CCSP®

Certified Cloud Security Professional

ISC2 Certification

Prüfungsübersicht für die Zertifizierung

Datum des Inkrafttretens: 1. August 2026

ISC2™

Über CCSP

ISC2 hat die Zertifizierung Certified Cloud Security Professional (CCSP) entwickelt, um sicherzustellen, dass Cloud-Sicherheitsexperten über die erforderlichen Kenntnisse, Fähigkeiten und Fertigkeiten in den Bereichen Cloud-Sicherheitsdesign, Implementierung, Architektur, Betrieb, Kontrolle und Einhaltung gesetzlicher Vorschriften verfügen. Ein CCSP wendet sein Fachwissen im Bereich der Informationssicherheit auf eine Cloud-Computing-Umgebung an und demonstriert seine Kompetenz in den Bereichen Cloud-Sicherheitsarchitektur, Design, Betrieb und Dienstorganisation.

Die in der CCSP Prüfungsübersicht enthaltenen Themen gewährleisten die Sachdienlichkeit aller Disziplinen im Bereich der Cloud-Sicherheit. Erfolgreiche Kandidaten weisen Kompetenzen in den folgenden sechs Bereichen auf:

- Cloud-Konzepte, Architektur und Design
- Sicherheit von Cloud-Daten
- Sicherheit von Cloud-Plattformen und -Infrastrukturen
- Sicherheit von Cloud-Anwendungen
- Cloud-Sicherheitsoperationen
- Recht, Risiko und Compliance

Anforderungen an Erfahrung

Kandidaten müssen über mindestens fünf Jahre kumulierte Vollzeit-Erfahrung in der Informationstechnologie (IT) verfügen. Drei Jahre müssen im Bereich Cybersicherheit liegen und ein Jahr in einem oder mehreren der sechs Bereiche des aktuellen CCSP-Prüfungsübersicht. Ein Hochschulabschluss (Bachelor oder Master) in Informatik, IT oder verwandten Bereichen kann bis zu einem Jahr der erforderlichen Erfahrung ausmachen. Der Erhalt des CCSK-Zertifikats von CSA kann als Ersatz für ein Jahr Berufserfahrung anerkannt werden. Nur ein Jahr Berufserfahrung kann erlassen werden. Ein aktives CISSP-Zertifikat kann die gesamte CCSP-Erfahrung ersetzen. Teilzeitarbeit und Praktika können ebenfalls auf die Erfahrungsanforderungen angerechnet werden.

Ein Kandidat, der nicht über die erforderliche Erfahrung verfügt, um ein CCSP zu werden, kann ein Partner des ISC2 werden, indem er die CCSP-Prüfung erfolgreich ablegt. Der Partner des ISC2 hat dann sechs Jahre Zeit, um die erforderlichen fünf Jahre Erfahrung zu sammeln. Mehr über die CCSP-Erfahrungsanforderungen und wie Teilzeitarbeit und Praktika angerechnet werden, erfahren Sie unter www.isc2.org/Certifications/CCSP/experience-requirements.

Akkreditierung

Das CCSP erfüllt die strengen Anforderungen der ISO/IEC-Norm 17024 des ANSI National Accreditation Board (ANAB).

Aufgabenanalyse (Job Task Analysis, JTA)

ISC2 ist gegenüber seinen Mitgliedern verpflichtet, die Relevanz des CCSP aufrechtzuerhalten. Die in regelmäßigen Abständen durchgeführte Analyse der Arbeitsaufgaben (JTA) ist ein methodischer und kritischer Prozess zur Ermittlung der Aufgaben, die von Sicherheitsfachkräften ausgeführt werden, die in dem vom CCSP definierten Beruf tätig sind. Die Ergebnisse der JTA werden zur Aktualisierung der Prüfung verwendet. Dieser Prozess stellt sicher, dass die Kandidaten in den Themenbereichen geprüft werden, die für die Rollen und Pflichten der heutigen Informationssicherheitsexperten mit Schwerpunkt auf Cloud-Technologien relevant sind.

