



**Certified Information
Systems Security Professional**

ISC2 Certification

Prüfungsübersicht: Zertifizierung

Datum des Inkrafttretens: 15. April 2027



ISC2



Über CISSP

Der Zertifizierte Sicherheitsexperte für Informationssysteme (CISSP) ist die weltweit anerkannteste Zertifizierung auf dem Markt für Informationssicherheit. Der CISSP bescheinigt Fachleuten für Informationssicherheit fundierte technische und betriebswirtschaftliche Kenntnisse und Erfahrungen, die sie in die Lage versetzen, den gesamten Sicherheitsstatus einer Organisation effektiv zu entwerfen, zu entwickeln und zu verwalten.

Das breite Spektrum an Themen, das in der CISSP-Prüfungsübersicht enthalten ist, gewährleistet deren Relevanz für alle Fachbereiche im Bereich der Informationssicherheit. Erfolgreiche Bewerber verfügen über Kompetenzen in den folgenden acht Bereichen:

- Sicherheits-Governance und Risikomanagement
- Asset-Sicherheit
- Sicherheitsarchitektur und Ingenieurtechnik
- Kommunikations- und Netzwerksicherheit
- Identitäts- und Zugriffsmanagement (IAM)
- Sicherheitsbewertung und -tests
- Sicherheitsoperationen
- Software-Entwicklungs-Sicherheit

Anforderungen an die Erfahrung

Die Kandidaten müssen mindestens fünf Jahre kumulierte Vollzeit-Erfahrung in zwei oder mehr der acht Bereiche des aktuellen CISSP-Prüfungsschemas haben. Ein Universitätsabschluss (Bachelor oder Master) in Informatik, Informationstechnologie (IT) oder verwandten Bereichen kann bis zu einem Jahr der geforderten Erfahrung ausmachen oder ein zusätzlicher Nachweis aus der vom ISC2 genehmigten Liste kann bis zu einem Jahr der geforderten Erfahrung ausmachen. Es kann nur ein Jahr Berufserfahrung erlassen werden. Teilzeitarbeit und Praktika können ebenfalls auf die Erfahrungsanforderungen angerechnet werden.

Ein Kandidat, der nicht über die erforderliche Erfahrung verfügt, um ein CISSP zu werden, kann ein Mitglied von ISC2 werden, indem er die CISSP-Prüfung erfolgreich ablegt. Das ISC2-Mitglied hat dann sechs Jahre Zeit, um die erforderlichen fünf Jahre Erfahrung zu sammeln. Weitere Informationen zu den Anforderungen an die CISSP-Erfahrung und zur Anrechnung von Teilzeitarbeit und Praktika finden Sie unter www.isc2.org/Certifications/CISSP/experience-requirements.

Akkreditierung

CISSP war die erste Zertifizierung im Bereich der Informationssicherheit, die die strengen Anforderungen der ANSI National Accreditation Board (ANAB) gemäß der Norm ISO/IEC 17024 erfüllte.

Job-Task-Analyse (JTA)

ISC2 ist gegenüber seinen Mitgliedern verpflichtet, die Relevanz des CISSP aufrechtzuerhalten. Die Job-Task-Analyse (JTA), die in regelmäßigen Abständen durchgeführt wird, ist ein methodischer und kritischer Prozess zur Ermittlung der Aufgaben, die von Sicherheitsfachkräften ausgeführt werden, die in dem vom CISSP definierten Beruf tätig sind. Die Ergebnisse der JTA werden zur Aktualisierung der Prüfung verwendet. Dieses Verfahren stellt sicher, dass die Kandidaten in den Themenbereichen geprüft werden, die für die Aufgaben und Verantwortlichkeiten der heutigen Informationssicherheitsexperten relevant sind.



Informationen zur CISSP-CAT-Prüfung

Bei der CISSP-Prüfung wird für alle Prüfungen in Englisch, Deutsch, Spanisch-Modern, Japanisch und vereinfachtem Chinesisch das Computerized Adaptive Testing (CAT) eingesetzt. Du kannst mehr über CISSP CAT unter www.isc2.org/certifications/CISSP-CAT erfahren.

