CCSP®

Certified Cloud Security Professional

ISC2 Certification

Zertifizierungs-**Prüfungsübersicht**

Datum des Inkrafttretens: 1. August 2022

ISC2™

Über CCSP

ISC2 hat den Zertifizierten Cloud Security Professional (CCSP) entwickelt, um sicherzustellen, dass Fachleute für Cloud-Sicherheit über die erforderlichen Kenntnisse, Fähigkeiten und Fertigkeiten in Bezug auf das Konzept, die Implementierung, die Architektur, den Betrieb und die Kontrolle der Cloud-Sicherheit sowie die Einhaltung gesetzlicher Vorschriften verfügen. Ein CCSP wendet sein Fachwissen im Bereich Informationssicherheit auf eine Cloud-Computing-Umgebung an und demonstriert seine Kompetenz in den Bereichen Cloud-Sicherheitsarchitektur, Konzept, Betrieb und Service-Orchestrierung. Diese berufliche Kompetenz wird anhand eines weltweit anerkannten Wissensbestands gemessen.

Die Themen, die im CCSP-Korpus des Wissens enthalten sind, gewährleisten seine Relevanz für alle Disziplinen im Bereich der Cloudsicherheit. Erfolgreiche Kandidaten verfügen über Kompetenzen in den folgenden sechs Bereichen:

- Cloud-Konzepte, Architektur und Konzept
- Cloud-Datensicherheit
- Sicherheit der Cloud-Plattform und -Infrastruktur
- Cloud-Anwendungssicherheit
- Cloud-Sicherheitsoperationen
- Recht, Risiko und Compliance

Anforderungen an die Erfahrung

Die Bewerber müssen mindestens fünf Jahre kumulierte Vollzeit-Erfahrung in der Informationstechnologie haben.
Drei Jahre müssen im Bereich Cybersicherheit liegen und ein Jahr in einer oder mehreren der sechs Bereiche des aktuellen CCSP-Prüfungsschemas. Ein postsekundärer Abschluss (Bachelor oder Master) in Informatik, Informationstechnologie (IT) oder verwandten Bereichen kann bis zu einem Jahr der erforderlichen Erfahrung ausmachen. Der Erwerb eines zusätzlichen Nachweises aus der vom ISC2 genehmigten Liste kann ein Jahr Erfahrung in einem oder mehreren der sechs Bereiche der CCSP-Prüfungsübersicht ersetzen. Ein aktives CISSP-Zertifikat kann die gesamte CCSP-Erfahrung ersetzen. Ein Kandidat, der nicht über die erforderliche Erfahrung verfügt, um ein CCSP zu werden, kann ein Mitglied des ISC2 werden, indem er die CCSP-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 CCSP-Erfahrung und zur Anrechnung von Teilzeitarbeit und Praktika finden Sie unter www.isc2.org/Certifications/CCSP/experience-requirements.

Akkreditierung

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

Job-Task-Analyse (JTA)

ISC2 ist gegenüber seinen Mitgliedern verpflichtet, die Relevanz des CC aufrechtzuerhalten. Die Job Task Analysis (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 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.

CCSP-Prüfungsinformationen

Dauer der Prüfung	3 Stunden
Anzahl der Fragen	125
Fragenformat	Mehrfachauswahl
Punktzahl zum Bestehen	700 von 1000 Punkten
Prüfungsverfügbarkeit	Englisch, Chinesisch, Deutsch, Japanisch
Testzentrum	Pearson VUE Testzentrum

CCSP-Prüfungsgewichtungen

Bereiche	Gewichtung
1. Cloud-Konzepte, Architektur und Konzept	17 %
2. Cloud-Datensicherheit	20 %
3. Sicherheit der Cloud-Plattform und -Infrastruktur	17 %
4. Cloud-Anwendungssicherheit	17 %
5. Cloud-Sicherheitsoperationen	16 %
6. Recht, Risiko und Compliance	13 %
Gesamt:	**100 %**

Bereich 1: Cloud-Konzepte, Architektur und Konzept

1.1 Verstehen von Cloud Computing-Konzepten

» Definitionen von Cloud Computing

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

» Wichtige Merkmale des Cloud Computing (z. B. Selfservice auf Abruf, breiter Netzwerkzugang, Mandantenfähigkeit, schnelle Elastizität und Skalierbarkeit, Ressourcenpooling, gemessener Service)