CCSP CAT-Prüfungsinformationen

Die CCSP-Prüfung verwendet computergestützte adaptive Tests (Computerized Adaptive Testing, CAT) für alle Prüfungen in Englisch, Chinesisch (vereinfacht), Deutsch und Japanisch. Mehr über CCSP CAT erfahren Sie unter www.isc2.org/certifications/computerized-adaptive-testing.

Dauer der Prüfung	3 Stunden
Anzahl der Fragen	100–150
Frageformat	Multiple-Choice-Fragen und erweiterte Fragetypen
Minimalanforderung zum Bestehen	700 von 1000 Punkten
Verfügbarkeit der Prüfung	Englisch, Chinesisch, Deutsch, Japanisch
Testzentrum	Pearson VUE Testing Center

CCSP CAT-Prüfgewichte

Bereiche	Durchschnittsgewicht
1. Cloud-Konzepte, Architektur und Design	17 %
2. Sicherheit von Cloud-Daten	20 %
3. Sicherheit von Cloud-Plattformen und -Infrastrukturen	17 %
4. Sicherheit von Cloud-Anwendungen	16 %
5. Cloud-Sicherheitsoperationen	17 %
6. Recht, Risiko und Compliance	13 %
	Insgesamt: 100 %

Bereich 1: Cloud-Konzepte, Architektur und Design

1.1 Verstehen von Cloud-Computing-Konzepten

- Definitionen des Cloud-Computings
- Rollen und Pflichten beim Cloud-Computing (z. B. Cloud-Service-Kunde, Cloud-Service-Anbieter (CSP), Cloud-Service-Partner, Cloud-Service-Broker, Regulierungsbehörde)
- Wesentliche Merkmale des Cloud Computing (z. B. Selbstbedienung auf Anfrage, breiter Netzwerkzugang, Mandantenfähigkeit, hohe Elastizität und Skalierbarkeit, Ressourcenpooling, gemessener Service)
- Bausteintechnologien (z. B. Virtualisierung, Speicherung, Vernetzung, Datenbanken, Organisation)

1.2 Beschreiben Sie die Cloud-Referenzarchitektur

- Cloud-Computing-Aktivitäten
- Cloud-Service-Fähigkeiten (z. B. Arten von Anwendungsfähigkeiten, Arten von Plattformfähigkeiten, Arten von Infrastrukturfähigkeiten)
- Kategorien von Cloud-Service (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS))
- Cloud-Bereitstellungsmodelle (z. B. öffentlich, privat, hybrid, gemeinschaftlich, Multi-Cloud)
- Cloud-geteilte Gegenleistungen (z. B. Interoperabilität, Portabilität, Reversibilität, Verfügbarkeit, Sicherheit, Datenschutz, Ausfallsicherheit, Leistung, Governance, Wartung und Versionierung, Service-Levels und Service-Level-Agreements (SLA), Auditierbarkeit, Regulierung, Outsourcing)
- Auswirkungen verwandter Technologien (z. B. Datenwissenschaft, maschinelles Lernen, künstliche Intelligenz (KI), Blockchain, Internet der Dinge (IoT), Container, Quantencomputer, Edge Computing, vertrauliche Datenverarbeitung, DevSecOps)

1.3 Verstehen der für das Cloud-Computing relevanten Sicherheitskonzepte

- Kryptographie und Schlüsselverwaltung
- Identitäts- und Zugangskontrolle (z. B. Benutzerzugang, Zugriffsrechte, Dienstzugang)
- Daten- und Mediensanierung (z. B. Überschreiben, kryptografisches Löschen)
- Netzwerksicherheit (z. B. Netzsicherheitsgruppen, Verkehrskontrolle, Geofencing)
- Virtualisierungssicherheit (z. B. Hypervisor-Sicherheit, Container-Sicherheit, flüchtiges Computing, serverlose Technologie, Isolierung)
- Häufige Cloud-Bedrohungen
- Sicherheitshygiene (z. B. Patching, Baselining, unveränderliche Architektur, Härtung)