Dauer der Prüfung	3 Stunden
Anzahl der Fragen	100–150
Fragenformat	Multiple-Choice-Fragen und fortgeschrittene Aufgabentypen
Punktzahl zum Bestehen	700 von 1000 Punkten
Verfügbare Prüfungssprachen	Chinesisch, Englisch, Deutsch, Japanisch, Spanisch
Testzentrum	Von ISC2 autorisierte PPC- und PVTC-Auswahl-Prüfungszentren von Pearson

CCSP-CAT-Prüfungsgewichtungen

Bereiche	Durchschn. Gewichtung
1. Sicherheits-Governance und Risikomanagement	13,6 %
2. Asset-Sicherheit	12 %
3. Sicherheitsarchitektur und Ingenieurtechnik	12,8 %
4. Kommunikations- und Netzwerksicherheit	12,8 %
5. Identitäts- und Zugriffsmanagement (IAM)	13,6 %
6. Sicherheitsbewertung und -tests	11,2 %
7. Sicherheitsmaßnahmen	12,8 %
8. Software-Entwicklungs-Sicherheit	11,2 %
Gesamt:	100 %



Bereich 1: Sicherheits-Governance und Risikomanagement

1.1 Verstehen, Befolgen und Fördern der Berufsethik

- » ISC2-Berufsethikkodex
- » Organisatorischer Ethikkodex
- » Ethik im Bereich der Künstlichen Intelligenz (KI)

1.2 Verstehen und Anwenden von Sicherheitskonzepten

- » Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nichtabstreitbarkeit

1.3 Prinzipien der Sicherheits-Governance evaluieren, anwenden und aufrechterhalten

- » Ausrichtung der Sicherheitsfunktion an der Unternehmensstrategie, den Zielen, dem Auftrag und den Vorhaben
- » Organisatorische Prozesse (z. B. Übernahmen, Veräußerungen, Governance-Ausschüsse)
- » Organisatorische Rollen und Verantwortlichkeiten
- » Frameworks für Sicherheitskontrollen (z. B. Internationale Organisation für Normung (ISO), Nationales Institut für Standards und Technologie (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Datensicherheitsstandard der Zahlungskartenindustrie (PCI DSS), Federal Risk and Authorization Management Program (FedRAMP))
- » Due Care und Due Diligence

1.4 Verstehen von rechtlichen, regulatorischen und Compliance-Fragen, die Informationssicherheit in einem ganzheitlichen Kontext betreffen

- » Cyberkriminalität und Datenschutzverletzungen
- » Anforderungen an Lizenzen und geistiges Eigentum
- » Steuerung von Import/Export
- » Grenzüberschreitender Datenfluss
- » Fragen zum Datenschutz (z. B. die Datenschutz-Grundverordnung (DSGVO), der California Consumer Privacy Act, das Gesetz zum Schutz personenbezogener Daten, das Gesetz zum Schutz personenbezogener Informationen, der Health Insurance Portability and Accountability Act (HIPAA))
- » Vertragliche, rechtliche, branchenübliche und regulatorische Anforderungen

1.5 Verstehen der Anforderungen für die verschiedenen Arten von Ermittlungen (z. B. verwaltungsrechtliche, strafrechtliche, zivilrechtliche, behördliche)

1.6 Entwicklung, Dokumentation und Umsetzung von Sicherheitsrichtlinien, Standards, Verfahren und Leitlinien

1.7 Identifizieren, Analysieren, Bewerten, Priorisieren und Implementieren von Geschäftskontinuitätsanforderungen

- » Business-Impact-Analyse (BIA)
- » Externe Abhängigkeiten

1.8 Mitwirkung an der Entwicklung und Durchsetzung von Richtlinien und Verfahren zur Personalsicherheit

- » Auswahl und Einstellung von Bewerbern
- » Arbeitsverträge und richtlinienbezogene Anforderungen
- » Einführungs-, Versetzungs- und Kündigungsprozesse
- » Vereinbarungen und Kontrollen für Anbieter, Berater und Auftragnehmer (z. B. Service-Level Agreements (SLA))

