CISSP®

Certified Information Systems Security Professional

Gliederung der **Zertifizierungsprüfung**

Stand: April 2018

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

Über CISSP

Das Zertifikat des „Certified Information Systems Security Professional" (CISSP) gilt als eines der weltweit am höchsten bewerteten Zertifikate auf dem Markt der Informationssicherheit. Der CISSP bescheinigt einem Informationssicherheitsexperten umfangreiche technische und organisatorische Kenntnisse sowie die Erfahrung zum effektiven designen, entwickeln und planen aller firmeninternen Sicherheitsanforderungen.

Das weitreichende Themenspektrum des „CISSP Common Body of Knowledge" (CBK) gewährleistet eine Relevanz über alle Themenfelder der Informationssicherheit. Zertifizierte Kandidaten sind erfahren in den nachfolgenden 8 Fachgebieten:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Anforderungen an die Berufserfahrung

Kandidaten benötigen insgesamt mindestens 5 Jahre einer Vollzeit Festanstellung, mit Erfahrungen in 2 oder mehr Fachgebieten des CISSP CBK. Der Nachweis eines 4-jährigen Universitätsabschlusses, eines anderweitig vergleichbaren oder eines Abschlusses, der auf der (ISC)² Anforderungsliste veröffentlicht ist, ist äquivalent zum Nachweis eines Jahres an Berufserfahrung. Jegliche Ausbildung ist auf den Nachweis von einem Jahr Erfahrung begrenzt.

Ein Kandidat ohne die für den CISSP benötigte Erfahrung kann durch die erfolgreiche Absolvierung des CISSP zum „Associate" des (ISC)² werden. Der „Associate" des (ISC)² hat die nächsten 6 Jahre Zeit, den Nachweis der fünfjährigen Erfahrung zu erbringen.

Akkreditierung

CISSP war das erste Zertifikat auf dem Gebiet der Informationssicherheit, das die hohen Anforderungen des ANSI/ ISO/IEC Standards 17024 erfüllt hat.

Job Task Analysis (JTA)

(ISC)² hat die Verpflichtung gegenüber seinen Mitgliedern, die Praxisrelevanz des CISSP sicherzustellen. In regelmäßig stattfindenden „Job Task Analysis" (JTA) Seminaren, werden die Aufgaben, die Informationssicherheitsexperten gemäß des CISSP durchführen, in einem methodischen und kritischen Prozess hinterfragt. Das Ergebnis des JTA dient zur Aktualisierung der Prüfungen. Dieser Prozess stellt sicher, daß die Kandidaten in Themenbereichen geprüft werden, die für die Rollen und Verantwortlichkeiten praktizierender Informationssicherheitsexperten relevant sind.

CISSP CAT Prüfungsinformationen

Die CISSP Prüfung bedient sich für alle englischen Prüfungen des „Computerized Adaptive Testing" (CAT). CISSP Prüfungen in allen anderen Sprachen bestehen aus einer festen Anzahl von Fragen pro Fachgebiet. Weitere Informationen über CISSP CAT sind verfügbar über: www.isc2.org/certificatons/CISSP-CAT.

Dauer der Prüfung	3 Stunden
Anzahl der Fragen	100 - 150
Aufbau der Prüfung	Multiple Choice und weitere innovative Fragetechniken
Mindestpunktzahl	700 von 1000 Punkten
Sprache	Englisch
Prüfungsort	(ISC)² autorisiertes PPC und PVTC Select Pearson VUE Testing Centers

CISSP CAT Gewichtungsverteilung

Fachgebiet	Gewichtung
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	14%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	10%
Summe:	**100%**

CISSP Prüfungen basierend auf Fragen pro Fachgebiet

Dauer der Prüfung	6 Stunden
Anzahl der Fragen	250
Aufbau der Prüfung	Multiple Choice und weitere innovative Fragetechniken
Mindestpunktzahl	700 von 1000 Punkten
Sprachen	Französisch, Deutsch, brasilianisches Portugiesisch, Spanisch, Japanisch, vereinfachtes Chinesisch, Koreanisch
Prüfungsort	(ISC)² Authorized PPC und PVTC Select Pearson VUE Testing Centers

