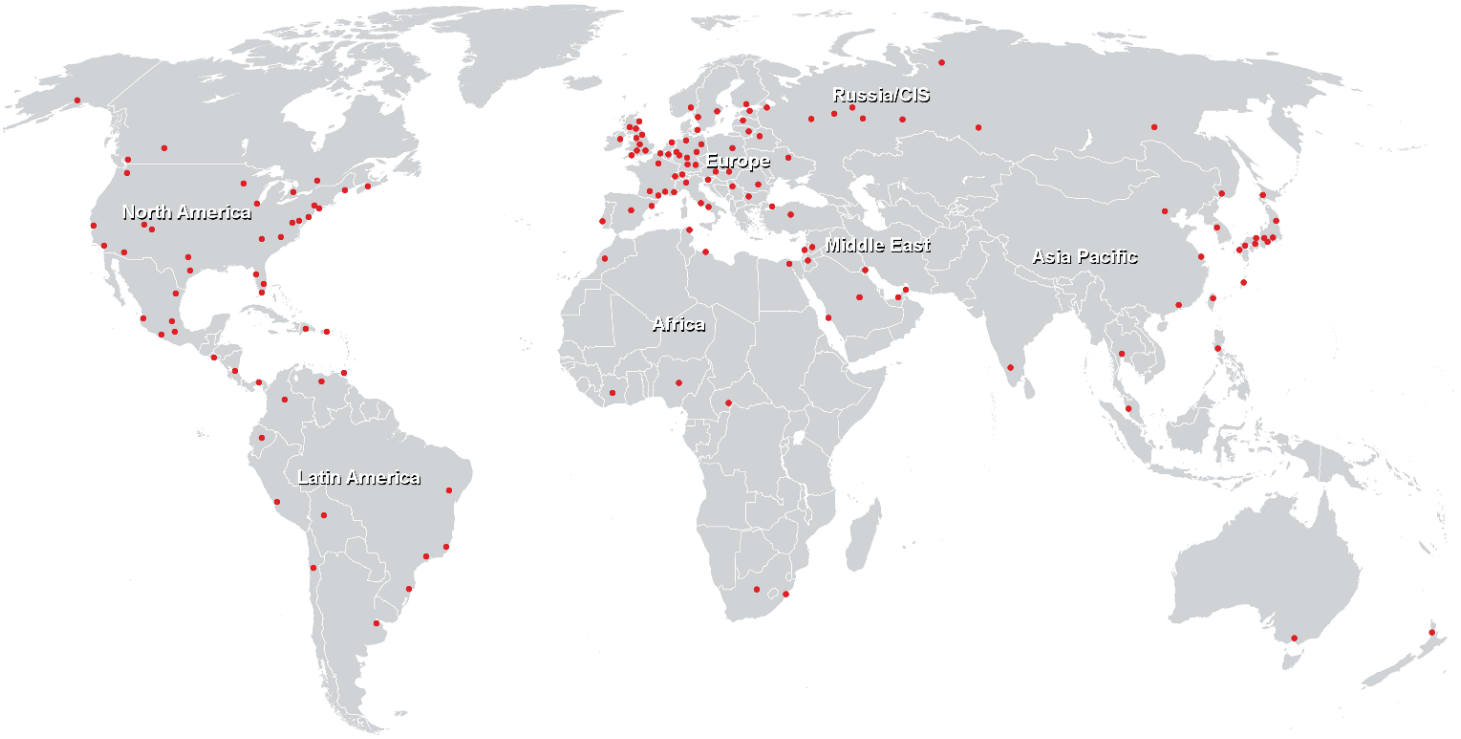
Tag 5 – Software Development Security + Gesamt Review (Domain 8)

- Zum Abschluss stehen SDLC, Secure Requirements, Secure Design und Threat Modeling im Fokus – auf CISSP Niveau.
- Sie behandeln Secure Coding Konzepte, Code Reviews, DevSecOps Grundlagen sowie Supply Chain Security.
- Danach folgt ein intensiver 40 Fragen Block mit Szenarioanteil sowie eine strukturierte Auswertung: High Yield Fallen, Prüfungsstrategie, Priorisierung und Zeitmanagement.

- Tägliche Fragenblöcke zur direkten Wissensverankerung
- Mini Mock am Donnerstag als realitätsnahe Prüfungssimulation
- 40 Fragen Abschlussblock am Freitag
- Schwerpunkt: Management orientierte Entscheidungen statt Technikdetails
- „Best Answer“-Ansatz für anspruchsvolle CISSP Szenariofragen
- Strukturierter Review aller Domains nach dem offiziellen CISSP CBK

Certified Information Systems Security Professional (CISSP)

Weltweite Trainingscenter





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch