CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

Überblick über die **Zertifizierungsprüfung**

Gültig ab: 1. Mai 2021

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

Zum CISSP

Das Zertifikat zum zertifizierten Sicherheitsexperten für Informationssysteme („Certified Information Systems Security Professional", CISSP) gilt als eines der weltweit am höchsten bewerteten Zertifikate auf dem Markt der Informationssicherheit. Der CISSP bescheinigt einem Informationssicherheitsexperten umfangreiche technische und organisatorische Kenntnisse sowie die Erfahrung zum effektiven Entwerfen, Entwickeln und Planen aller firmeninternen Sicherheitsanforderungen.

Das weitreichende Themenspektrum im CISSP Common Body of Knowledge (CBK®) soll dessen Bedeutung für alle Themenfelder der Informationssicherheit unterstreichen. Zertifizierte Kandidaten sind erfahren in den nachfolgenden acht Fachgebieten:

- Sicherheits- und Risikomanagement
- Sicherheit der Vermögenswerte
- Sicherheitsarchitektur und -technik
- Kommunikations- und Netzwerksicherheit
- Identitäts- und Zugriffsverwaltung
- Sicherheitsbewertung und -prüfung
- Sicherheitsabläufe
- Softwareentwicklungssicherheit

Anforderungen an die Berufserfahrung

Die Kandidaten benötigen mindestens fünf Jahre Berufserfahrung in mindestens zwei der acht Bereiche des CISSP-CBKs. Der Erwerb eines Hochschulabschlusses mit mindestens vierjähriger Ausbildung oder eines gleichwertigen landesspezifischen Abschlusses oder eines Zusatzzeugnisses von der durch die (ISC)² genehmigten Liste entspricht einem Jahr Berufserfahrung. Die Anrechnung der Ausbildung kann nur ein Jahr Berufserfahrung ersetzen.

Eine Kandidatin oder ein Kandidat, die/der nicht über die erforderliche Berufserfahrung verfügt, um ein CISSP zu werden, kann durch Bestehen der CISSP-Prüfung zum Associate of (ISC)² werden. Dem Associate of (ISC)² verbleiben ab diesem Zeitpunkt sechs Jahre zum Erwerb der fünfjährigen Berufserfahrung. Weitere Informationen über die Voraussetzungen zur CISSP-Berufserfahrung und über die Anrechnung von Teilzeitarbeit und Praktika finden Sie unter www.isc2.org/Certifications/CISSP/experience-requirements.

Akkreditierung

CISSP war das erste Diplom im Bereich der Informationssicherheit, das die strengen Anforderungen des ANSI/ISO/IEC-Standards 17024 erfüllte.

Arbeitsaufgabenanalyse

(ISC)² hat die Verpflichtung gegenüber seinen Mitgliedern, die Praxisrelevanz des CISSP sicherzustellen. Die regelmäßig erfolgende Arbeitsaufgabenanalyse (AAA) ist ein systematisches und kritisches Verfahren zur Bestimmung der Aufgaben von Sicherheitsexperten im durch den CISSP definierten Beruf. Die Ergebnisse der AAA dienen der Aufbereitung der Prüfung auf den jeweils neuestem Stand. Dieses Verfahren gewährleistet, dass die Kandidaten in denjenigen Themenbereichen geprüft werden, die für ihre Funktionen und Zuständigkeiten als Experten für Informationssicherheit im heutigen Berufsalltag von Bedeutung sind.

Angaben zur CISSP-CAT-Prüfung

Die CISSP-Prüfung nutzt für die englischsprachige Prüfung das Computerized Adaptive Testings (CAT). In allen anderen Sprachen bestehen CISSP-Prüfungen aus einer festen Anzahl von Fragen pro Fachgebiet. Mehr über CISSP-CAT finden Sie unter www.isc2.org/certificatons/CISSP-CAT.