CISSP Gewichtungsverteilung bei Fragen pro Fachgebiet

Fachgebiet	Gewichtung
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	14%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	10%
Summe:	**100%**

Fachgebiet 1: Security and Risk Management

1.1 Verständnis der Konzepte für Vertraulichkeit, Integrität und Verfügbarkeit sowie ihre Anwendung

1.2 Evaluierung und Anwendung von behördlichen Sicherheitsprinzipien

- Ausrichtung der Sicherheitsmechanismen gemäß der Geschäftsstrategie, Ziele und Aufgaben
- Organisatorische Prozesse (z.B. Zukäufe, Veräußerungen und gesetzgeberische Auflagen)
- Organisatorische Rollen und Verantwortlichkeiten
- Systeme für Sicherheitskontrollen
- „Due Care / Due Diligence“
- Untersuchung von Konformitätsanforderungen

1.3 Untersuchung von Konformitätsanforderungen

- Vertraglich, gesetzlich und gemäß der Anforderungen von Industriestandards sowie Aufsichtsbehörden
- Datenschutzanforderungen

1.4 Verständnis für rechtliche und regulatorische Fragen, die die Informationssicherheit in einem globaleren Kontext betreffen

- Cyberkriminalität und Datenmissbrauch
- Lizensierung und geistiges Eigentum
- Im- / Export-Kontrollen
- Grenzüberschreitender Datentransfer
- Privatsphäre

1.5 Verständnis, Anwendungen und Verbreitung eines Berufsethos

- Berufsethos des (ISC)²
- Ethische Grundsätze von Organisationen

1.6 Entwicklung, Dokumentation und Implementierung einer Sicherheitspolitik, von Standards, von Prozeduren und von Leitfäden

1.7 Identifizierung, Analyse und Priorisierung von Anforderungen zur Systemverfügbarkeit (Betriebskontinuitätsmanagement)

- Entwicklung und Dokumentation der Anforderungen und des Plans
- Business Impact Analyse (BIA)

1.8 Mitarbeit bei der Erstellung und Umsetzung von Sicherungsleitlinien und Prozeduren für Mitarbeiter

- Kandidaten Screening und ihre Einstellung
- Mitarbeitervereinbarungen und Leitlinien
- Einstellungs- und Entlassungsprozesse
- Vereinbarungen und Kontrollen für Zulieferer, Berater und Vertragspartner
- Konformitätsanforderungen
- Datenschutzbestimmungen

1.9 Verständnis von Risiko Management Konzepten und ihre Anwendung

- Identifikation von Bedrohungen und Sicherheitslücken
- Risikoprüfungen / Analyse
- Risikobetrachtungen
- Auswahl und Implementierung von Gegenmaßnahmen
- Anwendungsgerechte Kontrollen (z.B. preventive, detective, corrective)
- „Security Control Assessment" (SCA)
- Messung und Überwachung
- Vermögensbewertung
- Reporting
- Fortwährende Verbesserung
- Risikoabschätzungen

1.10 Verständnis von Methoden und Konzepten der Bedrohungsmodellierung und ihre Anwendung

- Methoden der Bedrohungsmodellierung
- Konzepte der Bedrohungsmodellierung

1.11 Anwendung risikobasierter Managementkonzepte in der Lieferkette

- Risiken verbunden mit Hardware, Software und Dienstleistungen
- Beurteilung und Kontrolle von Drittanbietern
- Minimale Sicherheitsanforderungen
- Anforderungen an den Servicelevel

1.12 Etablierung und Pflege eines Sicherheitsbewusstseins, einer Sicherheitsausbildung und eines Sicherheitstrainingsprogramms.