1.4 Verstehen der Designprinzipien des sicheren Cloud-Computings

- Sicherer Lebenszyklus von Daten in der Cloud
- Cloud-basierte Planung von Geschäftskontinuität (Business Continuity, BC) und Notfallwiederherstellung (Disaster Recovery, DR)
- Geschäftsauswirkungsanalyse (Business Impact Analysis, BIA) (z. B. Kosten-Nutzen-Analyse(Cost-Benefit Analysis, CBA), Investitionsrendite (Return On Investment, ROI))
- Funktionale Sicherheitsanforderungen (z. B. Übertragbarkeit, Interoperabilität, Herstellerbindung)
- Sicherheitserwägungen und Pflichten für verschiedene Cloud-Kategorien (z. B. Software als Service (Software as a Service, SaaS), Infrastruktur als Service (Infrastructure as a Service, IaaS), Plattform als Service (Platform as a Service, PaaS))
- Cloud-Designmuster (z. B. SANS-Sicherheitsgrundsätze, Well-Architected Framework, Cloud Security Alliance (CSA) Enterprise Architecture, Secure by Design)
- DevOps-Sicherheit

1.5 Bewerten Sie Cloud-Service-Anbieter (Cloud Service Providers, CSP)

- Überprüfung anhand von Kriterien
- System-/Subsystem-Produktzertifizierungen (z. B. Common Criteria (CC), Federal Information Processing Standard (FIPS) 140-2)

1.6 Verstehen von künstlicher Intelligenz (KI)/maschinellem Lernen (ML)

- Erkennung und Analyse von Cloud-Bedrohungen
- Validierung und Überprüfung von Datenquellen
- Sicherheitsorganisation, Automatisierung und Reaktion (SOAR)
- Ethische Anliegen
- Regulatorische Anforderungen

Bereich 2: Sicherheit von Cloud-Daten

2.1 Beschreiben der Konzepte für Cloud-Daten

- Phasen des Lebenszyklus von Cloud-Daten
- Streuung der Daten
- Datenströme

2.2 Entwurf und Implementierung von Cloud-Datenspeicherarchitekturen

- Speichertypen (z. B. Langzeitspeicher, flüchtig, Rohspeicher, Objektspeicher, Volumenspeicher)
- Bedrohungen für Lagertypen

2.3 Entwurf und Anwendung von Datensicherheitstechnologien und -strategien

- Verschlüsselung und Schlüsselverwaltung
- Hashing (z. B. Datenintegrität, Nichtabstreitbarkeit)
- Datenverschleierung (z. B. Maskierung, Anonymisierung)
- Tokenisierung
- Schutz vor Datenverlust (Data Loss Prevention, DLP)
- Verwaltung von Schlüsseln, Geheimnissen und Zertifikaten

2.4 Datenermittlung implementieren

- Strukturierte Daten
- Unstrukturierte Daten
- Halbstrukturierte Daten
- Standort der Daten

2.5 Planung und Umsetzung der Datenklassifizierung

- Richtlinien zur Datenklassifizierung
- Datenmapping
- Kennzeichnung und Markierung von Daten

2.6 Entwurf und Umsetzung von Information Rights Management (IRM)

- Ziele (z. B. Datenrechte, Bereitstellung, Zugriffsmodelle)
- Geeignete Instrumente (z. B. Ausstellung und Sperrung von Zertifikaten)

2.7 Planung und Umsetzung von Maßnahmen zur Aufbewahrung, Löschung und Archivierung von Daten

- Richtlinien zur Datenaufbewahrung
- Verfahren und Mechanismen zur Datenlöschung
- Verfahren und Mechanismen zur Datenarchivierung
- Gesetzliche Aufbewahrung (z. B. autorisierter Zugriff, Verhinderung der Löschung)

2.8 Konzeption und Umsetzung der Auditierbarkeit, Rückverfolgbarkeit und Rechenschaftspflicht von Datenereignissen

- Definition von Ereignisquellen und Anforderung von Ereignisattributen (z. B. Identität, Internetprotokoll (IP) Adresse, Geolokalisierung)
- Protokollierung, Speicherung und Analyse von Datenereignissen
- Überwachungskette und Unleugbarkeit

2.9 Verstehen des Datenschutzes für Daten aus den Bereichen künstliche Intelligenz (KI) und maschinelles Lernen (ML)

- Datensatz und Modelldatenschutz
- Datensatz- und Modellsicherheit (z. B. Validierung, Verifizierung)