Prüfungsdauer	4 Stunden
Anzahl der Fragen	125-175
Aufbau der Prüfung	Mehrfachauswahl und weitere innovative Fragetechniken
Mindestpunktzahl	700 von 1000 Punkten
Verfügbarkeit der Prüfungssprache	Englisch
Prüfungsort	(ISC)² Autorisierte Prüfungszentren PPC and PVTC Select Pearson VUE

Gewichtungsverteilungen bei CISSP-CAT-Prüfungen

Fachgebiete	Durchschnittsgewichtung
1. Sicherheits- und Risikomanagement	15 %
2. Sicherheit der Vermögenswerte	10 %
3. Sicherheitsarchitektur und -technik	13 %
4. Kommunikations- und Netzwerksicherheit	13 %
5. Identitäts- und Zugriffsverwaltung	13 %
6. Sicherheitsbewertung und -prüfung	12 %
7. Sicherheitsabläufe	13 %
8. Softwareentwicklungssicherheit	11 %
Summe:	**100 %**

Angaben zur linearen CISSP-Prüfung

Prüfungsdauer	6 Stunden
Anzahl der Fragen	250
Aufbau der Prüfung	Mehrfachauswahl und weitere innovative Fragetechniken
Mindestpunktzahl	700 von 1000 Punkten
Verfügbarkeit der Prüfungssprache	Vereinfachtes Chinesisch, Deutsch, Koreanisch, Japanisch, modernes Spanisch
Prüfungsort	(ISC)² Autorisierte Prüfungszentren PPC and PVTC Select Pearson VUE

Gewichtungsverteilungen bei Linearen CISSP-Prüfungen

Fachgebiete	Gewichtung
1. Sicherheits- und Risikomanagement	15 %
2. Sicherheit der Vermögenswerte	10 %
3. Sicherheitsarchitektur und -technik	13 %
4. Kommunikations- und Netzwerksicherheit	13 %
5. Identitäts- und Zugriffsverwaltung	13 %
6. Sicherheitsbewertung und -prüfung	12 %
7. Sicherheitsabläufe	13 %
8. Softwareentwicklungssicherheit	11 %
Summe:	**100 %**

Fachgebiet 1: Sicherheits- und Risikomanagement

1.1 Berufsethos verstehen, einhalten und fördern

» (ISC)² -Kodex der Berufsethik
» Organisatorischer Ethikkodex

1.2 Sicherheitskonzepte verstehen und anwenden

» Vertraulichkeit, Integrität und Verfügbarkeit, Authentizität und Nichtabstreitbarkeit

1.3 Grundsätze der Sicherheitsführung bewerten und anwenden

» Ausrichtung der Sicherheitsfunktion auf Geschäftsstrategie, Ziele und Auftrag
» Verwaltungsabläufe (z. B. Zukäufe, Veräußerungen, Führungsgremien)
» Verwaltungsrollen und -zuständigkeiten
» Rahmenbedingungen für die Sicherheitskontrolle
» Sorgfaltspflicht

1.4 Vorschriften und andere Anforderungen bestimmen

» Vertragliche, rechtliche, normgerechte und behördliche Anforderungen
» Anforderungen an den Datenschutz

1.5 Rechtliche und behördliche Auflagen zur Informationssicherheit in einem ganzheitlichen Kontext

» Cyberkriminalität und Datenschutzverletzungen
» Anforderungen an Lizenzierung und geistiges Eigentum
» Import-/Exportkontrolle
» Grenzüberschreitender Datenfluss
» Datenschutz

1.6 Anforderungen an Untersuchungstypen (d. h. verwaltungstechnische, straf- und zivilrechtliche, behördliche und normgerechte)

1.7 Sicherheitsrichtlinien, Normen, Verfahren und Leitfäden entwickeln, dokumentieren und einführen

1.8 Anforderungen an die Geschäftskontinuität erkennen, analysieren und einstufen

- Business-Impact-Analyse (BIA)
- Umfang und Zeitplan entwickeln und dokumentieren

1.9 Mitwirkung an und Durchsetzung von Richtlinien und Verfahren zur Personalsicherheit

- Prüfung und Einstellung von Bewerbern
- Beschäftigungsverträge und -richtlinien
- Einführungs-, Versetzungs- und Kündigungsverfahren
- Vereinbarungen und Kontrollen von Zulieferern, Beratern und Auftragnehmern
- Anforderungen zur Einhaltung von Vorschriften
- Anforderungen an den Datenschutz

