CCSP®

# Certified Cloud Security Professional

An (ISC)² Certification

# Gliederung der Zertifizierungsprüfung

Gültig ab: 1. August 2022

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

# Über CCSP

(ISC)² 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 Service-Orchestrierung. Diese berufliche Kompetenz wird anhand eines weltweit anerkannten Wissensbestands gemessen.

Die im CCSP Common Body of Knowledge (CBK) enthaltenen Themen gewährleisten seine Relevanz für alle Disziplinen im Bereich der Cloud-Sicherheit. Erfolgreiche Bewerber verfügen über Kompetenzen in den folgenden sechs Bereichen:

- Cloud-Konzepte, Architektur und Design
- Datensicherheit in der Cloud
- Sicherheit von Cloud-Plattformen und -Infrastrukturen
- Anwendungssicherheit in der Cloud
- Sicherheitsabläufe in der Cloud
- Recht, Risiko und Compliance

## Anforderungen bezüglich der Erfahrung

Die Kandidaten müssen eine einschlägige Berufserfahrung von mindestens fünf Jahren in der Informationstechnologie besitzen, davon drei Jahre in der Informationssicherheit und ein Jahr in einem oder mehreren der sechs Bereiche des CCSP CBK. Der Erwerb des CCSK-Zertifikats von CSA kann ein Jahr Erfahrung in einem oder mehreren der sechs Bereiche des CCSP CBK ersetzen. Der Erwerb des CISSP-Zertifikats von (ISC)² kann die gesamte CCSP-Erfahrung ersetzen.

Ein Kandidat, der nicht über die erforderliche Erfahrung verfügt, um ein CCSP zu werden, kann durch Bestehen der CCSP-Prüfung Associate of (ISC)² werden. Der Associate of (ISC)² hat dann sechs Jahre Zeit, um die erforderlichen fünf Jahre Erfahrung zu sammeln. Weitere Informationen zu den Anforderungen an die CCSP-Erfahrung und zur Anrechnung von Teilzeitarbeit und Praktika finden Sie unter www.isc2.org/Certifications/CCSP/experience-requirements.

## Akkreditierung

Das CCSP erfüllt die strengen Anforderungen der ANSI/ISO/IEC-Norm 17024.

## Analyse der Arbeitsaufgaben (JTA)

(ISC)² ist gegenüber seinen Mitgliedern verpflichtet, die Relevanz des CCSP aufrechtzuerhalten. Die in regelmäßigen Abständen durchgeführte Job Task Analysis (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. Dieses Verfahren stellt sicher, dass die Kandidaten in den Themenbereichen geprüft werden, die für die Aufgaben und Verantwortlichkeiten der heutigen Informationssicherheitsexperten mit Schwerpunkt auf Cloud-Technologien relevant sind.

# Informationen zur CCSP-Prüfung

| | |
|---|---|
| **Dauer der Prüfung** | 4 Stunden |
| **Anzahl der Fragen** | 150 |
| **Aufbau der Prüfung** | Mehrfachauswahl |
| **Mindestpunktzahl** | 700 von 1000 Punkten |
| **Verfügbarkeit der Prüfung** | Englisch, Chinesisch, Deutsch, Koreanisch, Japanisch, Spanisch |
| **Prüfungsort** | Pearson-VUE-Prüfungszentrum |

# Gewichtsverteilung bei CCSP-Prüfungen

| Domäne | Gewicht |
|---|---|
| 1. Cloud-Konzepte, Architektur und Design | 17% |
| 2. Datensicherheit in der Cloud | 20% |
| 3. Sicherheit von Cloud-Plattformen und -Infrastrukturen | 17% |
| 4. Anwendungssicherheit in der Cloud | 17% |
| 5. Sicherheitsabläufe in der Cloud | 16% |
| 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 Computing
- Rollen und Verantwortlichkeiten beim Cloud Computing (z. B. Cloud-Service-Kunde, Cloud-Service-Anbieter, Cloud-Service-Partner, Cloud-Service-Broker, Regulierungsbehörde)
- Hauptmerkmale des Cloud Computing (z. B. Selbstbedienung auf Anfrage, breiter Netzzugang, Mandantenfähigkeit, schnelle Elastizität und Skalierbarkeit, Ressourcenpooling, gemessener Service)
- Bausteintechnologien (z. B. Virtualisierung, Speicherung, Vernetzung, Datenbanken, Orchestrierung)