- Präsentation von Methoden und Techniken zur Sensibilisierung und für Trainings
- Regelmäßige Überprüfung der Inhalte
- Evaluierung der Effektivität des Programms

Fachgebiet 2: Asset Security

2.1 Identifizierung und Klassifizierung von Informationen und Vermögenswerten

- Klassifizierung von Daten
- Klassifizieren von Vermögenswerten

2.2 Bestimmen und Verwalten der Eigentümerschaft von Informationen und Vermögenswerten

2.3 Datenschutz

- Eigentum von Daten
- Verarbeitung von Daten
- Datenremanenz
- Beschränkung bei der Datensammlung

2.4 Sicherstellung angemessener Pflege von Vermögenswerten

2.5 Festlegung von Kontrollen zur Datensicherheit

- Verstehen von Datenzuständen
- Fokussierung und Anpassung
- Auswahl von Standards
- Methoden des Datenschutzes

2.6 Etablierung von Anforderungen für die Behandlung von Information und Vermögenswerten

Fachgebiet 3: Security Architecture and Engineering

3.1 Implementierung und Verwaltung von technischen Prozessen unter Nutzung von Prinzipien des sicheren Design

3.2 Verständnis für die grundlegenden Konzepte von Sicherheitsmodellen

3.3 Selektion von Kontrollen basierend auf den Sicherheitsanforderungen von Systemen

3.4 Verständnis für die Tauglichkeit von Informationssystemen hinsichtlich Sicherheit (z .B. Schutz des Speichers, Trusted Platform Module (TPM), Verschlüsselung / Entschlüsselung)

3.5 Untersuchung und Verringerung der Schwachstellen von Sicherheitsarchitekturen, Designs und Lösungsansätzen

- Client-basierte Systeme
- Server-basierte Systeme
- Datenbank-Systeme
- Kryptographische Systeme
- „Industrial Control Systems“ (ICS)
- Cloud-basierte Systeme
- Verteilte Systeme
- „Internet of Things“ (IoT)

3.6 Untersuchung und Verringerung der Schwachstellen in Web-basierten Systemen

3.7 Untersuchung und Verringerung der Schwachstellen in mobilen Systemen

3.8 Untersuchung und Verringerung der Schwachstellen in eingebetteten Einheiten

3.9 Anwendung von Kryptographie

- Kryptographischer Lebenszyklus (z.B. Schlüsselmanagement, Auswahl von Algorithmen)
- Kryptographische Methoden (z. B. symmetrische, asymmetrische, elliptische Kurven)
- Public Key Infrastrukturen (PKI)
- Key Management Methoden
- Digitale Signaturen
- Non-repudiation
- Integrität (z. B. Hashing)
- Verständnis von Angriffsmethoden der Kryptoanalyse
- Digitales Rechte Management (DRM)

3.10 Anwendung der Sicherheitsmaßnahmen beim Design von Standorten und Anlagen

3.11 Implementierung von Sicherheitskontrollen für Standorte und Anlagen

- Kabelschränke / Zwischenverteileranlagen
- Serverräume / Rechenzentren
- Medienspeicher
- Speicher zur Beweissicherung
- Beschränkungen und Arbeitsplatzsicherheit
- Dienstprogramme & Heizung, Lüftung und Klimaanlage
- Umweltprobleme
- Feuer-Verhütung, -Erkennung sowie -Bekämpfung

Fachgebiet 4: Communication and Network Security

4.1 Implementierung von Methoden eines sicheren Designs in Netzwerk Architekturen

- Open System Interconnection (OSI) und Transmission Control Protocol/Internet Protocol (TCP/IP) Modelle
- Internet Protocol (IP) Netzwerke
- Auswirkungen von multilayer Protokollen
- Konvergierende Protokolle
- Software-definierte Netzwerke
- Drahtlose Netzwerke

4.2 Komponenten sicherer Netzwerke

- Betrieb von Hardware
- Medien zur Übertragung
- Network Access Control (NAC) Geräte
- Sicherheit an Endpunkten
- Inhalt verteilende Netzwerke