1.10 Konzepte des Risikomanagements verstehen und anwenden

- Identifizierung von Gefahren und Schwachstellen
- Risikoabschätzung/-analyse
- Risikobehandlung
- Auswahl und Durchführung der Gegenmaßnahme
- Geltende Kontrollmechanismen (z. B. präventiv, aufdeckend, behebend)
- Kontrollbewertungen (Sicherheit und Datenschutz)
- Überwachung und Messung
- Berichtswesen
- Stetige Verbesserung (z. B. Modellierung der Risikoreife)
- Risikorahmenbedingungen

1.11 Konzepte und Methoden der Gefahrenmodellierung verstehen und anwenden

1.12 Konzepte des Supply Chain Risikomanagements (SCRM) anwenden

- Risiken im Zusammenhang mit Hardware, Software und Diensten
- Bewertung und Überwachung durch Dritte
- Mindestsicherheitsanforderungen
- Dienstleistungsvereinbarungsanforderungen

1.13 Einrichtung und Durchführung eines Programms für Sicherheitsbewusstsein, Aus- und Fortbildung

- Verfahren und Techniken zur Darstellung von Sensibilisierung und Fortbildung (z. B. Social Engineering, Phishing, Sicherheits-Champions, Gamifizierung)
- Regelmäßige Überprüfung der Inhalte
- Bewertung der Effizienz des Programms

Fachgebiet 2: Sicherheit der Vermögenswerte

2.1 Identifizieren und Klassifizieren von Informationen und Vermögenswerten

- Datenklassifizierung
- Klassifizierung von Vermögenswerten

2.2 Anforderungen an die Handhabung von Informationen und Vermögenswerten

2.3 Ressourcen abgesichert anbieten

- Zuständigkeiten bei Informationen und Vermögenswerten
- Inventarisierung von Vermögenswerten (z. B. materiell, immateriell)
- Verwaltung von Vermögenswerten

2.4 Verwalten des Datenlebenszyklus

- Datenfunktionen (d. h. Verantwortliche, Bearbeiter, Verwahrer, Verarbeiter, Benutzer/ Subjekte)
- Datensammlung
- Datenspeicherung
- Datenpflege
- Datenaufbewahrung
- Datenremanenz
- Datenlöschung

2.5 Aufrechterhaltung geeigneter Bewahrung der Vermögenswerte (z. B. Ausmusterung, Einstellung des Kundendienstes [End of life])

2.6 Anforderungen an Datensicherheitskontrollen und -vorschriften bestimmen

- Datenzustände (z. B. in use, in transit, at rest)
- Umfang und Anpassung
- Normenauswahl
- Datenschutzverfahren (z. B. Digitale Rechteverwaltung (DRM), Verhinderung von Datenverlust (DLP), Cloud Access Security Broker (CASB))

Fachgebiet 3: Sicherheitsarchitektur und -technik

3.1 Recherchieren, Einführen und Verwalten von technischen Vorgängen unter sicheren Entwurfsprinzipien

- Modellierung von Gefahren
- Geringstes Privileg
- Verteidigung in der Tiefe
- Sicherheitsvorgaben
- Ausfallsicherung
- Aufgabentrennung
- Einfachheit
- Zero Trust
- Datenschutz durch Design (Privacy by design)
- Überprüftes Vertrauen
- Geteilte Verantwortung

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

3.3 Kontrollen anhand der Anforderungen an die Systemsicherheit wählen

3.4 Verstehen der Sicherheitskapazitäten von Informationssystemen (z. B. Speicherschutz, Trusted Platform Module (TPM), Ver-/Entschlüsselung)