1.9 Verstehen und Anwenden von Risikomanagementkonzepten

- » Identifikation von Bedrohungen und Schwachstellen
- » Risikoanalyse, -bewertung und -umfang
- » Risikoreaktion und -behandlung (z. B. Cybersecurity-Versicherung, Risikominderungsstrategien)
- » Anwendbare Arten von Kontrollen (z. B. präventiv, aufdeckend, korrigierend)
- » Kontrollbewertungen (z. B. Sicherheit und Datenschutz)
- » Kontinuierliche Überwachung und Messung
- » Berichterstattung (z. B. intern, extern)
- » Kontinuierliche Verbesserung (z. B. Modellierung der Reife)
- » Risikorahmenwerke (z. B. Internationale Organisation für Normung (ISO), National Institute of Standards and Technology (NIST), Steuerungsvorgaben für die Informationstechnologie und damit verbundene Technologien (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI), The Health Insurance Portability and Accountability Act (HIPAA))

1.10 Verstehen und Anwenden von Konzepten und Methoden zur Bedrohungsmodellierung

1.11 Anwendung von Konzepten des Supply-Chain-Risikomanagements (SCRM)

- » Risiken im Zusammenhang mit dem Erwerb von Produkten und Dienstleistungen von Lieferanten und Anbietern (z. B. Produktmanipulation, Fälschungen, Implantate, Reputationsrisiken)
- » Risikominderung (z. B. Bewertung und Überwachung durch Dritte, Mindestsicherheitsanforderungen, Dienstleistungsvereinbarungsanforderungen, Silicon Root of Trust, physisch nicht zuordenbare Funktion, Software-Stückliste)

1.12 Einrichtung, Pflege und Bewertung eines Programms zur Sensibilisierung, Aufklärung und Schulung im Bereich Sicherheit

- » Methoden und Techniken zur Steigerung des Sicherheitsbewusstseins und zur Schulung (z. B. Sicherheitsbeauftragte, Gamifizierung)
- » Regelmäßige inhaltliche Überprüfung, um neue Technologien und Trends (z. B. Kryptowährung, künstliche Intelligenz (KI), Blockchain) zu berücksichtigen
- » Evaluierung der Programmwirksamkeit und Einbindung der Stakeholder



Bereich 2: Asset-Sicherheit

2.1 Identifizierung und Klassifizierung von Informationen und Assets

- » Datenklassifizierung
- » Asset-Klassifizierung

2.2 Festlegung der Anforderungen für den Umgang mit Informationen und Assets

- » Physisch
- » Digital/elektronisch
- » Sichere Medienvernichtung
- » Datenverschlüsselung (z. B. ruhende Daten, in Übertragung/in Bewegung)

2.3 Sicheres Bereitstellen von Informationen und Assets

- » Eigentum von Informationen und Assets
- » Asset-Inventar (z. B. materiell, immateriell)
- » Asset-Management

2.4 Verwaltung des Lebenszyklus von Daten

- » Datenmanagement-Richtlinie
- » Datenrollen (z. B. Eigentümer, Verantwortliche, Verwahrer, Verarbeiter, Nutzer)
- » Datenerhebung
- » Standort der Daten
- » Datenpflege
- » Datenaufbewahrung
- » Datenremanenz
- » Datenvernichtung

2.5 Sorgen Sie für eine angemessene Verwaltung von Assets (z. B. „End of Life“ (EOL), „End of Support“ (EOS))

- » Asset-Management-Richtlinie
- » Asset-Aufbewahrung
- » Asset-Außerbetriebnahme

2.6 Festlegen von Datensicherheitskontrollen und Compliance-Anforderungen

- » Datenzustände (z. B. in Gebrauch, in Übertragung, im Ruhezustand)
- » Scoping und Anpassung
- » Auswahl von Standards und Kontrollen
- » Datenschutzmethoden (z. B. Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB)), Cloud-Native Application Protection Platform (CNAPP))



Bereich 3: Sicherheitsarchitektur und Ingenieurtechnik

3.1 Erforschung, Implementierung und Verwaltung von technischen Prozessen unter Anwendung der Grundsätze des sicheren Entwurfs

