CISSP®

Certified Information Systems Security Professional

ISC2 Certification

Zertifizierungs-**Prüfungsübersicht**

Datum des Inkrafttretens: 15. April 2024

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 der Themen, die im CISSP-Wissenskorpus enthalten sind, stellt sicher, dass es für alle Disziplinen im Bereich der Informationssicherheit relevant ist. Erfolgreiche Bewerber verfügen über Kompetenzen in den folgenden acht Bereichen:

- Sicherheit 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. 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 der erste Abschluss im Bereich der Informationssicherheit, der die strengen Anforderungen der ANSI/ISO/IEC-Norm 17024 erfüllt.

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/certificatons/CISSP-CAT erfahren.

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

CCSP-CAT-Prüfungsgewichtungen

Bereiche	Durchschnittliche Gewichtung
1. Sicherheit und Risikomanagement	16 %
2. Asset-Sicherheit	10 %
3. Sicherheitsarchitektur und Ingenieurtechnik	13 %
4. Kommunikations- und Netzwerksicherheit	13 %
5. Identitäts- und Zugriffsmanagement (IAM)	13 %
6. Sicherheitsbewertung und -tests	12 %
7. Sicherheitsoperationen	13 %
8. Software-Entwicklungs-Sicherheit	10 %
Gesamt:	**100 %**

Bereich 1: Sicherheit und Risikomanagement

1.1 Verstehen, Befolgen und Fördern der Berufsethik

- ISC2-Berufsethikkodex
- Organisatorischer Ethikkodex

1.2 Verstehen und Anwenden von Sicherheitskonzepten

- Vertraulichkeit, Integrität und Verfügbarkeit, Authentizität und Nichtabstreitbarkeit (5 Säulen der Informationssicherheit)

1.3 Bewertung und Anwendung von Grundsätzen der Sicherheits-Governance

- 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
- Rahmenwerke für Sicherheitskontrollen (z. B. Internationale Organisation für Normung (ISO), National Institute of Standards and Technology (NIST), Control Steuerungsvorgabe für die Informationstechnologie und damit verbundenen Technologien (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP))
- Sorgfaltspflicht/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
- Themen im Zusammenhang mit dem Datenschutz (z. B. Datenschutz-Grundverordnung (DSGVO), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act)
- Vertragliche, rechtliche, branchenübliche und regulatorische Anforderungen

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

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 mit Lieferanten, Beratern und Auftragnehmern

1.9 Verstehen und Anwenden von Risikomanagementkonzepten

- Identifikation von Bedrohungen und Schwachstellen
- Risikoanalyse, -bewertung und -umfang
- Risikobewältigung und -behandlung (z. B. Cybersicherheitsversicherung)
- 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 Risikoreife)
- 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))

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. Produktmanipulationen, Fälschungen, Implantate)
- Risikominderung (z. B. Bewertung und Überwachung durch Dritte, Mindestsicherheitsanforderungen, Dienstleistungsvereinbarungsanforderungen, Silicon Root of Trust, physisch nicht zuordenbare Funktion, Software-Stückliste)

1.12 Einrichtung und Aufrechterhaltung eines Programms zur Sensibilisierung, Ausbildung und Schulung in Sachen Sicherheit

- Methoden und Techniken zur Sensibilisierung und Schulung (z. B. Social Engineering, Phishing, Security Champions, Gamification)
- Regelmäßige inhaltliche Überprüfung, um neue Technologien und Trends (z. B. Kryptowährung, künstliche Intelligenz (KI), Blockchain) zu berücksichtigen
- Bewertung der Wirksamkeit des Programms

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

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

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

2.5 Sicherstellung einer angemessenen Aufbewahrung von Assets (z. B. End of Life (EOL), End of Support)

2.6 Festlegen von Datensicherheitskontrollen und Compliance-Anforderungen

- Datenzustände (z. B. in Gebrauch, in Übertragung, im Ruhezustand)
- Scoping und Anpassung
- Auswahl von Standards
- Datenschutzmethoden (z. B. digitales Rechtemanagement (DRM), Verhinderung von Datenverlust (DLP), Cloud Access Security Broker (CASB))

Bereich 3: Sicherheitsarchitektur und Ingenieurtechnik

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

- Bedrohungsmodellierung
- Geringstes Privileg
- Verteidigung in der Tiefe
- Sichere Standardeinstellungen
- Sicher ausfallen
- Aufgabentrennung
- Einfach und klein halten
- Zero-Trust oder Vertrauen aber Überprüfen
- Datenschutz durch Entwurf
- Geteilte Verantwortung
- Sicherer Zugang Servicekante