Bereich 3: Cloud-Plattform und Infrastruktur Sicherheit

3.1 Verstehen der Komponenten der Cloud-Infrastruktur

- Physische Umgebung
- Netzwerk und Kommunikation
- Rechenleistung
- Virtualisierung
- Lagerung
- Verwaltungsebene

3.2 Entwurf eines sicheren Rechenzentrums

- Logischer Entwurf (z. B. Mieterpartitionierung, Zugangskontrolle)
- Physisches Design (z. B. Standort, Kauf oder Bau)
- Umweltdesign (z. B. Heizung, Lüftung und Klimatisierung (HLK), Verbindungen zwischen verschiedenen Anbietern)
- Belastbarkeit der Konstruktion (z. B. Strom, Heizung, Lüftung und Klimatisierung (HLK), Konnektivität)

3.3 Analyse der Risiken im Zusammenhang mit Cloud-Infrastrukturen und -Plattformen

- Risikobewertung (z. B. Identifizierung, Analyse)
- Schwachstellen, Bedrohungen und Angriffe in der Cloud
- Strategien zur Risikobehandlung

3.4 Planung und Durchführung von Sicherheitskontrollen

- Physischer Schutz und Umweltschutz (z. B. vor Ort)
- System-, Speicher- und Kommunikationsschutz
- Identifizierung, Authentifizierung und Autorisierung in Cloud-Umgebungen
- Auditmechanismen (z. B. Protokollerfassung, Korrelation, Paketerfassung)

3.5 Planung von Geschäftskontinuität (BC) und Notfallwiederherstellung (DR)

- Strategie für Geschäftskontinuität (BC) / Notfallwiederherstellung (DR)
- Geschäftsanforderungen (z.B. Wiederherstellungszeitziel (Recovery Time Objective, RTO), Wiederherstellungspunktziel (Recovery Point Objective, RPO), Wiederherstellungsservicelevel)
- Erstellung, Umsetzung und Prüfung des Plans

Bereich 4: Sicherheit von Cloud-Anwendungen

4.1 Förderung von Schulungen und Sensibilisierung für Anwendungssicherheit

- Grundlagen der Cloud-Entwicklung
- Häufige Stolperfallen
- Häufige Cloud-Schwachstellen (z. B. Open Web Application Security Project (OWASP) Top-10, Application Security Verification Standard (ASVS), Top 10 Application Programming Interface (API), Top 10 for Large Language Model Applications, SANS Top-25)

4.2 Beschreibung des Prozesses des Lebenszyklus der sicheren Softwareentwicklung (SDLC)

- Geschäftliche Anforderungen
- Phasen und Methoden (z. B. Design, Code, Test, Wartung, Wasserfall vs. Agil)

4.3 Anwendung des Lebenszyklus der sicheren Softwareentwicklung (SDLC)

- Cloud-spezifische Risiken (z. B. gemeinsame Technologieprobleme, Bedrohungen durch Insider des Cloud-Service-Providers (CSP), mangelnde Transparenz und Kontrolle, rechtliche und juristische Fragen)
- Bedrohungsmodellierung (z. B. Spoofing, Manipulation, Repudiation, Information Disclosure, Denial of Service und Elevation of Privilege (STRIDE), Disaster, Reproducibility, Exploitability, Affected Users und Discoverability (DREAD), Architecture, Threats, Attack Surfaces, and Mitigations (ATASM), Process for Attack Simulation and Threat Analysis (PASTA))
- Vermeiden häufiger Schwachstellen bei der Entwicklung
- Sichere Kodierung (z. B. Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS), Software Assurance Forum for Excellence in Code (SAFECode))
- Software-Konfigurationsmanagement (Configuration Management, CM) und -Versionierung

4.4 Anwendung von Cloud Software-Sicherung und -Validierung

- Funktionale und nicht-funktionale Tests (z. B. Kontinuierliche Integration und kontinuierliche Lieferung (Continuous Integration And Continuous Delivery, CI/CD)-Prozesse)
- Sicherheitstestmethoden (z. B. Blackbox, Whitebox, Softwarezusammenstellungsanalyse (Software Composition Analysis, SCA), Interaktive Applikationssicherheitstests (Interactive Application Security Testing,IAST), Statische Anwendungssicherheitstests (Static Application Security Testing, SAST), Sicherheitstests für dynamische Anwendungen (Dynamic Application Security Testing, DAST))
- Qualitätssicherung (QA)
- Testen von Missbrauchsfällen