- » Bedrohungsmodellierung
- » Prinzip des geringsten Privilegs (Principle of Least privilege, PoLP)
- » Verteidigung in der Tiefe (Defense in Depth, DiD)
- » Sichere Standardeinstellungen
- » Sicher ausfallen
- » Aufgabentrennung (Separation of Duties, SoD)
- » Der Grundsatz „Einfach und klein halten“
- » Zero Trust (ZT)
- » Privacy by Design (z. B. datenschutzfördernde Technologien)
- » Geteilte Verantwortung
- » Secure Access Service Edge (SASE)
- » Well-Architected Framework
- » Aufgabenrotation
- » Zwei-Personen-Integrität

3.2 Verstehen der grundlegenden Konzepte von Sicherheitsmodellen (z. B. Biba, Star, Bell-LaPadula)

3.3 Auswahl der Kontrollen anhand der Sicherheitsanforderungen des Systems

3.4 Verstehen der Sicherheitsfunktionen von Informationssystemen (z. B. Speicherschutz, Trusted Platform Module (TPM), Hardware Security Module (HSM), Ver- und Entschlüsselung)

3.5 Bewerten und entschärfen der Schwachstellen von Sicherheitsarchitekturen, Entwürfen und Lösungselementen

- » Clientbasierte Systeme
- » Serverbasierte Systeme
- » Datenbank-Systeme
- » Kryptografische Systeme
- » Betriebstechnik (BT) und industrielle Steuerungssysteme (ICS)
- » Cloud-basierte Systeme (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS), serverlos, Funktion als Service (FaaS))
- » Verteilte Systeme
- » Internet der Dinge (IoT)
- » Microservices und Containerisierung
- » Eingebettete Systeme
- » Hochleistungsrechnersysteme
- » Edge-Computing-Systeme
- » Virtualisierte Systeme
- » Lieferkettenrisiko
- » Autonome Systeme
- » Quantencomputing

3.6 Auswahl und Festlegung kryptografischer Lösungen

- » Kryptographischer Lebenszyklus (z. B. Schlüssel, Auswahl von Algorithmen)
- » Kryptografische Verfahren (z. B. symmetrisch, asymmetrisch, elliptische Kurven, Quanten)
- » Public-Key-Infrastruktur (PKI) (z. B. Schlüsselverteilung)
- » Praktiken des Schlüsselmanagements (z. B. Rotation, Zugriffsverwaltung)
- » Digitale Signaturen und digitale Zertifikate (z. B. Nichtabstreitbarkeit, Integrität)

3.7 Verstehen der Methoden kryptoanalytischer Angriffe

- » Brute Force
- » Nur Chiffretext
- » Bekannter Klartext
- » Frequenzanalyse
- » Gewählter Chiffretext
- » Implementierungsangriffe
- » Seitenkanal
- » Fehlerinjektion
- » Timing
- » Mittelsmann-Angriff (Man-in-the-Middle, MITM)
- » Pass the Hash
- » Kerberos-Ausnutzung
- » Ransomware
- » Zero-Day-Angriffe
- » Bedrohungen durch künstliche Intelligenz (KI) (z. B. adversarische KI, Vergiftung von KI-Modellen, Deepfake-Angriffe)

3.8 Anwendung von Sicherheitsprinzipien beim Entwurf von Standorten und Einrichtungen

3.9 Entwurf von Sicherheitskontrollen für Standorte und Einrichtungen

- » Verteilerkästen/Zwischenverteiler
- » Serverräume/Rec
- » Medienspeichereinrichtungen
- » Beweissicherung
- » Sicherheit im Sperrbereich und im Arbeitsbereich
- » Versorgung und Heizung, Lüftung und Klimatisierung (HVAC)
- » Umweltprobleme (z. B. Naturkatastrophen, vom Menschen verursachte)
- » Brandverhütung, -erkennung und -bekämpfung
- » Stromversorgung (z. B. redundant, Backup)

3.10 Verwalten des Lebenszyklus des Informationssystems

- » Bedürfnisse und Anforderungen der Stakeholder
- » Analyse der Anforderungen
- » Sicherer architektonischer Entwurf
- » Entwicklung/Implementierung
- » Integration
- » Verifizierung und Validierung
- » Kontinuierliche Sicherheitsüberprüfung
- » Übergang/Bereitstellung
- » Betrieb und Instandhaltung/Nachhaltigkeit
- » Außerbetriebnahme/sichere Entsorgung