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

3.3 Auswahl der Kontrollen anhand der Sicherheitsanforderungen des Systems

3.4 Verstehen der Sicherheitsfunktionen von Informationssystemen (IS) (z. B. Speicherschutz, Trusted Platform Module (TPM), Verschlüsselung/Entschlüsselung)

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

- Clientbasierte Systeme
- Serverbasierte Systeme
- Datenbank-Systeme
- Kryptografische Systeme
- Industrielle Steuersysteme (ICS)
- Cloudbasierte Services (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS))
- Verteilte Systeme
- Internet der Dinge (IoT)
- Microservices (z. B. Programmierschnittstelle (API))
- Containerisierung
- Serverless
- Eingebettete Systeme
- Hochleistungsrechnersysteme
- Edge-Computing-Systeme
- Virtualisierte Systeme

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. Quantenschlüsselverteilung)
- Praktiken des Schlüsselmanagements (z. B. Rotation)
- 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

3.8 Anwendung von Sicherheitsprinzipien beim Entwurf von Standorten und Einrichtungen

3.9 Entwurf von Sicherheitskontrollen für Standorte und Einrichtungen

- Verteilerschränke/Zwischenverteileranlagen
- 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
- Architektonischer Entwurf
- Entwicklung/Implementierung
- Integration
- Verifizierung und Validierung
- Übergang/Bereitstellung
- Betrieb und Instandhaltung/Nachhaltigkeit
- Stilllegung/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
- Internet Protocol (IP) Version 4 und 6 (IPv6) (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 Angrifferkennungssystem (IPS), Zero Trust)
- Edge-Netzwerke (z. B. Ingress/Egress, Peering)
- Drahtlose Netzwerke (z. B. Bluetooth, Wi-Fi, Zigbee, Satellit)
- Mobilfunknetze (z. B. 4G, 5G)
- Content Distribution Networks (CDN)
- Software-definierte Netzwerke (SDN), (z. B. Programmierschnittstelle (API), Software-definiertes Wide-Area-Netzwerk, Network Functions Virtualization)
- Virtuelle private Cloud (VPC)
- Überwachung und Management (z. B. Beobachtbarkeit des Netzes, Traffic-Fluss/Shaping, Kapazitätsmanagement, Fehlererkennung und -behandlung)

4.2 Sichern von Netzwerkkomponenten

- Betrieb der Infrastruktur (z. B. redundante Stromversorgung, Garantie, Support)
- Übertragungsmedien (z. B. physische Sicherheit der Medien, Qualität der Signalausbreitung)
- Netzwerkzugriffskontrollsysteme (NAC) (z. B. physische und virtuelle Lösungen)
- Endpunktsicherheit (z. B. hostbasiert)

4.3 Implementierung von sicheren Kommunikationskanälen gemäß dem Entwurf

- Sprache, Video und Zusammenarbeit (z. B. Konferenzen, Zoom-Räume)
- Fernzugriff (z. B. Netzwerkverwaltungsfunktionen)
- Datenkommunikation (z. B. Backhaul-Netze, Satellit)
- Konnektivität mit Dritten (z. B. Telekommunikationsanbieter, Hardware-Support)

Bereich 5: Identitäts- und Zugriffsmanagement (IAM)

5.1 Kontrolle des physischen und logischen Zugangs zu Assets

- Informationen
- Systeme
- Geräte
- Einrichtungen
- Anwendungen
- Dienste

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

- Gruppen und Rollen
- Authentifizierung, Autorisierung und Abrechnung (AAA) (z. B. Multi-Faktor-Authentifizierung (MFA), Authentifizierung ohne Passwort)
- 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

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
- Zwingend erforderliche Zugriffskontrolle (Mandatory Access Control, MAC)
- Benutzerbestimmbare Zugriffskontrolle (Discretionary Access Control, DAC)
- Attributbasierte Zugriffskontrolle (Attribute-based access control, ABAC)
- Regelbasierte Zugriffskontrolle
- 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)
- Verwaltung von Servicekonten
- Rollendefinition und Übergang (z. B. Personen, die neuen Rollen zugewiesen werden)
- Privilegienerweiterung (z. B. Verwendung von sudo, Überprüfung der Verwendung)