3.5 Schwachstellen von Sicherheitsarchitekturen, Entwürfen und Lösungselementen abschätzen und beheben

- Client-gestützte Systeme
- Server-gestützte Systeme
- Datenbanksysteme
- Kryptographische Systeme
- Industrielle Steuersysteme
- Cloud-gestützte Systeme (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS))
- Verteilte Systeme
- Internet der Dinge (IoT)
- Mikroservices
- Containerisierung
- Serverlos
- Eingebettete Systeme
- Hochleistungsrechnersysteme (High Performance Computing, HPC)
- Edge-Computing-Systeme
- Virtualisierte Systeme

3.6 Kryptographische Lösungen auswählen und bestimmen

- Kryptographischer Lebenszyklus (z. B. Schlüssel, Auswahl des Algorithmus)
- Kryptographische Verfahren (z. B. symmetrische, asymmetrische, elliptische Kurven, Quanten)
- Public-Key-Infrastruktur (PKI)
- Wichtige Verwaltungspraktiken
- Digitale Signaturen und elektronische Zertifikate
- Nichtabstreitbarkeit
- Integrität (z. B. Hashing)

3.7 Methoden kryptoanalytischer Angriffe verstehen

- Brute Force
- Nur Chiffretext
- Bekannter Klartext
- Häufigkeitsanalyse
- Ausgewählter Chiffretext
- Angriffe auf die Umsetzung
- Seitenkanal
- Fehlerinjektion
- Zeitpunkt
- Mittelsmann (Man in the middle)
- Erweitere Passwortattacken
- Kerberos-Ausnutzung
- Lösegeldforderung

3.8 Sicherheitsgrundsätze auf den Entwurf von Anlagen und Einrichtungen anwenden

3.9 Sicherheitskontrollen für Anlagen und Einrichtungen entwerfen

- Verteilerschränke/Zwischenverteileranlagen
- Server-Räume/Rechenzentren
- Einrichtungen zur Medienspeicherung
- Beweissicherung
- Absichern von Sperr- und Arbeitsbereichen
- Einrichtung und Heizung, Lüftung und Klimatisierung (HVAC)
- Umweltfragen
- Brandverhütung, -erkennung und -bekämpfung
- Stromversorgung (z. B. redundant, Notstrom)

Fachgebiet 4: Kommunikations- und Netzwerksicherheit

4.1 Bewertung und Einführung sicherer Entwurfsprinzipien in Netzwerkarchitekturen

- Modelle der offenen Systemverbindung (OSI) und des Transmission Control Protocol/Internet Protocol (TCP/IP)
- Internet Protocol (IP)-Netzwerke (z.B. Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)
- Sichere Protokolle
- Implikationen von Mehrschichtprotokollen
- Konvergierte Protokolle (z. B. Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))
- Mikro-Segmentierung (z. B. Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Kapselung, software-definiertes Wide Area Network (SD-WAN))
- Drahtlose Netze (z. B. Li-Fi, WLAN, Zigbee, Satellit)
- Mobiltelefonnetze (z. B. 4G, 5G)
- Content Distribution Networks (CDN)

4.2 Netzwerkkomponenten absichern

- Betrieb von Hardware (z. B. redundante Stromversorgung, Garantie, Kundendienst)
- Übertragungsmedien
- Geräte für Netzwerkzugriffskontrolle
- Sicherheit am Endpunkt

4.3 Einführung abgesicherter Kommunikationskanäle entsprechend dem Entwurf

- Sprachübertragung
- Multimedia-Zusammenarbeit
- Fernzugriff
- Datenkommunikation
- Virtualisierte Netzwerke
- Konnektivität von Drittanbietern

Fachgebiet 5: Identitäts- und Zugriffsverwaltung

5.1 Physikalischen und logischen Zugriff auf Vermögenswerte kontrollieren

- Informationen
- Systeme
- Geräte
- Einrichtungen
- Anwendungen

5.2 Verwalten der Identifikation und Authentifizierung von Personen, Geräten und Diensten

- Implementierung von Identitätsmanagement (IdM)
- Einzel-/Multifaktorauthentifizierung (MFA)
- Verantwortlichkeit
- Verwaltung von Sitzungen
- Registrierung, Nachweis und Feststellung der Personalien
- Identitätsmanagement im Verbund
- Systeme zur Verwaltung von Anmeldedaten
- Einmalige Anmeldung (SSO)
- Just-in-Time (JIT)