Bereich 4: Kommunikations- und Netzwerksicherheit

4.1 Anwendung sicherer Entwurfsprinzipien in Netzwerkarchitekturen

- » Open System Interconnection (OSI) und Transmission Control Protocol/Internet Protocol (TCP/IP) Modelle
- » IP-Version 4 und 6 (IPv4) (z. B. Unicast, Broadcast, Multicast, Anycast)
- » Sichere Protokolle (z. B. Internet Protocol Security (IPSec), Secure Shell (SSH), Secure Sockets Layer (SSL)/Transport Layer Security (TLS))
- » Auswirkungen von Mehrschichtprotokollen
- » Konvergente Protokolle (z. B. Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP), InfiniBand over Ethernet, Compute Express Link)
- » Transportarchitektur (z. B. Topologie, Daten-/Kontroll-/Verwaltungsebene, Cut-Through/Shore-and-Forward)
- » Kennzahlen zur Performance (z. B. Bandbreite, Latenz, Jitter, Durchsatz, Signal-Rausch-Verhältnis)
- » Trafficströme (z. B. Nord-Süd, Ost-West)
- » Physikalische Segmentierung (z. B. In-Band, Out-of-Band, Air-Gapped)
- » Logische Segmentierung (z. B. virtuelle lokale Netzwerke (VLANs), virtuelle private Netzwerke (VPNs), virtuelles Routing und Weiterleitung, virtueller Bereich)
- » Mikrosegmentierung (z. B. Netzwerk-Overlays/Einkapselung; verteilte Firewalls, Router, Intrusion Detection System (IDS) und Angreiferkennungssystem (IPS), Zero Trust)
- » Edge-Netzwerke (z. B. Ingress/Egress, Peering)
- » Drahtlose Netzwerke (z. B. Bluetooth, Wi-Fi, Zigbee, Satellit)
- » Mobilfunknetze (z. B. 4G, 5G)
- » Netzwerke für die Bereitstellung von Inhalten (Content Delivery Networks, CDN)
- » Software-definierte Netzwerke (SDN), (z. B. Programmierschnittstelle (API), Software-definiertes Wide-Area-Netzwerk (SDWAN), Network Functions Virtualization)
- » Virtuelle private Cloud (VPC)
- » Überwachung und Management (z. B. Beobachtbarkeit des Netzes, Traffic-Fluss/Shaping, Kapazitätsmanagement, Fehlererkennung und -behandlung)
- » Software-definierte Sicherheit

4.2 Sichern von Netzwerkkomponenten

- | | |
|---|--|
| <ul style="list-style-type: none"> » Betrieb der Infrastruktur (z. B. redundante Stromversorgung, Garantie, Support) » Übertragungsmedien (z. B. physische Sicherheit der Medien, Qualität der Signalausbreitung) | <ul style="list-style-type: none"> » Netzwerkzugriffskontrollsysteme (NAC) (z. B. physische und virtuelle Lösungen) » Endpunktsicherheit (z. B. hostbasiert) |
|---|--|

4.3 Implementierung von sicheren Kommunikationskanälen gemäß dem Entwurf

- | | |
|--|---|
| <ul style="list-style-type: none"> » Sprache, Video und Zusammenarbeit (z. B. Konferenzen, Video-Meeting-Räume) » Fernzugriff (z. B. Netzwerkverwaltungsfunktionen, Remote-Arbeit) | <ul style="list-style-type: none"> » Datenkommunikation (z. B. Backhaul-Netze, Satellit) » Konnektivität mit Dritten (z. B. Telekommunikationsanbieter, Hardware-Support) |
|--|---|



Bereich 5: Identitäts- und Zugriffsmanagement (IAM)

5.1 Verwaltung des physischen und logischen Zugriffs auf Assets (z. B. Bereitstellung, Steuerung, Überprüfung, Widerruf)

- » Informationen
- » Systeme
- » Geräte
- » Einrichtungen
- » Anwendungen
- » Dienste
- » Identitäten