4.3 Implementierung von sicheren Kommunikationskanälen gemäß des Designs

- Sprache
- Multimediale Zusammenarbeit
- Fernzugriff
- Kommunikation von Daten
- Virtualisierte Netzwerke

Fachgebiet 5: Identity and Access Management (IAM)

5.1 Kontrolle des physischen und logischen Zugriffs auf Vermögenswerte

- Informationen
- Systeme
- Geräte
- Einrichtungen

5.2 Management der Identifikation und Authentifizierung von Personen, Systemen oder Diensten

- Identity Management Installationen
- Single- / Multi-Faktor Authentifizierung
- Nachweisbarkeit
- Session Management
- Erfassung und Nachweis von Identitäten
- Systemübergreifendes Identitätsmanagement (FIM)
- Verwaltungssysteme der Anmeldeinformationen

5.3 Integration der Identitätsfeststellung als Dienstleistung Dritter

- vor Ort
- cloudbasiert
- integriert

5.4 Implementierung und Verwaltung von Autorisierungsmechanismen

- „Role Based Access Control" (RBAC)
- „Rule-based access Control"
- „Mandatory Access Control" (MAC)
- „Discretionary Access Control" (DAC)
- „Attribute Based Access Control" (ABAC)

5.5 Verwaltung des Lebenszyklus der Bereitstellung von Identitäten und Zugriffsberechtigungen

- Überprüfung der Zugriffe von Nutzern
- Überprüfung der Zugriff von Systemkonten
- Bereitstellung und Deaktivierung

Fachgebiet 6: Security Assessment and Testing

6.1 Design und Validierung von Prüfungen, Tests und Auditstrategien

- Intern
- Extern
- Dritt-Anbieter

6.2 Test-Durchführung von Sicherheitskontrollen

- Prüfungen von Schwachstellen
- Penetrationstests
- Log Reviews
- Synthetische Transaktionen
- Code Review und Testen
- Falsche Ausführung von Testfällen
- Analyse der Testfallabdeckung
- Test der Schnittstellen

6.3 Daten-Sammlung bei Sicherheitsprozessen (z.B. technisch und administrativ)

- Management von Konten
- Review und Genehmigung durch das Management
- Schlüsselindikatoren für Laufzeit und Risiko
- Verifizierung der Backup-Daten
- Training und Sensibilisierung
- Notfallwiederherstellungspläne and Betriebskontinuitätsmanagement

6.4 Analyse der Testergebnisse und Generierung von Berichten

6.5 Durchführung oder Unterstützung von Sicherheits-Audits

- Intern
- Extern
- Dritt-Anbieter

Fachgebiet 7: Security Operations

7.1 Verstehen und Unterstützen von Ermittlungen

- Beweissammlung und Auswertung
- Berichtswesen und Dokumentation
- Ermittlungstechniken
- Digitale forensische Werkzeuge, Taktiken und Prozeduren

7.2 Verständnis für die Anforderung der Ermittlungsfälle

- administrative Anforderungen
- strafrechtliche Anforderungen
- zivilrechtliche Anforderungen
- regulatorische Anforderungen
- Anforderungen gemäß Industriestandards

7.3 Durchführung von Protokollierungen und Überwachungsaktivitäten

- Intrusion Detection Systeme und Präventionen
- Security Information und Event Management (SIEM)
- durchgehende Überwachung
- Austrittsüberwachung

7.4 Sichere Bereitstellung von Betriebsmitteln

- Inventar der Vermögenswerte
- Management der Vermögenswerte
- Konfigurationsmanagement

7.5 Verständnis grundlegender Konzepte zum sicheren Betrieb und ihrer Anwendung

- „Need-to-know" / „least privileges"
- Trennung von Pflichten und Verantwortlichkeiten
- Management von privilegierten Konten
- Jobrotation
- Lebenszyklus von Informationen
- Service Level Agreements (SLA)

7.6 Anwendung von Techniken zum Schutz von Betriebsmitteln

- Management von Medien
- Management von Hard- und Software

7.7 Durchführung von Störfallhandlings

- Erkennung
- Reaktion
- Verringerung
- Berichtswesen
- Wiederherstellung
- Sanierung
- „Lessons learned"