5.3 Verbundidentität mit einem Drittdienst

- Lokal
- Cloud
- Hybrid

5.4 Autorisierungsmechanismen einrichten und verwalten

- Rollenbasierte Zugriffskontrolle (RBAC)
- Regelbasierte Zugriffskontrolle
- Zwingende Zugangskontrolle
- Benutzerbestimmbare Zugriffskontrolle
- Attributbasierte Zugriffskontrolle
- Risikobasierte Zugriffskontrolle

5.5 Lebenszyklus des Angebots von Personalien und Zugriffen verwalten

- Überprüfung des Zugriffs auf Konten (z. B. Benutzer, System, Dienst)
- Beschaffung und Entlassung (z. B. Einstellung, Kündigung, Überstellung)
- Rollendefinition (z. B. Personen, die neuen Rollen zugeordnet sind)
- Privilegienerweiterung (z. B. verwaltete Konten, Nutzung von Sudo, Minimierung der Nutzung)

5.6 Authentifizierungssysteme einführen

- OpenID Connect (OIDC)/Open Authorization (Oauth)
- Security Assertion Markup Language (SAML)
- Kerberos
- Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)

Fachgebiet 6: Sicherheitsbewertung und -prüfung

6.1 Entwurf und Validierung von Beurteilungs-, Test- und Prüfstrategien

- Intern
- Extern
- Drittpartei

6.2 Sicherheitskontrolltests vollziehen

- Bewertung der Verwundbarkeit
- Eindringprüfung
- Protokollprüfung
- Synthetische Transaktionen
- Code überprüfen und testen
- Prüfung von Missbrauchsfällen
- Analyse des Testumfangs
- Schnittstellenprüfung
- Simulationen von Verstößen
- Konformitätsprüfungen

6.3 Daten über Sicherheitsverfahren erheben (z. B. technische und administrative Daten)

- Kontenverwaltung
- Überprüfung und Genehmigung durch das Management
- Wesentliche Leistungs- und Risikokennzahlen
- Verifikationsdaten sichern
- Ausbildung und Sensibilisierung
- Notfallwiederherstellung und Geschäftskontinuität

6.4 Testergebnisse analysieren und Berichtserstellung

- Wiederherstellung
- Behandlung von Ausnahmen
- Ethische Offenlegung

6.5 Sicherheitsaudits durchführen oder erleichtern

- Intern
- Extern
- Drittpartei

Fachgebiet 7: Sicherheitsabläufe

7.1 Untersuchungen verstehen und weiter verfolgen

- Beweiserhebung und -bearbeitung
- Berichtswesen und Dokumentation
- Ermittlungstechniken
- Werkzeuge, Taktiken und Verfahren der digitalen Forensik
- Artefakte (z. B. Computer, Netzwerk, Mobilgerät)

7.2 Protokollierungs- und Überwachungsaktivitäten durchführen

- Erkennung und Abwehr von Eindringlingen
- Sicherheitsinformationen und Ereignisverwaltung
- Durchgehende Überwachung
- Überwachung der Ausgänge
- Protokollverwaltung
- Bedrohungsaufklärung (z. B. Bedrohungsfeeds, Bedrohungsaufspürung)
- Analyse des Benutzer- und Entitätsverhaltens

7.3 Konfigurationsmanagement durchführen (z. B. Beschaffung, Grundausstattung, Automatisierung)

7.4 Grundlegende Konzepte für Sicherheitsabläufe

- Unabdingbare Kenntnisse/Geringste Privilegien
- Trennung von Aufgaben und Zuständigkeiten
- Verwaltung privilegierter Konten
- Arbeitsplatzrotation
- Service Level Agreements (SLAs)

7.5 Ressourcenschutz anwenden

- Medienverwaltung
- Medienschutzverfahren

7.6 Vorfallmanagement durchführen

- Erkennung
- Behandlung
- Milderung
- Berichtswesen
- Wiederherstellung
- Abhilfe
- Gewonnene Erkenntnisse