» Bausteintechnologien (z. B. Virtualisierung, Speicherung, Netzwerke, Datenbanken, Orchestrierung)

1.2 Beschreiben der Cloud-Referenzarchitektur

» Aktivitäten im Cloud Computing

» Cloud-Service-Fähigkeiten (z. B. Arten von Anwendungsfähigkeiten, Arten von Plattformfähigkeiten, Arten von Infrastrukturfähigkeiten)

» Kategorien von Cloud-Services (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS))

» Cloud-Bereitstellungsmodelle (z. B. öffentliche, private, hybride, gemeinschaftliche, Multi-Cloud)

» Gemeinsame Überlegungen zur Cloud (z. B. Interoperabilität, Portabilität, Reversibilität, Verfügbarkeit, Sicherheit, Datenschutz, Ausfallsicherheit, Performance, Governance, Wartung und Versionierung, Service-Levels und Service-Level-Agreements (SLA), Auditierbarkeit, Regulierung, Outsourcing)

» Überlegungen zur gemeinsamen Nutzung der Cloud (z. B. Interoperabilität, Portabilität, Reversibilität, Verfügbarkeit, Sicherheit, Datenschutz, Ausfallsicherheit, Performance, Governance, Wartung und Versionierung, Service-Levels und Service-Level-Agreements (SLA), Auditierbarkeit, Regulierung, Outsourcing)

1.3 Verstehen von Sicherheitskonzepten, die für Cloud Computing relevant sind

» Kryptografie und Schlüsselverwaltung

» Identitäts- und Zugriffskontrolle (z. B. Benutzerzugriff, Zugriff auf Privilegien, Zugriff auf Dienste)

» Daten- und Mediensanierung (z. B. Überschreiben, kryptografisches Löschen)

» Netzwerksicherheit (z. B. Netzwerksicherheitsgruppen, Traffic Inspection, Geofencing, Zero Trust Network)

» Virtualisierungssicherheit (z. B. Hypervisor-Sicherheit, Container-Sicherheit, ephemeres Computing, serverlose Technologie)

» Allgemeine Bedrohungen

» Sicherheitshygiene (z. B. Patching, Baselining)

1.4 Verstehen von Konzepten für sicheres Cloud Computing

» Sicherer Lebenszyklus von Daten in der Cloud

» Cloud-basierter Plan für Geschäftskontinuität (BC) und Notfallwiederherstellung (DR)

» Business-Impact-Analyse (BIA) (z. B. Kosten-Nutzen-Analyse, Return on Investment (ROI))

» Funktionale Sicherheitsanforderungen (z. B. Portabilität, Interoperabilität, Anbieterbindung)

» Sicherheitsüberlegungen und Verantwortlichkeiten für verschiedene Cloud-Kategorien (z. B. Software als Service (SaaS), Infrastructure als Service (IaaS), Plattform als Service (PaaS))

» Entwurfsmuster für die Cloud (z. B. SANS-Sicherheitsprinzipien, Well-Architected Framework, Cloud Security Alliance (CSA) Enterprise-Architektur)

» DevOps-Sicherheit

1.5 Bewerten von Cloud-Service-Anbietern

» Überprüfung anhand von Kriterien (z. B. International Organization for Standardization/International Electrotechnical Commission (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: Cloud-Datensicherheit

2.1 Beschreiben von Konzepten für Cloud-Daten

- Phasen des Lebenszyklus von Cloud-Daten
- Datenstreuung
- Datenflüsse

2.2 Entwurf und Implementierung von Cloud-Datenspeicherarchitekturen

- Speichertypen (z. B. Langzeitspeicher, flüchtige Speicher, Rohspeicher)
- 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 (Data loss prevention, DLP)
- Verwaltung von Schlüsseln, Geheimnissen und Zertifikaten

2.4 Implementierung der Datenermittlung

- Strukturierte Daten
- Unstrukturierte Daten
- Semi-strukturierte Daten
- Standort der Daten

2.5 Planung und Umsetzung der Datenklassifizierung

- Richtlinien zur Datenklassifizierung
- Datenzuordnung
- Kennzeichnung von Daten

