Certified in Cybersecurity

ISC2 Certification

Zertifizierungsprüfung **Übersicht**

Datum des Inkrafttretens: 1. September 2026

ISC2

Über die Zertifizierung in Cybersicherheit

Mit dem Titel Zertifizierung in Cybersicherheit (CC) weisen Sie gegenüber Arbeitgebern nach, dass Sie über die grundlegenden Kenntnisse, Fähigkeiten und Fertigkeiten verfügen, die für eine Stelle auf Einstiegs- oder Junior-Level im Bereich Cybersicherheit erforderlich sind. Sie zeigen damit, dass Sie die grundlegenden Best Practices, Richtlinien und Verfahren im Bereich Sicherheit verstehen und bereit und in der Lage sind, mehr zu lernen und sich im Beruf weiterzuentwickeln.

Die Prüfung umfasst fünf Bereiche:

- Sicherheitsprinzipien
- Sicherheits-Governance
- Konzepte der Identitäts- und Zugriffsverwaltung (IAM)
- Netzwerk- und Cloud-Sicherheitskonzepte
- Sicherheitsmaßnahmen und Reaktion auf Zwischenfälle

Erfahrungsanforderungen

Es gibt keine besonderen Voraussetzungen für die Teilnahme an der Prüfung. Es wird empfohlen, dass die Kandidaten über Grundkenntnisse der Informationstechnologie (IT) verfügen. Es sind weder Berufserfahrung im Bereich der Cybersicherheit noch ein formaler Bildungsabschluss erforderlich. Der nächste Karriereschritt für die Kandidaten wäre der Erwerb von ISC2-Zertifizierungen auf Expertenebene, für welche Erfahrung in diesem Bereich erforderlich ist.

Akkreditierung

CC entspricht den strengen Anforderungen der ANSI National Accreditation Board (ANAB) ISO/IEC-Norm 17024.

Arbeitsaufgabenanalyse (Job Task Analysis, JTA)

ISC2 ist gegenüber seinen Mitgliedern verpflichtet, die Relevanz des CC aufrechtzuerhalten. Die regelmäßig durchgeführte Arbeitsaufgabenanalyse (JTA) ist ein methodischer und kritischer Prozess zur Ermittlung der Aufgaben, die von Sicherheitsfachkräften ausgeführt werden, die in dem vom CC definierten Beruf tätig sind. Die Ergebnisse der JTA werden zur Aktualisierung der Prüfung verwendet. Dieses Verfahren gewährleistet, dass die Kandidaten in den Themenbereichen geprüft werden, die für die Aufgaben und Verantwortlichkeiten der heutigen Informationssicherheitsexperten relevant sind.

CC-CAT-Prüfungsinformationen

Die CC-Prüfung verwendet computergestützte adaptive Tests (CAT) für alle Prüfungen in Englisch, Vereinfachtem Chinesisch, Japanisch, Deutsch und Spanisch (modern). Mehr über CC CAT erfahren Sie unter ISC2.org/certifications/computerized-adaptive-testing

Prüfungsdauer	2 Stunden
Anzahl der Fragen	100 - 125
Fragenformat	Multiple-Choice-Fragen und erweiterte Fragenarten
Bestehende Note	700 von 1000 Punkten
Verfügbarkeit der Prüfung	Englisch, Chinesisch, Japanisch, Deutsch, Spanisch
Testzentrum	Pearson VUE Testzentrum

CC CAT-Prüfungsgewichte

Bereiche	Durchschnittliches Gewicht
1. Sicherheitsprinzipien	24 %
2. Sicherheits-Governance	17,3 %
3. Konzepte der Identitäts- und Zugriffsverwaltung (IAM)	20 %
4. Netzwerk- und Cloud-Sicherheitskonzepte	21,3 %
5. Sicherheitsmaßnahmen und Reaktion auf Zwischenfälle	17,3 %
	Gesamt: 100 %

Bereich 1: Sicherheitsprinzipien

1.1 Verstehen von Konzepten der Cybersicherheit

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentifizierung, Autorisierung, Abrechnung (AAA)
- Nichtabstreitbarkeit
- Datenschutz

1.2 Verstehen von Risikomanagementkonzepten

- Lebenszyklus des Risikomanagements
- Prozesse des Risikomanagements

1.3 Verstehen von Governance-Konzepten

- Vorschriften und Gesetze
- Rahmenwerke und Leitlinien
- Richtlinien, Normen (z. B. Internationale Organisation für Normung (ISO), Zentrum für Internetsicherheit), Verfahren

1.4 Verstehen von Cybersicherheitskontrollen

- Technische Kontrollen
- Administrative Kontrollen
- Physische Kontrollen

1.5 Aufrechterhalten eines professionellen und ethischen Verhaltens

- Beruflicher Verhaltenskodex
- Sorgfalt und Sorgfaltspflicht
- ISC2-Ethikkodex

Bereich 2: Sicherheits-Governance

2.1 Planen von Governance, Risiko und Compliance (GRC)

- Zweck
- Bedeutung
- Frameworks und Tools

2.2 Verstehen von Redundanz

- Geschäftskontinuität (Business Continuity, BC)
- Notfallwiederherstellung (Disaster recovery, DR)