4.5 Verwendung geprüfter sicherer Software

- Sicherung von Programmierschnittstellen (Application Programming Interfaces, API)
- Management der Lieferkette (z. B. Bewertung von Anbietern, Integrität, Authentizität, Lizenzierung)
- Verwaltung von Fremdsoftware
- Validierte Open-Source-Software

4.6 Verstehen und Anwenden der Besonderheiten der Architektur von Cloud-Anwendungen

- Zusätzliche Sicherheitskomponenten (z. B. Webanwendungsfirewall (Web Application Firewall, WAF), Aktivitätsüberwachung bei Datenbanken (Database Activity Monitoring, DAM), Extensible Markup Language (XML)-Firewalls,Programmierschnittstellen (Application Programming Interface, API)-Gateway, Load Balancer)
- Kryptographie
- Sandboxing
- Anwendungsvirtualisierung und -organisation (z. B. Microservices, Container, Docker, Kubernetes)

4.7 Entwicklung geeigneter Lösungen für die Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM)

- Identitätsverbund
- Identitätsanbieter (Identity Providers, IdP)
- Einmalige Anmeldung (Single Sign-On, SSO)
- Multi-Faktor-Authentifizierung (Multi-Factor Authentication, MFA)
- Sicherheits-Broker für den Cloud-Zugang (Cloud Access Security Broker, CASB)
- Verwaltung von Geheimnissen, Schlüsseln und Zertifikaten

Bereich 5: Cloud-Sicherheitsoperationen

5.1 Aufbau und Implementierung der physischen und logischen Infrastruktur für die Cloud-Umgebung

- Hardware-spezifische Anforderungen an die Sicherheitskonfiguration (z. B. Hardware-Sicherheitsmodul (Hardware Security Module, HSM) und vertrauenswürdiges Plattformmodul (Trusted Platform Module, TPM))
- Standardmäßig sicher
- Installation und Konfiguration der Tools der Verwaltungsebene
- Spezifische Anforderungen an die Sicherheitskonfiguration der virtuellen Hardware (z. B. Netzwerk, Speicher, Arbeitsspeicher, Zentraleinheit (Central Processing Unit, CPU), Hypervisor Typ 1 und 2)
- Installation von Tools zur Virtualisierung von Gastbetriebssystemen (Operating System, OS)

5.2 Betrieb und Wartung der physischen und logischen Infrastruktur für die Cloud-Umgebung

- Zugriffskontrollen für den lokalen und den Fernzugriff (z. B. Remote Desktop Protocol (RDP), sicherer Terminalzugriff, Secure Shell (SSH), konsolenbasierte Zugriffsmechanismen, Jumpboxes, virtueller Client, einmalige Anmeldung (SSO))
- Sichere Netzwerkkonfiguration (z B. virtuelle lokale Netzwerke (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System Security Extensions (DNSSEC), virtuelles privates Netzwerk (VPN))
- Netzwerksicherheitskontrollen (z. B. Firewalls, Intrusion Detection Systems (IDS), Angrifferkennungssystem ((Intrusion Prevention Systems, IPS), Honeypots, Schwachstellenbewertungen, Netzwerksicherheitsgruppen, Bastion Host, Segmentierung)
- Härtung von Betriebssystemen (OS) durch die Anwendung von Baselines, Überwachung und Abhilfemaßnahmen (z. B. Windows, Linux, VMware)
- Patch-Verwaltung
- Verfügbarkeit von geclusterten Hosts (z. B. verteilte Ressourcenplanung, dynamische Optimierung, Speichercluster, Wartungsmodus, Hochverfügbarkeit (HV))
- Verfügbarkeit des Gastbetriebssystems (OS)
- Leistungs- und Kapazitätsüberwachung (z. B. Netzwerk, Rechenleistung, Speicherplatz, Reaktionszeit)
- Hardware-Überwachung (z. B. Festplatte, Prozessor (CPU), Lüftergeschwindigkeit, Temperatur)
- Konfiguration der Sicherungs- und Wiederherstellungsfunktionen für Host- und Gastbetriebssysteme (OS)
- Verwaltungsebene (z. B. Zeitplanung, Orchestrierung, Wartung)