2.6 Entwurf und Implementierung von Information Rights Management (IRM)

- Zielsetzungen (z. B. Datenrechte, Bereitstellung, Zugriffsmodelle)
- Geeignete Tools (z. B. Ausstellung und Widerruf von Zertifikaten)

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

- Richtlinien zur Datenaufbewahrung
- Verfahren und Mechanismen zur Löschung von Daten
- Verfahren und Mechanismen zur Datenarchivierung
- Gesetzliche Aufbewahrung

2.8 Entwurf und Implementierung von Prüfbarkeit, Rückverfolgbarkeit und Verantwortlichkeit von Datenereignissen

- Definition von Ereignisquellen und Anforderung von Ereignisattributen (z. B. Identität, Internet Protocol (IP)-Adresse, Geolocation)
- Protokollierung, Speicherung und Analyse von Datenereignissen
- Aufbewahrungskette und Nichtabstreitbarkeit

Bereich 3: Cloud-Plattform und -Infrastruktur Sicherheit

3.1 Verstehen von Komponenten der Cloud-Infrastruktur und -Plattform

- Physische Umgebung
- Netzwerk und Kommunikation
- Compute
- Virtualisierung
- Speicher
- Verwaltungsebene

3.2 Entwurf eines sicheren Rechenzentrums

- Logischer Entwurf (z. B. Mandantenpartitionierung, Zugriffskontrolle)
- Physischer Entwurf (z. B. Standort, Kauf oder Bau)
- Entwurf der Umgebung (z. B. Heizung, Lüftung und Klimaanlage (HLK), Konnektivität mit mehreren Anbietern)
- Belastbarer Entwurf

3.3 Analyse der mit der Cloud-Infrastruktur und den Plattformen verbundenen Risiken

- 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 Umgebungsschutz (z. B. vor Ort)
- System-, Speicher- und Kommunikationsschutz
- Identifizierung, Authentifizierung und Autorisierung in Cloud-Umgebungen
- Audit-Mechanismen (z. B. Protokollerfassung, Korrelation, Paketaufzeichnung)

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

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

Bereich 4: Cloud-Anwendungssicherheit

4.1 Förderung von Schulungen und Sensibilisierung für 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 SDLC-Prozesses (Secure Software Development Life Cycle)

- Geschäftsanforderungen
- 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
- Bedrohungsmodelle (z. B. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE), Disaster, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD), Architecture, Threats, Attack Surfaces, and Mitigations (ATASM), Process for Attack Simulation and Threat Analysis (PASTA))
- Vermeidung häufiger Schwachstellen bei der Entwicklung
- Sichere Codierung (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 von Cloud-Software-Assurance und -Validierung

- Funktionale und nicht-funktionale Tests
- Methoden für Sicherheitstests (z. B. Blackbox, Whitebox, statisch, dynamisch, Software Composition Analysis (SCA), interaktives Testen der Anwendungssicherheit (IAST))
- Qualitätssicherung (QS)
- Testen von Missbrauchsfällen

4.5 Verwenden von geprüfter sicherer Software

- Absicherung von Programmierschnittstellen (API)
- Supply-Chain-Management (z B. Lieferantenbewertung)
- Verwaltung der Software von Drittanbietern (z. B. Lizenzierung)
- Validierte Open-Source-Software

4.6 Verstehen von Einzelheiten der Architektur von Cloud-Anwendungen

- Ergänzende Sicherheitskomponenten (z. B. Webanwendungs-Firewall (WAF), Datenbankaktivitätsüberwachung (DAM), Extensible Markup Language (XML)-Firewalls, Application Programming Interface (API)-Gateway)
- Kryptografie
- Sandboxing
- Anwendungsvirtualisierung und Orchestrierung (z. B. Microservices, Container)

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

- Verbundidentität
- Identitätsanbieter (IdP)
- Einmalige Anmeldung (Single sign-on, 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 Fernzugriff (z. B. Remote Desktop Protocol (RDP), sicherer Terminalzugriff, Secure Shell (SSH), konsolenbasierte Zugriffsmechanismen, Jumpboxen, virtuelle Clients)
- 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 Systeme (IDS), Intrusion Prevention Systeme (IPS), Honeypots, Schwachstellenbewertungen, Netzwerksicherheitsgruppen, Bastion Host)
- Härtung von Betriebssystemen (OS) durch die Anwendung von Baselines, Überwachung und Abhilfemaßnahmen (z. B. Windows, Linux, VMware)
- Patch-Management
- Strategie für Infrastruktur als Code (IaC)
- Verfügbarkeit von geclusterten Hosts (z. B. verteilte Ressourcenplanung, dynamische Optimierung, Speichercluster, Wartungsmodus, hohe Verfügbarkeit (HV))
- Verfügbarkeit des Gastbetriebssystems (OS)
- Überwachung von Performance und Kapazität (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. Planung, Orchestrierung, Wartung)