5.6 Implementierung von Authentifizierungssystemen

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 (z. B. rote, blaue und/oder violette Teamübungen)
- Log-Bewertungen
- Synthetische Transaktionen/Benchmarks
- Codeüberprüfung und -test
- Testen von Missbrauchsfällen
- Analyse der Abdeckung
- Schnittstellentests (z. B. Benutzeröberfläche, Netzwerkschnittstelle, Programmierschnittstelle (API))
- Simulationen von Einbruchsversuchen
- 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 (DR) und Business Continuity (BC)

6.4 Analyse der Testergebnisse und Erstellung eines Berichts

- Abhilfe
- Behandlung von Ausnahmen
- Ethische 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
- Berichterstattung und Dokumentation
- Ermittlungsmethoden
- 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)
- Kontinuierliche Überwachung und Optimierung
- Egress-Überwachung
- Log-Verwaltung
- Bedrohungsdaten (z. B. Threat Feeds, Threat Hunting)
- Analyse des Benutzer- und Entitätsverhaltens (UEBA)

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

7.4 Anwendung grundlegender Konzepte für Sicherheitsoperationen

- Kenntnis nur bei Bedarf/geringstes Privileg
- Trennung der Aufgaben und Verantwortlichkeiten
- Verwaltung von privilegierten Konten
- Job-Rotation
- Service-Level-Vereinbarungen (SLA)

7.5 Anwendung des Ressourcenschutzes

- Medienverwaltung
- Techniken zum Schutz von Medien
- Daten im Ruhezustand/Daten in Übertragung

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 Angrifferkennungssystem (IPS)
- Whitelisting/Blacklisting
- Sicherheitsdienste von Drittanbietern
- Sandboxing
- Honeypots/Honeynets
- Anti-Malware
- Auf maschinellem Lernen 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, ausgelagert)
- Strategien für Wiederherstellungsstandorte (z. B. Cold vs. Hot, Vereinbarungen über Ressourcenkapazitäten)
- Mehrere Verarbeitungsstandorte
- Systemausfallsicherheit, Hochverfügbarkeit (HV), Servicequalität (QoS) und Fehlertoleranz

7.11 Implementierung von Notfallwiederherstellungsprozessen (DR)

- Antwort
- Personal
- Kommunikation (z. B. Methoden)
- Bewertung
- Wiederherstellung
- Schulung und Bewusstsein
- Gewonnene Erkenntnisse

7.12 Test von Notfallwiederherstellungsplänen (DRP)

- Read-through/Tabletop
- Walkthrough
- Read-through/tabletop
- Parallel
- Vollständige Unterbrechung
- Kommunikation (z. B. Stakeholder, Teststatus, Aufsichtsbehörden)

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

7.14 Implementierung und Verwaltung der physischen Sicherheit

- Sicherheitskontrollen des Perimeters
- Interne Sicherheitskontrollen

7.15 Berücksichtigung der Belange der Personalsicherheit und des Arbeitsschutzes

- Reisen
- Sicherheitsschulung und -bewusstsein (z. B. Insider-Bedrohungen, Auswirkungen sozialer Medien, Ermüdung bei der Zwei-Faktor-Authentifizierung (2FA))
- 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

8.2 Identifizieren und Anwenden von Sicherheitskontrollen in Ökosystemen der Softwareentwicklung

- Programmiersprachen
- Bibliotheken
- Toolsets
- Integrierte Entwicklungsumgebung
- Laufzeit
- Kontinuierliche Integration und kontinuierliche Lieferung (CI/CD)
- Softwarekonfigurationsmanagement (CM)
- Code-Repositories
- Prüfung der Anwendungssicherheit (z. B. statische Anwendungssicherheitstests (SAST), dynamische Anwendungssicherheitstests (DAST), Softwarezusammenstellungsanalyse, Interactive Application Security Test (IAST))

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
- Drittanbieter
- Verwaltete Services (z. B. Unternehmensanwendungen)
- Cloud-Services (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS))

8.5 Definition und Anwendung von Richtlinien und Standards für sichere Kodierung

- Sicherheitslücken und Schwachstellen auf Quellcode-Ebene
- Sicherheit von Programmierschnittstellen (API)
- Sichere Kodierungspraktiken
- Software-definierte Sicherheit

Zusätzliche Informationen zur Prüfung

Ergänzende Referenzen

Die Kandidaten werden ermutigt, ihre Ausbildung und Erfahrung zu ergänzen, indem sie relevante Ressourcen, die sich auf das CBK beziehen, durchsehen und Bereiche identifizieren, die zusätzliche Aufmerksamkeit erfordern.

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 (0)203-960-7800
E-Mail: info-emea@isc2.org

ISC2