5.2 Entwurf einer Identifizierungs- und Authentifizierungsstrategie (z. B. für Menschen, Geräte und Dienste)

- » Gruppen und Rollen
- » Authentifizierung, Autorisierung und Buchhaltung (Authentication, Authorization, Accounting, AAA)
- » Sitzungsmanagement
- » Registrierung, Nachweis und Feststellung der Identität
- » Verbundidentitätsmanagement (FIM)
- » Systeme zur Verwaltung von Anmeldeinformationen (z. B. Password Vault)
- » Einmalige Anmeldung (Single sign-on, SSO)
- » Just-In-Time
- » Kennwortlose Authentifizierung (z. B. Fast Identity Online (FIDO), WebAuthn, Passkeys, Biometrie)

5.3 Verbundidentität mit einem Dienst eines Drittanbieters

- » Vor-Ort
- » Cloud
- » Hybrid

5.4 Implementierung und Verwaltung von Autorisierungsmechanismen

- » Rollenbasierte Zugriffskontrolle (Role-based Access Control, RBAC)
- » Regelbasierte Zugriffskontrolle (Rule-based Access Control, RuBAC)
- » Zwingend erforderliche Zugriffskontrolle (Mandatory Access Control, MAC)
- » Benutzerbestimmbare Zugriffskontrolle
- (Discretionary Access Control, DAC)
- » Attributbasierte Zugriffskontrolle (Attribute-based access control, ABAC)
- » Risikoadaptive Zugriffskontrolle (Risk-Adaptable Access Control, RAdAC)
- » Durchsetzung der Zugangsrichtlinie (z. B. Entscheidungspunkt, Durchsetzungspunkt)

5.5 Verwaltung des Lebenszyklus der Identitäts- und Zugriffsbereitstellung

- » Überprüfung des Kontozugriffs (z. B. Nutzer, System, Dienst)
- » Provisionierung und Deprovisionierung (z. B. On-/Offboarding und Versetzungen)
- » Rollendefinition und Übergang (z. B. Personen, die neuen Rollen zugewiesen werden)
- » Erweiterung von Berechtigungen (z. B. Nutzung von Administratorgruppen/sudo, Überwachung der Nutzung, Prinzip des geringsten Privilegs (Principle of Least Privilege, PoLP))
- » Verwaltung von Servicekonten

5.6 Implementierung von Authentifizierungs- und Autorisierungssystemen



Bereich 6: Sicherheitsbewertung und -tests

6.1 Entwurf und Validierung von Bewertungs-, Test- und Auditstrategien

- » Intern (z. B. innerhalb der Kontrolle der Organisation)
- » Extern (z. B. außerhalb der Kontrolle der Organisation)
- » Drittanbieter (z. B. außerhalb der Kontrolle des Unternehmens)
- » Standort (z. B. vor Ort, in der Cloud, hybrid)

6.2 Durchführung von Sicherheitskontrolltests

- » Schwachstellenbewertung
- » Penetrationstests
- » Log-Bewertungen
- » Synthetische Transaktionen/Benchmarks
- » Codeüberprüfung und -test
- » Testen von Missbrauchsfällen
- » Analyse der Abdeckung
- » Schnittstellentests (z. B. Benutzeroberfläche, Netzwerkschnittstelle, Programmierschnittstelle (API))
- » Angriffssimulationen
- » Compliance-Kontrollen

6.3 Sammlung von Sicherheitsprozessdaten (z. B. technische und administrative)

- » Kontoverwaltung
- » Überprüfung und Genehmigung durch das Management
- » Wichtige Performance- und Risikoindikatoren
- » Sicherung der Verifikationsdaten
- » Schulung und Bewusstsein
- » Notfallwiederherstellung (Disaster Recovery, DR) und Business Continuity (BC)

6.4 Analyse der Test-/Audit-Ergebnisse und Erstellung eines Berichts

- » Abhilfe
- » Behandlung von Ausnahmen
- » Verantwortungsvolle Offenlegung

6.5 Durchführung oder Unterstützung von Sicherheitsaudits

- » Intern (z. B. innerhalb der Kontrolle der Organisation)
- » Extern (z. B. außerhalb der Kontrolle der Organisation)
- » Drittanbieter (z. B. außerhalb der Kontrolle des Unternehmens)
- » Standort (z. B. vor Ort, in der Cloud, hybrid)