5.3 Implementierung von Betriebskontrollen und Standards (z. B. Information Technology Infrastructure Library (ITIL), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20000-1)

- Änderungsmanagement
- Kontinuitätsmanagement
- Management der Informationssicherheit
- Management der kontinuierlichen Serviceverbesserung
- Management von Zwischenfällen
- Problem-Management
- Release-Management
- Bereitstellungsmanagement
- Konfigurationsmanagement
- Service-Level-Management
- Verfügbarkeitsmanagement
- Kapazitätsmanagement

5.4 Unterstützung digitaler Forensik

- Methoden der forensischen Datenerfassung
- Beweismittel-Management
- Sammeln, Beschaffen und Bewahren digitaler Beweise

5.5 Verwaltung der Kommunikation mit relevanten Parteien

- Anbieter
- Kunden
- Partner
- Regulierungsbehörden
- Andere Stakeholder

5.6 Verwaltung von Sicherheitsoperationen

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

Bereich 6: Recht, Risiko und Compliance

6.1 Formulierung rechtlicher Anforderungen und einzigartiger Risiken innerhalb der Cloud-Umgebung

- Widersprüchliche internationale Gesetzgebung
- Bewertung der für Cloud Computing spezifischen rechtlichen Risiken
- Rechtlicher Rahmen und Richtlinien
- eDiscovery (z. B. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27050, Cloud Security Alliance (CSA) Guidance)
- Forensische Anforderungen

6.2 Verstehen von Fragen des Datenschutzes

- Unterschied zwischen vertraglichen und regulierten privaten Daten (z. B. geschützte Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII))
- Länderspezifische Gesetzgebung in Bezug auf personenbezogene Daten (z .B. geschützte Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII))
- Juristische Unterschiede beim Datenschutz
- Standard-Datenschutzanforderungen (z. B. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27018, Generally Accepted Privacy Principles (GAPP), General Data Protection Regulation (GDPR))
- Datenschutz-Folgenabschätzungen („Privacy Impact Assessment", PIA)

6.3 Verstehen des Audit-Prozesses, der Methoden und der erforderlichen Anpassungen für eine Cloud-Umgebung

- Interne und externe Audit-Kontrollen
- Auswirkungen von Audit-Anforderungen
- Identifizierung der Sicherheitsherausforderungen 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 Prüfungsumfangs (z. B. Statement on Standards for Attestation Engagements (SSAE), International Standard on Assurance Engagements (ISAE))
- Lückenanalyse (z. B. Kontrollanalyse, Baselines)
- Audit-Planung
- Internes System zur Verwaltung der Informationssicherheit
- 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 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/Kontrolleur vs. Datentreuhänder/Verarbeiter
- Regulatorische Transparenzanforderungen (z. B. Benachrichtigung bei Verstößen, Sarbanes-Oxley (SOX), General Data Protection Regulation (GDPR))
- Risikobehandlung (d. h. vermeiden, abmildern, übertragen, teilen, akzeptieren)
- Unterschiedliche Risiko-Rahmenwerke
- Metriken für das Risikomanagement
- Bewertung der Risikoumgebung (z. B. Service, Anbieter, Infrastruktur, Unternehmen)

6.5 Verstehen des Entwurfs von Outsourcing- und Cloud-Verträgen

- Geschäftsanforderungen (z. B. Service Level Agreement (SLA), Master Service Agreement (MSA), Statement of Work (SOW))
- Anbietermanagement (z. B. Anbieterbewertungen, Risiken der Anbieterbindung, Lebensfähigkeit der Anbieter, 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 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) 58035662
E-Mail: isc2asia@isc2.org

Europa, Naher Osten und Afrika
Tel: +44 (0) 203-960-7800
E-Mail: info-emea@isc2.org