CCSP®

Zertifizierter Cloud-Sicherheitsexperte

ISC2 Certification

Gliederung der Zertifizierungsprüfung

Datum des Inkrafttretens: 1. Oktober 2025

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 Service-Orchestrierung.

Die in der CCSP-Prüfungsübersicht enthaltenen Themen gewährleisten ihre Relevanz für alle Disziplinen im Bereich der Cloud-Sicherheit. Erfolgreiche Kandidaten verfügen über Kompetenzen in den folgenden sechs Bereichen:

- 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 die Erfahrung

Die 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-Prüfungsschemas. Ein postsekundärer Abschluss (Bachelor oder Master) in Informatik, IT oder verwandten Bereichen kann bis zu einem Jahr der erforderlichen Erfahrung ausmachen. Die Erlangung des CCSK-Zertifikats von CSA kann ein Jahr Berufserfahrung ersetzen. Nur ein Jahr Berufserfahrung kann erlassen werden. Ein aktives CISSP-Zertifikat kann die gesamte CCSP-Erfahrung ersetzen. Auch Teilzeitbeschäftigungen und Praktika können auf das Erfordernis der Berufserfahrung angerechnet werden.

Ein Kandidat, der nicht über die erforderliche Erfahrung verfügt, um ein CCSP zu werden, kann ein Associate des ISC2 werden, indem er die CCSP-Prüfung erfolgreich ablegt. Der Associate 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).

Analyse der Arbeitsaufgaben (JTA)

ISC2 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. Dieser Prozess stellt sicher, dass die Kandidaten in den Themenbereichen geprüft werden, die für die Rollen und Verantwortlichkeiten der heutigen Informationssicherheitsexperten mit Schwerpunkt auf Cloud-Technologien relevant sind.

Informationen zur CCSP CAT-Prüfung

Die CCSP-Prüfung erfolgt unter Verwendung von 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
Fragenformat	Multiple-Choice-Fragen und erweiterte Fragetypen
Bestehende Note	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	17 %
5. Cloud-Sicherheitsoperationen	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-Computings

» Rollen und Verantwortlichkeiten beim Cloud-Computing (z. B. Cloud-Service-Kunde, Cloud-Service-Anbieter, Cloud-Service-Partner, Cloud-Service-Broker, Regulierungsbehörde)

» Hauptmerkmale des Cloud-Computings (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)

» Kategorien von Cloud-Diensten (z. B. Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a 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), Überprüfbarkeit, 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, Verkehrskontrolle, 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-Computings

» Sicherer Lebenszyklus von Daten in der Cloud

» Cloud-basierter Business Continuity (BC)- und Disaster Recovery (DR)-Plan

» Analyse der geschäftlichen Auswirkungen (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 as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a 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: 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, flüchtige Speicher, Rohspeicher)
- Bedrohungen für Lagertypen

2.3 Entwurf und Anwendung von Datensicherheitstechnologien und -strategien

- Verschlüsselung und Schlüsselverwaltung
- Hashing
- Datenverschleierung (z. B. Maskierung, Anonymisierung)
- Tokenisierung
- Schutz vor Datenverlust (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
- Datenlabeling

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

- Maßnahmen zur Datenspeicherung
- Verfahren und Mechanismen zur Datenlöschung
- Verfahren und Mechanismen zur Datenarchivierung
- Rechtlicher Halt

2.8 Konzeption und Umsetzung 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 Unleugbarkeit

Bereich 3: Cloud-Plattform und Infrastruktur Sicherheit

3.1 Verstehen von Cloud-Infrastruktur- und Plattformkomponenten

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

3.2 Entwurf eines sicheren Rechenzentrums

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

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 Risikominderung

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
- Audit-Mechanismen (z. B. Protokollerfassung, Korrelation, Paketerfassung)

3.5 Planung von 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, Umsetzung und Prüfung des Plans

Bereich 4: Sicherheit von Cloud-Anwendungen

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 Beschreiben Sie den Prozess des sicheren Softwareentwicklungslebenszyklus (SDLC)

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

4.3 Anwendung des Lebenszyklus für sichere Softwareentwicklung (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))
- Vermeiden Sie häufige 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 Cloud-Software-Sicherung und -Validierung anwenden

- 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 Anwendungsprogrammierschnittstellen (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)

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

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 (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 der 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)

- Management von Veränderungen
- Management von Kontinuität
- Management der Informationssicherheit
- Management der kontinuierlichen Verbesserung der Dienstleistungen
- Management von Zwischenfällen
- Management von Problemen
- Management von Freigaben
- Management der Bereitstellung
- Management der Konfiguration
- Management der Dienstgüte
- Management der Verfügbarkeit
- Management der Kapazitäten

5.4 Unterstützung der digitalen Forensik

- Methoden der forensischen Datenerhebung
- Management von Beweismitteln
- Sammeln, Beschaffen und Sichern digitaler Beweise

5.5 Verwaltung der Kommunikation mit den relevanten Parteien

- Anbieter
- Kunden
- Partner
- Regulierungsbehörden
- Andere Interessengruppen

5.6 Verwaltung von Sicherheitsmaßnahmen

- Sicherheitsoperationszentrum (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. 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. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27050, Cloud Security Alliance (CSA) Guidance)
- Forensische Anforderungen

6.2 Verständnis für Datenschutzprobleme

- Unterschied zwischen vertraglichen und regulierten privaten Daten (z. B. geschützte Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII))
- Länderspezifische Gesetzgebung in Bezug auf private Daten (z. B. geschützte Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII))
- 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 (PIA)

6.3 Verständnis des Auditprozesses, 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 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 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 Risikomanagement von Unternehmen

- Bewertung der Risikomanagementprogramme der Anbieter (z. B. Kontrollen, Methoden, Richtlinien, Risikoprofil, Risikobereitschaft)
- Unterschied zwischen Dateneigentümer/Kontrolleur und Datentreuhänder/Verarbeiter
- Regulatorische Transparenzanforderungen (z. B. Meldung von Verstößen, Sarbanes-Oxley (SOX), Allgemeine Datenschutzverordnung (GDPR))
- Risikobehandlung (d.h. vermeiden, mindern, übertragen, teilen, akzeptieren)
- 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, Zusicherung, Compliance, Zugang zu Cloud/Daten, Versicherung gegen Cyberrisiken)
- Management 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-Prüfungsschema 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 zur Prüfung anmelden. Lesen Sie die umfassende Aufschlüsselung dieser wichtigen Informationen unter www.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