## 1.2 Beschreiben der Cloud-Referenzarchitektur

- Cloud Computing-Aktivitäten
- Cloud-Service-Fähigkeiten (z. B. Arten von Anwendungsfähigkeiten, Arten von Plattformfähigkeiten, Arten von Infrastrukturfähigkeiten)
- Cloud-Service-Kategorien (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS))
- Cloud-Bereitstellungsmodelle (z. B. öffentlich, privat, hybrid, gemeinschaftlich, Multi-Cloud)
- Gemeinsame Überlegungen zur Cloud (z. B. Interoperabilität, Übertragbarkeit, Reversibilität, Verfügbarkeit, Sicherheit, Datenschutz, Belastbarkeit, 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)
- Netzsicherheit (z. B. Netzsicherheitsgruppen, Netzübertragungskontrollen, Geofencing, Zero Trust Network)
- Virtualisierungssicherheit (z. B. Hypervisor-Sicherheit, Container-Sicherheit, ephemeres Computing, serverlose Technologie)
- Häufige Bedrohungen
- Sicherheitshygiene (z. B. Patching, Baselining)

## 1.4 Verstehen der Gestaltungsprinzipien des sicheren Cloud Computing

- Sicherer Lebenszyklus von Daten in der Cloud
- Plan zur Cloud-basierten Geschäftskontinuität (BC) Notfallwiederherstellung (DR)
- Business-Impact-Analyse (BIA) (z. B. Kosten-Nutzen-Analyse, Investitionsrendite (ROI))
- Funktionale Sicherheitsanforderungen (z. B. Übertragbarkeit, Interoperabilität, Herstellerbindung)
- Sicherheitsüberlegungen und Verantwortlichkeiten für verschiedene Cloud-Kategorien (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS))
- Cloud-Entwurfsmuster (z. B. SANS-Sicherheitsgrundsätze, Well-Architected Framework, Cloud Security Alliance (CSA) Enterprise Architecture)
- DevOps-Sicherheit

## 1.5 Bewertung von Cloud-Service-Anbietern

- Überprüfung anhand von Kriterien (z. B. Internationale Organisation für Normung/Internationale Elektrotechnische Kommission (ISO/IEC) 27017, Payment Card Industry Data Security Standard (PCI DSS))
- System-/Subsystem-Produktzertifizierungen (z. B. Common Criteria (CC), Federal Information Processing Standard (FIPS) 140-2)

# Bereich 2: Datensicherheit in der Cloud

## 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. langfristige, ephemere oder rohe Datenspeicherung)
- Bedrohungen für Speichertypen

## 2.3 Entwurf und Anwendung von Datensicherheitstechnologien und -strategien

- Verschlüsselung und Schlüsselverwaltung
- Hashing
- Datenverschleierung (z. B. Maskierung, Anonymisierung)
- Tokenisierung
- Verhinderung von Datenverlust (DLP)
- Verwaltung von Schlüsseln, Geheimnissen und Zertifikaten

## 2.4 Implementierung der Datenermittlung

- Strukturierte Daten
- Unstrukturierte Daten
- Halbstrukturierte Daten
- Speicherort der Daten

## 2.5 Planung und Implementierung der Datenklassifizierung

- Richtlinien zur Datenklassifizierung
- Datenzuordnung
- Kennzeichnung der Daten

## 2.6 Entwurf und Implementierung von Information Rights Management (IRM)

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

## 2.7 Planung und Implementierung von Maßnahmen zur Aufbewahrung, Löschung und Archivierung von Daten

- Richtlinien zur Datenaufbewahrung
- Verfahren und Mechanismen zur Datenlöschung
- Verfahren und Mechanismen zur Datenarchivierung
- Gesetzliche Aufbewahrung