Bereich 7: Sicherheitsoperationen

7.1 Verstehen und Befolgen von Untersuchungen

- » Sammlung und Handhabung von Beweisen
- » Ermittlungsmethoden
- » Berichterstattung und Dokumentation
- » Werkzeuge, Taktiken und Verfahren der digitalen Forensik
- » Artefakte (z. B. Daten, Computer, Netzwerk, Mobilgerät)

7.2 Durchführung von Protokollierungs- und Überwachungsaktivitäten

- » Intrusion Detection and Prevention (IDPS)
- » Sicherheitsinformationen und Ereignisverwaltung (SIEM)
- » Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR)
- » Kontinuierliche Überwachung und Optimierung
- » Egress-Monitoring (z. B. Verhinderung von Datenverlust (Data loss prevention, DLP))
- » Log-Verwaltung
- » Bedrohungsdaten (z. B. Threat Feeds, Threat Hunting)
- » Analyse des Benutzer- und Entitätsverhaltens (UEBA)

7.3 Durchführung von Konfigurationsmanagement (Configuration Management, CM) (z. B. Provisioning, Baselining, Automatisierung)

7.4 Anwenden grundlegender Konzepte des Sicherheitsbetriebs (z. B. Verteidigung in der Tiefe (Defense in Depth, DiD))

- » Kenntnis nur bei Bedarf/geringstes Privileg
- » Aufgabentrennung (Separation of Duties, SoD) und Verantwortlichkeiten
- » Verwaltung von privilegierten Konten
- » Job-Rotation

7.5 Anwendung des Ressourcenschutzes

- » Medienverwaltung
- » Techniken zum Schutz von Medien (z. B. Archivierung, Verschlüsselung, Entsorgung/Wiederverwendung)
- » Datenzustände (z. B. in Gebrauch, in Übertragung, im Ruhezustand)

7.6 Durchführung des Managements von Zwischenfällen

- » Erkennung
- » Antwort
- » Abmilderung
- » Berichterstattung
- » Wiederherstellung
- » Abhilfe
- » Gewonnene Erkenntnisse

7.7 Durchführung und Wartung von Erkennungs- und Präventionsmaßnahmen

- » Firewalls (z. B. Next Generation, Webanwendung, Netzwerk)
- » Intrusion Detection System (IDS) und Angreiferkennungssystem (IPS)
- » Allowlist/Denylist
- » Von Drittanbietern bereitgestellte Sicherheitsdienste (z. B. Distributed-Denial-of-Service (DDoS)-Scrubbing-Dienste, Managed Security Service Provider)
- » Sandboxing
- » Honeypots/Honeynets
- » Endpunktschutz (z. B. Anti-Malware, Endpunkterkennung und -antwort (EDR), Extended Detection and Response (XDR))
- » Auf maschinellem Lernen (ML) und künstlicher Intelligenz (KI) basierende Tools

7.8 Implementierung und Unterstützung von Patch- und Schwachstellenmanagement

7.9 Verstehen und Mitwirken bei Veränderungsprozessen

7.10 Umsetzung von Wiederherstellungsstrategien

- » Strategien für die Datensicherung (z. B. Cloud-Speicher, vor Ort, extern, unveränderlich, verschlüsselt)
- » Strategien für Wiederherstellungsstandorte (z. B. „Cold“ vs. „Warm“ vs. „Hot“, Vereinbarungen über die Ressourcenkapazität)
- » Mehrere Verarbeitungsstandorte
- » Systemausfallsicherheit, Hochverfügbarkeit (HV), Servicequalität (QoS) und Fehlertoleranz

7.11 Implementierung von Notfallwiederherstellungsprozessen (Disaster Recovery, DR)

- » Antwort
- » Personal
- » Kommunikation (z. B. Methoden, Priorisierung)
- » Bewertung
- » Wiederherstellung
- » Schulung und Bewusstsein
- » Gewonnene Erkenntnisse
- » Metriken (z. B. Baseline, Mittlere Zeit bis zur Behebung)
- » (MTTR, mittlere Zeit zwischen Ausfällen (MTBF))

7.12 Test von Notfallwiederherstellungsplänen (DRP)

- » Read-through/Tabletop
- » Walkthrough
- » Read-through/tabletop
- » Parallele vollständige Unterbrechung
- » Kommunikation (z. B. intern/extern)