7.8 Durchführung und Verwaltung von vorgelagerten und nachgelagerten Maßnahmen

- Firewalls
- „Intrusion Detection" und Präventionssystems
- „White- & Blacklists"
- Sicherheitsdienstleistung Dritter
- „Sandboxing"
- „Honeypots" und „Honeynets"
- Anti-Schadsoftware

7.9 Implementierung und Unterstützung eines Patch- und Schwachstellenmanagement

7.10 Verständnis und Beteiligung an einem Change Management Prozess

7.11 Implementierung eines Wiederherstellungsstrategie

- Strategien beim Speicher-Backup
- Strategien bei der Wiederherstellung von Standorten
- Standortübergreifende Prozesse
- Belastbarkeit von Systemen, Hochverfügbarkeit, „Quality of Service" (QoS) und Fehlertoleranz

7.12 Installation eines Disaster Recovery (DR) Prozesses

- Antwort
- Personal
- Kommunikation
- Einschätzung
- Wiederaufbau
- Training und Sensibilisierung

7.13 Test eines Disaster Recovery Plans (DRP)

- „Readthrough"
- „Walkthrough"
- Simulation
- Paralleler Betrieb
- Abschaltung

7.14 Teilnahme an Planungen und Übungen zum Betriebskontinuitätsmanagement

7.15 Implementierung und Verwaltung physikalischer Sicherheit

- Sicherheitskontrollen für den Umkreis
- Interne Sicherheitskontrollen

7.16 Adressieren von Bedenken des persönlichen Schutzes und der persönlichen Sicherheit

- bei Reisen
- Sicherheitstraining und Sensibilisierung
- Notfall Management
- bei Nötigung

Fachgebiet 8: Software Development Security

8.1 Verständnis von Sicherheit im Software Entwicklungsprozess (SDLC) und ihre Integration

- Entwicklungsmethoden
- Reifegradmodell (Maturity Model)
- Durchführung und Wartung
- Change Management
- Integrierte Produktteams

8.2 Identifizierung und Anwendung von Sicherheitskontrollen in Entwicklungsumgebungen

- Sicherheit der Software-Umgebungen
- Konfigurationsmanagement als Komponente von sicherem Kodieren
- Sicherheit von digitalen Archiven für Softwarecode

8.3 Überprüfung der Effektivität von Software-Sicherheit

- Prüfung und Protokollierung von Änderungen
- Risikoanalyse und Risikominimierung

8.4 Bewertung der Sicherheitsauswirkung bei zugekaufter Software

8.5 Definition und Anwendung von Richtlinien und Standards für sicheres Kodieren

- Sicherheitslücken und Schwachstellen auf Source-Code-Niveau
- Sicherheit bei der Programmierung der Anwendungsschnittstellen
- Sicherheitspraktiken beim Kodieren

Weitere Informationen zur Prüfung

Weitergehende Referenzen

Kandidaten sind aufgefordert, ihr Wissen und ihre Erfahrung fortwährend zu erweitern. Dies durch die Sichtung weiterer – die CBKs betreffenden – Quellen, um zusätzliche Themenbereiche zu identifizieren, die zusätzlicher Aufmerksamkeit bedürfen.

Eine vollständige Liste weitergehender Referenzen ist verfügbar unter: www.isc2.org/certifications/References.

Richtlinien und Prozeduren der Prüfung

(ISC)² empfiehlt, daß CISSP Kandidaten die Prüfungsrichtlinien und Prozeduren vor der Registrierung durcharbeiten. Das Lesen der zusammenfassenden Analyse ist wichtig und diese ist verfügbar unter: www.isc2.org/Register-for-Exam.

Rechtliche Informationen

Für jegliche Fragen zu den (ISC)²'s rechtlichen Richtlinien, kontaktieren Sie bitte das (ISC)² Legal Department unter legal@isc2.org.

Fragen?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org