## 2.8 Konzeption und Implementierung der Prüfbarkeit, 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 Nichtabstreitbarkeit

# Bereich 3: Cloud-Plattform und -Infrastruktur Sicherheit

## 3.1 Verstehen der Cloud-Infrastruktur und -Plattform-Komponenten

- Physische Umgebung
- Netzwerk und Kommunikation
- Berechnung
- Virtualisierung
- Speicherung
- Verwaltungsebene

## 3.2 Entwurf eines sicheren Rechenzentrums

- Logischer Entwurf (z. B. Mieterpartitionierung, Zugangskontrolle)
- Physische Gestaltung (z. B. Standort, Kauf oder Bau)
- Umgebungsdesign (z. B. Heizung, Belüftung und Klimatisierung (HVAC), Verbindungen zwischen verschiedenen Anbietern)
- Belastbar gestalten

## 3.3 Analyse der mit Cloud-Infrastrukturen und -Plattformen verbundenen Risiken

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

## 3.4 Planung und Implementierung von Sicherheitskontrollen

- Physische und umgebungsbezogene Sicherheit (z. B. vor Ort)
- System-, Speicher- und Kommunikationsschutz
- Identifizierung, Authentifizierung und Autorisierung in Cloud-Umgebungen
- Audit-Mechanismen (z. B. Protokollerfassung, Korrelation, Paketerfassung)

## 3.5 Plan zur Geschäftskontinuität (BC)- und Notfallwiederherstellung (DR)

- Strategie für Geschäftskontinuität (BC) / Notfallwiederherstellung (DR)
- Geschäftsanforderungen (z. B. Recovery Time Objective (RTO), Recovery Point Objective (RPO), Recovery Service Level)
- Erstellung, Implementierung und Prüfung des Plans

# Bereich 4: Anwendungssicherheit in der Cloud

## 4.1 Förderung von Schulungen und Sensibilisierung für die Anwendungssicherheit

» Grundlagen der Cloud-Entwicklung

» Häufige Fallstricke

» Häufige Cloud-Schwachstellen (z. B. Open Web Application Security Project (OWASP) Top-10, SANS Top-25)

## 4.2 Beschreibung des Prozesses des Software Development Life Cycle (SDLC)

» Geschäftliche Anforderungen

» Phasen und Methoden (z. B. Entwurf, Code, Test, Wartung, Wasserfall vs. Agile)

## 4.3 Anwendung des Secure Software Development Life Cycle (SDLC)

» Cloud-spezifische Risiken

» 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))

» Vermeidung 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 und Versionierung

## 4.4 Anwendung der Cloud-Software-Sicherung und -Validierung

» Funktionale und nicht-funktionale Tests

» Sicherheitstestmethoden (z. B. Blackbox, Whitebox, statisch, dynamisch, Software Composition Analysis (SCA), interaktives Testen der Anwendungssicherheit (IAST))

» Qualitätssicherung (QA)

» Testen von Missbrauchsfällen

## 4.5 Verwendung geprüfter sicherer Software

» Sicherung von Programmierschnittstellen (API)

» Management der Lieferkette (z. B. Lieferantenbewertung)

» Verwaltung von Fremdsoftware (z. B. Lizenzierung)

» Validierte Open-Source-Software

## 4.6 Verstehen der Besonderheiten der Architektur von Cloud-Anwendungen

- Zusätzliche Sicherheitskomponenten (z. B. Web Application Firewall (WAF), Database Activity Monitoring (DAM), Extensible Markup Language (XML)-Firewalls, Application Programming Interface (API)-Gateway)
- Kryptographie
- Sandboxing
- Anwendungsvirtualisierung und -orchestrierung (z. B. Microservices, Container)

## 4.7 Entwicklung geeigneter Lösungen für das Identitäts- und Zugriffsmanagement (IAM)

- Föderierte Identität
- Identitätsanbieter (IdP)
- Einmalige Anmeldung (SSO)
- Multi-Faktor-Authentifizierung (MFA)
- Cloud Access Security Broker (CASB)
- Verwaltung von Geheimnissen