5.3 Implementierung von betrieblichen Kontrollen und Standards (z. B. National Institute Of Standards And Technology (NIST), Internationale Organisation für Normung (ISO), Health Insurance Portability and Accountability Act (HIPPA), Steuerungsvorgaben für die Informationstechnologie und damit verbundene Technologien (COBIT), Center For Internet Security (CIS) Controls, Comittee Of Sponsoring Organizations (COSO), Information Technology Infrastructure Library (ITIL) International Organization For Standardization/International Electrotechnical Commission (ISO/IEC) 20000-1)

- Verwaltung von Veränderungen
- Kontinuitätsverwaltung
- Verwaltung der Informationssicherheit
- Verwaltung der kontinuierlichen Verbesserung der Dienstleistungen
- Verwaltung von Zwischenfällen
- Verwaltung von Problemen
- Verwaltung der Freigabe
- Verwaltung der Einsätze
- Konfigurationsverwaltung (Configuration Management, CM)
- Verwaltung des Service Level
- Verwaltung der Verfügbarkeit
- Verwaltung der Kapazitäten

5.4 Unterstützung der digitalen Forensik

- Methoden der forensischen Datenerhebung
- Verwaltung von Beweismitteln
- Sammeln, Beschaffen und Bewahren digitaler Beweismittel

5.5 Verwaltung der Kommunikation mit relevanten Parteien

- Anbieter
- Kunden
- Partner
- Regulierungsbehörden
- Andere Interessengruppen

5.6 Verwaltung von Sicherheitsmaßnahmen

- Sicherheits-Operations-Center (Security Operations Center, SOC)
- Intelligente Überwachung von Sicherheitskontrollen (z. B. Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Honeypots, Netzwerksicherheitsgruppen, künstliche Intelligenz (KI))
- Protokollerfassung und Analyse (z. B. Sicherheitsinformationen und Ereignisverwaltung (SIEM), Protokollverwaltung, Threat Intelligence)
- Reaktion auf Zwischenfälle (Incident Response, IR)
- Schwachstellenanalysen
- Penetrationstests

Bereich 6: Recht, Risiko und Compliance

6.1 Darstellung der rechtlichen Anforderungen und der besonderen Risiken in der Cloud-Umgebung

- Widersprüchliche internationale Rechtsvorschriften
- Bewertung der für das Cloud-Computing spezifischen rechtlichen Risiken
- Rechtliche und regulatorische Rahmenbedingungen und Leitlinien
- eDiscovery (z. B. Internationale Organisation für Normung/Internationale Elektrotechnische Kommission (ISO/IEC) 27050, Leitlinien der Cloud Security Alliance (CSA))
- Forensische Anforderungen (z. B. Cloud Security Alliance (CSA), Internationale Organisation für Normung/International Electrotechnical Commission (ISO/IEC) 27037:2012/27041:2015/ 27042:2015/ 27043:2015)

6.2 Verstehen der Datenschutzanforderungen

- Unterschied zwischen vertraglichen und regulierten privaten Daten (z. B. geschützte Gesundheitsinformationen, persönlich identifizierbare Informationen (PII))
- Länderspezifische Gesetzgebung in Bezug auf private Daten (z. B. Family Educational Rights And Privacy Act (FERPA), The Personal Information Protection And Electronic Documents Act (PIPEDA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPPA), Digital Personal Data Protection Act)
- Juristische Unterschiede beim Datenschutz
- Standard-Datenschutzanforderungen (z B. Internationale Organisation für Normung/Internationale Elektrotechnische Kommission (ISO/IEC) 27018, allgemein anerkannte Datenschutzgrundsätze (GAPP), allgemeine Datenschutzverordnung (GDPR))
- Datenschutz-Folgenabschätzungen (Privacy Impact Assessments, PIA)