7.13 Teilnahme an Business Continuity (BC)-Planung und Übungen

7.14 Implementierung und Verwaltung der physischen Sicherheit

- » Externe Sicherheitskontrollen
- » Interne Sicherheitskontrollen

7.15 Implementierung und Verwaltung der physischen Sicherheit

- » Reisen
- » Schulungen und Sensibilisierung im Bereich Sicherheit
- » Notfallmanagement
- » Bedrohung



Bereich 8: Software-Entwicklungs-Sicherheit

8.1 Verstehen und Integrieren von Sicherheit in den Software Development Life Cycle (SDLC)

- » Entwicklungsmethoden (z. B. Agile, Wasserfall, DevOps, DevSecOps, Scaled Agile Framework)
- » Reifegradmodelle (z. B. Reifegradmodell (Capability Maturity Model, CMM), Software Assurance Maturity Model (SAMM))
- » Betrieb und Wartung
- » Änderungsmanagement
- » Integriertes Produkt-Team
- » Anforderungen an das Secure Software Development Framework (SSDF) und die Software Bill of Materials (SBOM)
- » Shift-Left (Vorziehen von Sicherheitstests)

8.2 Identifizieren und Anwenden von Sicherheitskontrollen in Ökosystemen der Softwareentwicklung

- » Programmiersprachen (z. B. speichersicher, objektorientiert)
- » Bibliotheken
- » Toolsets
- » Integrierte Entwicklungsumgebung
- » Laufzeit
- » Kontinuierliche Integration und kontinuierliche Lieferung (CI/CD)
- » Softwarekonfigurationsmanagement (CM)
- » Code-Repositories
- » Anwendungssicherheitstests (z. B. Statische Anwendungssicherheitstests (Static Application Security Testing, SAST), Sicherheitstests für dynamische Anwendungen (Dynamic Application Security Testing, DAST))

8.3 Bewertung der Wirksamkeit der Softwaresicherheit

- » Auditierung und Protokollierung von Änderungen
- » Risikoanalyse und -minderung

8.4 Bewertung der Sicherheitsauswirkungen erworbener Software

- » Kommerzielle Standardtechnik (Commercial-off-the-shelf, COTS)
- » Open Source (z. B. Softwarezusammenstellungsanalyse (Software Composition Analysis, SCA))
- » Drittanbieter
- » Verwaltete Services (z. B. Unternehmensanwendungen)
- » Cloud-Services (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS), Funktion als Service (FaaS))

8.5 Definition und Anwendung von Richtlinien und Standards für sichere Kodierung

- » Sicherheitslücken und Schwachstellen auf Quellcode-Ebene
- » Sicherheit von Programmierschnittstellen (APIs)
- » Sichere Kodierungspraktiken



Zusätzliche Informationen zur Prüfung

Ergänzende Referenzen

Den Kandidaten wird empfohlen, ihre Ausbildung und Erfahrung zu ergänzen, indem sie relevante Materialien zum Prüfungsleitfaden für die CISSP-Prüfung durcharbeiten und Lernbereiche ermitteln, die möglicherweise besonderer Aufmerksamkeit bedürfen.

Die vollständige Liste der ergänzenden Referenzen finden Sie unter www.isc2.org/certifications/References.

Prüfungsrichtlinien und -verfahren

ISC2 empfiehlt den Kandidaten, die Prüfungsrichtlinien und -verfahren zu lesen, bevor sie sich für die Prüfung anmelden. Lesen Sie die umfassende Übersicht über diese wichtigen Informationen unter www.isc2.org/Register-for-Exam.

Rechtliche Informationen

Bei Fragen zu den rechtlichen [Richtlinien von ISC2](#) wenden Sie sich bitte an die Rechtsabteilung von ISC2 unter legal@isc2.org.

Haben Sie noch Fragen?

Wenden Sie sich an den ISC2-Kandidatenservice in Ihrer Region:

Nord- und Südamerika

Tel: +1.866.331.ISC2 (4722), drücken Sie 1

E-Mail: membersupport@isc2.org

Asien-Pazifik

Tel: +(852) 5803-5662

E-Mail: isc2asia@isc2.org

Europa, Naher Osten und Afrika

Tel: +44 203-960-7800

E-Mail: info-emea@isc2.org