# Bereich 5: Sicherheitsabläufe in der Cloud

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

- Hardware-spezifische Anforderungen an die Sicherheitskonfiguration (z. B. Hardware-Sicherheitsmodul (HSM) und Trusted Platform Module (TPM))
- Installation und Konfiguration von Verwaltungstools
- Spezifische Anforderungen an die Sicherheitskonfiguration virtueller Hardware (z. B. Netzwerk, Speicher, Arbeitsspeicher, Zentraleinheit (CPU), Hypervisor Typ 1 und 2)
- Installation von Tools zur Virtualisierung von Gastbetriebssystemen (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)
- 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), Intrusion Prevention Systems (IPS), Honeypots, Schwachstellenbewertungen, Netzwerksicherheitsgruppen, Bastion Host)
- Härtung von Betriebssystemen (OS) durch die Anwendung von Baselines, Überwachung und Abhilfemaßnahmen (z. B. Windows, Linux, VMware)
- Patch-Verwaltung
- Strategie "Infrastruktur als Code" (IaC)
- Verfügbarkeit von geclusterten Hosts (z. B. verteilte Ressourcenplanung, dynamische Optimierung, Speichercluster, Wartungsmodus, Hochverfügbarkeit (HA))
- Verfügbarkeit des Gastbetriebssystems (OS)
- Leistungs- und Kapazitätsüberwachung (z. B. Netzwerk, Rechenleistung, Speicherplatz, Reaktionszeit)
- Hardware-Überwachung (z. B. Festplatte, Zentraleinheit (CPU), Lüftergeschwindigkeit, Temperatur)
- Konfiguration von Sicherungs- und Wiederherstellungsfunktionen für Host- und Gastbetriebssysteme (OS)
- Verwaltungsebene (z. B. Zeitplanung, Orchestrierung, Wartung)

## 5.3. Implementierung von Betriebskontrollen und Standards (z. B. Information Technology Infrastructure Library (ITIL), Internationale Organisation für Normung/Internationale Elektrotechnische Kommission (ISO/IEC) 20000-1)

- Änderungsmanagement
- Kontinuitätsmanagement
- Management der Informationssicherheit
- Management der kontinuierlichen Verbesserung von Dienstleistungen
- Management von Zwischenfällen
- Problemmanagement
- Freigabe-Management
- Verwaltung des Einsatzes
- Konfigurationsmanagement
- Service-Level-Management
- Verfügbarkeitsmanagement
- Kapazitätsmanagement

## 5.4 Unterstützung der digitalen Forensik

- Methoden zur forensischen Datenerhebung
- Beweismittelmanagement
- Sammeln, Beschaffen und Sichern digitaler Beweismittel

## 5.5. Verwaltung der Kommunikation mit den relevanten Parteien

- Anbieter
- Kunden
- Partner
- Regulierungsbehörden
- Andere Interessengruppen

## 5.6 Verwaltung von Sicherheitsmaßnahmen

- Sicherheits-Operations-Center (SOC)
- Intelligente Überwachung von Sicherheitskontrollen (z. B. Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Honeypots, Netzsicherheitsgruppen, künstliche Intelligenz (KI))
- Protokollerfassung und -analyse (z. B. Sicherheitsinformations- und Ereignisverwaltung (SIEM), Protokollverwaltung)
- Management von Zwischenfällen
- Schwachstellenanalysen

# 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
- Rechtlicher Rahmen und Leitlinien
- eDiscovery (z. B. Internationale Organization für Normungen/Internationale Elektrotechnische Kommission (ISO/IEC) 27050, Leitlinie zur Cloud Security Alliance (CSA))
- Forensische Anforderungen

## 6.2 Verstehen der Datenschutzfragen

- Unterschied zwischen vertraglichen und regulierten privaten Daten (z. B. geschützte Gesundheitsdaten (PHI), Personenbezogene Daten (PII))
- Landesspezifische Gesetze bezüglich privater Daten (z. B. geschützte Gesundheitsdaten (PHI), personenbezogene Daten (PII))
- Juristische Unterschiede beim Datenschutz
- Standdartanforderungen an den Datenschutz (z.B. Internationale Organisation für Normungen/ Internationale Elektrotechnsiche Kommission (ISO/IEC) 27018, Allgemein anerkannte Datenschutzgrundsätze (GAPP), Datenschutz-Grundverordnung (DSGVO))
- Datenschutz-Folgenabschätzungen (PIA)