6.3 Verständnis der Auditprozesse, der Methoden und der erforderlichen Anpassungen für eine Cloud-Umgebung

- Interne und externe Auditkontrollen
- Auswirkungen der Audit-Anforderungen
- Identifizierung der Herausforderungen von Virtualisierung und Cloud
- Arten von Auditberichten (z. B. Statement on Standards for Attestation Engagements (SSAE), Service Organization Control (SOC), International Standard on Assurance Engagements (ISAE))
- Beschränkungen des Auditumfangs (z. B. Statement on Standards for Attestation Engagements (SSAE), International Standard on Assurance Engagements (ISAE))
- Lückenanalyse (z. B. Kontrollanalyse, Baselines Risiko und Selbstbewertung der Kontrollen)
- Audit-Planung
- Internes Informations sicherheit sverwaltungs system (Internal Information Security Management System, ISMS)
- Internes Kontrollsystem für die Informationssicherheit
- Richtlinien (z. B. organisatorisch, funktional, Cloud-Computing)
- Identifizierung und Einbeziehung relevanter Interessengruppen
- Spezielle Compliance-Anforderungen für stark regulierte Branchen (z. B. North American Electric Reliability Corporation / Critical Infrastructure Protection (NERC CIP), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, Payment Card Industry (PCI))
- Auswirkungen des Modells der verteilten Informationstechnologie (IT) (z. B. verschiedene geografische Standorte und übergreifende Rechtssysteme)

6.4 Verstehen der Auswirkungen der Cloud auf das Risikoverwaltung von Unternehmen

- Bewertung der Risikoverwaltungsprogramme der Anbieter (z. B. Kontrollen, Methoden, Richtlinien, Risikoprofil, Risikobereitschaft)
- Unterschiede zwischen Datenrollen (z. B. Eigentümer, Verantwortlicher, Verwahrer, Verarbeiter, Verwalter)
- Regulatorische Transparenzanforderungen (z. B. Meldung von Verstößen, Sarbanes-Oxley (SOX), Datenschutz-Grundverordnung (GDPR))
- Risikobehandlung (z. B. vermeiden, mindern, übertragen, teilen, akzeptieren)
- Unterschiedliche Risiko-Rahmenbedingungen
- Metriken für die Risikoverwaltung
- Bewertung der Risikoumgebung (z. B. Dienst, Anbieter, Infrastruktur, Unternehmen)

6.5 Verstehen von Outsourcing und Cloud-Vertragsgestaltung

- Geschäftsanforderungen (z. B. Service Level Agreement (SLA), Master Service Agreement (MSA), Leistungsbeschreibung (Statement of Work, SOW))
- Lieferantenverwaltung (z. B. Lieferantenbewertungen, Lock-in-Risiken, Lebensfähigkeit von Lieferanten, Treuhand)
- Vertragsverwaltung (z. B. Recht auf Audit, Kennzahlen, Definitionen, Kündigung, Rechtsstreitigkeiten, Versicherung, Compliance, Zugang zu Cloud/Daten, Cyber-Risikoversicherung, Dateneigentum, Sicherheitsanforderungen)
- Verwaltung der Lieferkette (z. B. Internationale Organisation für Normung/Internationale Elektrotechnische Kommission (ISO/IEC) 27036)

Zusätzliche Informationen zur Prüfung

Ergänzende Referenzen

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

Die vollständige Liste der ergänzenden Referenzen finden Sie unter ISC2.org/certifications/References.

Prüfungsrichtlinien und -verfahren

ISC2 empfiehlt den Kandidaten, die Prüfungsrichtlinien und -verfahren zu lesen, bevor sie sich zur Prüfung anmelden. Lesen Sie die umfassende Aufschlüsselung dieser wichtigen Informationen unter ISC2.org/Register-for-Exam.

Rechtliche Hinweise

Bei Fragen zu den Rechtsgrundsätzen von ISC2 wenden Sie sich bitte an die Rechtsabteilung von ISC2 unter legal@isc2.org.

Haben Sie Fragen?

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

Amerika
Tel.: +1.866.331.ISC2 (4722), drücken Sie 1
E-Mail: membersupport@isc2.org

Asia-Pacific
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

ISC2