2.3 Verstehen von Sicherheitsbewusstsein

- Organisationskultur (z. B. Bedeutung der Sicherheit, Führung im Sicherheitsbereich)
- Konzepte (z. B. Social Engineering, Passwortschutz, Phishing)

2.4 Messung der Wirksamkeit der Cybersicherheit

- Schlüsselmetriken, Wichtige Risikoindikatoren (Key Risk Indicators, KRI)
- Dashboards, Scorekarten, Berichte

Bereich 3: Konzepte der Identitäts- und Zugriffsverwaltung (IAM)

3.1 Verstehen des Lebenszyklusmanagements von Identitäten

- Definition der Rollen
- Provisionierung
- Überprüfung
- Deprovisionierung
- Frameworks und Tools

3.2 Verstehen der logischen Zugriffskontrollen

- Grundsatz des geringsten Privilegs (Principle of Least Privilege, PoLP)
- Aufgabentrennung (Segregation of Duties, SoD)
- Modelle der Zugriffskontrolle

Bereich 4: Netzwerk- und Cloud-Sicherheitskonzepte

4.1 Verstehen von Netzwerksicherheit

- Konzepte (z. B. Open Systems Interconnection (OSI)-Modell, Transmission Control Protocol/Internet Protocol (TCP/IP)-Modell, Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6), virtuelles privates Netzwerk (Virtual Private Network, VPN))
- Firewalls (z. B. Ports, Anwendungen)
- Drahtlos (z. B. Wi-Fi, Bluetooth)
- Eingebettete Systeme (z. B. Industrielle Kontrollsysteme (Industrial Control System, ICS), Internet der Dinge (Internet Of Things, IoT))

4.2 Verständnis von Netzsicherheitsarchitektur

- Verstehen der Netzwerksegmentierung (z. B. Firewall-Zonen, virtuelles lokales Netzwerk (Virtual Local Area Network, VLAN), Mikrosegentierung)
- Verteidigung in der Tiefe
- Zero Trust (ZT)

4.3 Verstehen von Cloud-Sicherheit

- Merkmale (z. B. breiter Netzzugang, schnelle Elastizität, gemessener Service, Selfservice auf Abruf, Ressourcenpooling)
- Dienstleistungsmodelle
- Bereitstellungsmodelle
- Modell für geteilte Sicherheit (z. B. Rollen und Verantwortlichkeiten)

Bereich 5: Sicherheitsmaßnahmen und Reaktion auf Zwischenfälle

5.1 Verstehen von Datensicherheit

- Datenverarbeitung (z. B. Klassifizierung, Kennzeichnung, Maskierung und Bereinigung)
- Verschlüsselung (z. B. symmetrisch, asymmetrisch, Hashing, quantenresistente Kryptographie)

5.2 Verstehen von Sicherheitsmaßnahmen

- Protokollierung und Überwachung von Sicherheitsereignissen
- Triage von Sicherheitsereignissen (z. B. Anwendungsfälle für Zwischenfälle, Priorisierung, Korrelation)
- Bedrohungsakteure (z. B. Arten, Motivationen)
- Informationen über Cyber-Bedrohungen
- Frameworks für Bedrohungen

5.3 Verstehen der Reaktion auf Zwischenfälle (Incident Response, IR)

- Richtlinie für den Umgang mit Daten, die einen Plan zur Reaktion auf Zwischenfälle (Incident Response Plan, IRP) umsetzt
- Übungen zur Reaktion auf Zwischenfälle (Incident Response, IR) (z. B. Tests, Tabletop-Übungen)

5.4 Verstehen von Asset-Schutz

- Verwaltung des Lebenszyklus von Assets (z. B. End of Life (EOL) Software und Geräte)
- Konfigurations- und Änderungsmanagement

5.5 Verstehen von Sicherheitstests

- Sicherheitsbereitschaftstests (z. B. Blue Teaming, Purple Teaming, Red Teaming)
- Anwendungstests (z. B. Scannen auf Sicherheitslücken, statische Analyse, dynamische Analyse, Bedrohungsmodellierung)
- Physische Penetrationstests (z. B. Phishing, Tailgating, Identitätsdiebstahl)

Zusätzliche Informationen zur Prüfung

Ergänzende Referenzen

Bewerber werden dazu ermutigt, ihre Ausbildung und Erfahrung durch die Sichtung relevanter Ressourcen, die sich auf die CC-Prüfungsübersicht beziehen, zu ergänzen und Lernbereiche zu identifizieren die möglicherweise zusätzliche Aufmerksamkeit erfordern.

Siehe die vollständige Liste der ergänzenden Referenzen unter ISC2.org/certifications/References.

Prüfungsrichtlinien und -verfahren

ISC2 empfiehlt den Kandidaten, sich vor der Anmeldung zur Prüfung mit den Prüfungsrichtlinien und -verfahren vertraut zu machen. Lesen Sie die umfassende Aufschlüsselung dieser wichtigen Informationen unter ISC2.org/Register-for-Exam.

Rechtliche Informationen

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

Haben Sie Fragen?

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

Amerika

Telefon: +1-866-331-ISC2 (4722), Taste 1 drücken
E-Mail: membersupport@isc2.org

Asien-Pazifik

Telefon: +852-5803-5662
E-Mail: isc2asia@isc2.org

Europa, Naher Osten und Afrika

Telefon: +44-203-960-7800
E-Mail: info-emea@isc2.org