## 6.3 Verstehen des Auditprozesses, der Methoden und der erforderlichen Anpassungen für eine Cloud-Umgebung

- Interne und externe Auditkontrollen
- Auswirkungen der Prüfungsanforderungen
- Identifizieren der Herausforderungen für die Sicherung von Virtualisierung und Cloud
- Arten von Prüfungsberichten (z. B. Statement on Standards for Attestation Engagements (SSAE), Service Organization Control (SOC), International Standard on Assurance Engagements (ISAE))
- Beschränkungen des Prüfungsumfangs (z. B. Statement on Standards for Attestation Engagements (SSAE), International Standard on Assurance Engagements (ISAE))
- Lückenanalyse (z. B. Kontrollanalyse, Baselines)
- Audit-Planung
- Internes Informationssicherheitsmanagementsystem
- Internes Kontrollsystem für 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))
- Auswirkung des Modells der verteilten Informationstechnologie (IT) (z. B. verschiedene geografische Standorte und Überschreiten von Rechtsprechungen)

## 6.4 Verstehen der Auswirkungen der Cloud auf das Risikomanagement von Unternehmen

- Bewertung der Risikomanagementprogramme der Anbieter (z. B. Kontrollen, Methoden, Richtlinien, Risikoprofil, Risikobereitschaft)
- Unterschied zwischen Dateneigentümer/Verantwortlicher und Datentreuhänder/Verarbeiter
- Regulatorische Transparenzanforderungen (z. B. Meldung von Verstößen, Sarbanes-Oxley (SOX), Allgemeine Datenschutzverordnung (GDPR))
- Risikobehandlung (d. h. Vermeidung, Abschwächung, Übertragung, Teilung, Akzeptanz)
- Unterschiedliche Risiko-Rahmenbedingungen
- Metriken für das Risikomanagement
- 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), Statement of Work (SOW))
- Lieferantenmanagement (z. B. Lieferantenbewertungen, Lock-in-Risiken, Lebensfähigkeit von Lieferanten, Treuhand)
- Vertragsmanagement (z. B. Recht auf Audit, Metriken, Definitionen, Kündigung, Rechtsstreitigkeiten, Versicherung, Compliance, Zugang zu Cloud/Daten, Cyber-Risikoversicherung)
- Management der Lieferkette (z. B. Internationale Organisation für Normung/Internationale Elektrotechnische Kommission (ISO/IEC) 27036)

# Zusätzliche Informationen zur Prüfung

## Ergänzende Quellen

Die Kandidaten werden aufgefordert, ihre Ausbildung und Erfahrung zu erweitern, indem sie relevante Quellen, die den CBK betreffen, einsehen und Themenbereiche finden, die möglicherweise zusätzlicher Aufmerksamkeit bedürfen.

Die gesamte Liste der ergänzenden Quellen finden Sie unterwww.isc2.org/certifications/References.

## Prüfungsrichtlinien und -verfahren

(ISC)² empfiehlt, dass CSSP-Kandidaten die Prüfungsrichtlinien und -verfahren vor der Registrierung durcharbeiten. Lesen Sie die umfassende Aufschlüsselung dieser wichtigen Angaben unter www.isc2.org/Register-for-Exam.

## Rechtliche Hinweise

Bei Fragen zu rechtlichen Richtlinien von (ISC)² wenden Sie sich an die Rechtsabteliung der (ISC)² unter legal@isc2.org.

## Noch Fragen?

(ISC)²-Kandidatendienste
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Amerika
Tel: +1-727-785-0189
E-Mail: info@isc2.org

(ISC)² Asien-Pazifik
Tel: +852-5803-5662
E-Mail: isc2asia@isc2.org

(ISC)² Eurasien
Tel: +44 (0)203-960-7800
E-Mail: info-emea@isc2.org

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