7.7 Aufdeckende und präventive Maßnahmen betreiben und verwalten

- Firewalls (z.B. nächste Generation, Webanwendung, Netzwerk)
- Angrifferkennungs- und -abwehrsysteme
- Freigabe-/Sperrliste
- Von Dritten angebotene Sicherheitsdienste
- Sandboxen
- Honeypots/Honeynets
- Antimalware
- Werkzeuge für maschinelles Lernen und künstliche Intelligenz (KI)

7.8 Patch- und Schwachstellenmanagement einführen und betreuen

7.9 Verstehen und Mitwirken bei Change Management Prozessen

7.10 Abhilfestrategien umsetzen

- Datensicherungsstrategien
- Wiederherstellungsstrategien
- Mehrfachverarbeitungsorte
- Systemstabilität, Hochverfügbarkeit, Servicequalität und Fehlertoleranz

7.11 Notfallwiederherstellung umsetzen

- Behandlung
- Personal
- Mitteilungen
- Bewertung
- Wiederaufbau
- Ausbildung und Sensibilisierung
- Gelernte Lektionen

7.12 Notfallwiederherstellungspläne testen

- Kenntnisnahme
- Begehung
- Simulation
- Parallel
- Vollständige Unterbrechung

7.13 Teilnahme an Planungen und Übungen zur Geschäftskontinuität

7.14 Physische Sicherheit umsetzen und verwalten

- Perimeter-Sicherheitskontrollen
- Interne Sicherheitskontrollen

7.15 Bedenken hinsichtlich der Sicherheit und des Schutzes von Personal ausräumen

- Reisen
- Sicherheitsausbildung und Sensibilisierung
- Krisenmanagement
- Belastung

Fachgebiet 8: Softwareentwicklungssicherheit

8.1 Sicherheit im Software Development Life Cycle (SDLC) verstehen und einplanen

- Entwicklungsverfahren (z. B. Agile, Wasserfall, DevOps, DevSecOps)
- Reifegradmodelle (z. B. Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
- Bedienung und Wartung
- Änderungsverwaltung
- Integrated Product Team (IPT)

8.2 Sicherheitskontrollen in Ökosystemen der Software-Entwicklung erkennen und anwenden

- Programmiersprachen
- Bibliotheken
- Werkzeugsätze
- Integrierte Entwicklungsumgebung
- Laufzeit
- Kontinuierliche Integration und Lieferung
- Sicherheits-Orchestrierung, Automatisierung und Reaktion
- Softwarekonfigurationsmanagement
- Codebestände
- Anwendungssicherheitstests (z. B. statische, dynamische)

8.3 Effizienz der Softwaresicherheit bewerten

- Auditierung und Protokollierung von Änderungen
- Risikoanalyse und -milderung

8.4 Bewertung der Sicherheitsauswirkungen der erworbenen Software

- kommerzielle Standardtechnik
- Open Source
- Drittpartei
- Verwaltete Systeme (z. B. Software als Service (SaaS), Infrastruktur als Service (IaaS), Plattform als Service (PaaS))

8.5 Sichere Kodierungsrichtlinien und -normen definieren und anwenden

- Sicherheitsschwächen und -schwachstellen auf Quellcodeebene
- Sicherheit von Programmierschnittstellen
- Sichere Kodierungspraktiken
- Softwaredefinierte Sicherheit

Zusätzliche Angaben zur Prüfung

Ergänzende Quellen

Die Kandidaten sind angehalten, 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 ist unter www.isc2.org/certifications/References aufgeführt.

Prüfungsrichtlinien und -verfahren

(ISC)² empfiehlt, dass CISSP-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 Auskünfte

Bei Fragen zu (ISC)²s rechtlichen Vorgaben wenden Sie sich an die Rechtsabteilung der (ISC)² unter legal@isc2.org.

Noch Fragen?

(ISC)² Candidate Services
625 N. Washington Street, Suite 400
Alexandria, VA 22314

(ISC)² Amerika
Tel: +1-866-331-ISC2 (4722)
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