CC SM

Zertifiziert in Cybersicherheit

ISC2 Certification

Gliederung der Zertifizierungsprüfung

Datum des Inkrafttretens: 1. Oktober 2025

ISC2

Über die Zertifizierung in Cybersicherheit

Mit dem Titel Certified in Cybersecurity (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
- Geschäftskontinuität (Business Continuity, BC), Notfallwiederherstellung (Disaster Recovery, DR) und Konzepte zur Reaktion auf Zwischenfälle
- Zugangskontrollkonzepte
- Netzwerksicherheit
- Sicherheitsmaßnahmen

Erfahrungsanforderungen

Es gibt keine besonderen Voraussetzungen für die Teilnahme an der Prüfung. Es wird empfohlen, dass die Bewerber über Grundkenntnisse der Informationstechnologie (IT) verfügen. Es ist 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 die Erfahrung in diesem Bereich erforderlich ist.

Akkreditierung

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

Job-Aufgabenanalyse (JTA)

ISC2 ist gegenüber seinen Mitgliedern verpflichtet, die Relevanz des CC aufrechtzuerhalten. Die regelmäßig durchgeführte Job-Aufgabenanalyse (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 erfährst du unter www.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	26 %
2. Geschäftskontinuität (Business Continuity, BC), Notfallwiederherstellung (Disaster Recovery, DR) und Konzepte zur Reaktion auf Zwischenfälle	10 %
3. Zugangskontrollkonzepte	22 %
4. Netzwerksicherheit	24 %
5. Sicherheitsmaßnahmen	18 %
	Gesamt: 100 %

Bereich 1: Sicherheitsprinzipien

1.1 Die Sicherheitskonzepte der Informationssicherung verstehen

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentifizierung (z. B. Methoden der Authentifizierung, Multi-Faktor-Authentifizierung (MFA))
- Unleugbarkeit
- Datenschutz

1.2 Verständnis des Risikomanagementprozesses

- Risikomanagement (z. B. Risikoprioritäten, Risikotoleranz)
- Risikoerkennung, -bewertung und -behandlung

1.3 Verstehen der Sicherheitskontrollen

- Technische Kontrollen
- Administrative Kontrollen
- Physische Kontrollen

1.4 Den ISC2-Ethikkodex verstehen

- Beruflicher Verhaltenskodex

1.5 Verstehen von Governance-Prozessen

- Politiken
- Verfahren
- Standards
- Vorschriften und Gesetze

Bereich 2: Geschäftskontinuität (Business Continuity, BC), Notfallwiederherstellung (Disaster Recovery, DR) und Konzepte zur Reaktion auf Zwischenfälle

2.1 Verstehen der Geschäftskontinuität (Business Continuity, BC)

- Zweck
- Bedeutung
- Komponenten

2.2 Verstehen von Notfallwiederherstellung (Disaster recovery, DR)

- Zweck
- Bedeutung
- Komponenten

2.3 Verstehen der Reaktion auf Vorfälle

- Zweck
- Bedeutung
- Komponenten

Bereich 3: Zugangskontrollkonzepte

3.1 Verstehen der physischen Zugangskontrollen

- Physische Sicherheitskontrollen (z. B. Ausweissysteme, Zugangskontrollen, Umgebungsgestaltung)
- Überwachung (z. B. Sicherheitspersonal, Videoüberwachung/Überwachungskamerasysteme, Alarmsysteme, Protokolle)
- Autorisiertes und nicht autorisiertes Personal

3.2 Verstehen der logischen Zugriffskontrollen

- Grundsatz des geringsten Rechtsanspruchs
- Aufgabentrennung
- Benutzerbestimmbare Zugriffskontrolle (Discretionary access control, DAC)
- Zwingend erforderliche Zugriffskontrolle (Mandatory access control, MAC)
- Rollenbasierte Zugriffskontrolle (Role-based access control, RBAC)

Bereich 4: Netzwerksicherheit

4.1 Verstehen von Computernetzwerken

» Netzwerke (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), WiFi)

» Ports

» Anwendungen

4.2 Verstehen von Netzwerkbedrohungen und Angriffen

» Arten von Bedrohungen (z. B. Verteilte Denial-of-Service (Distributed Denial-of-Service, DDoS), Virus, Wurm, Trojaner, Mittelsmann (Man-in-the-Middle, MITM), Side-Channel)

» Identifizierung (z. B. Intrusion Detection System (IDS), Host-basiertes IDS (host-based intrusion detection system, HIDS), Netzwerk-basiertes IDS (Network Intrusion Detection System, NIDS))

» Vorbeugung (z. B. Antivirus, Scans, Firewalls, Angrifferkennungssystem (IPS))

4.3 Verständnis der Netzsicherheitsinfrastruktur

» Vor Ort (z. B. Stromversorgung, Rechenzentrum/Schränke, Heizung, Lüftung und Klimatisierung (Heating, Ventilation, and Air Conditioning, HVAC), Umweltschutz, Brandbekämpfung, Redundanz, Grundsatzvereinbarung (Memorandum of Understanding, MOU)/ Partnerschaftsvertrag (Memorandum of Agreement, MOA))

» Design (z. B. Netzwerksegmentierung (demilitarisierte Zone (Demilitarized Zone, DMZ), virtuelles lokales Netzwerk (Virtual Private Network, VLAN), virtuelles privates Netzwerk (VPN), Mikrosegmentierung), Verteidigung in der Tiefe, Netzwerkzugriffskontrolle (Network Access Control, NAC) (Segmentierung für eingebettete Systeme, Internet der Dinge (Internet of Things, IoT))

» Cloud (z. B. Service Level Agreement (SLA), Managed Service Provider (MSP), Software als Service (Software as a Service, SaaS), Infrastruktur als Service (Infrastructure as a Service, IaaS), Plattform als Service (Platform as a Service, PaaS), Hybrid)

Bereich 5: Sicherheitsmaßnahmen

5.1 Verstehen der Datensicherheit

» Verschlüsselung (z. B. symmetrisch, asymmetrisch, Hashing)
» Umgang mit Daten (z. B. Vernichtung, Aufbewahrung, Klassifizierung, Kennzeichnung)
» Protokollierung und Überwachung von Sicherheitsereignissen

5.2 Verstehen der Systemhärtung

» Konfigurationsmanagement (z. B. Baselines, Updates, Patches)

5.3 Verstehen von Best-Practice-Sicherheitsrichtlinien

» Richtlinie zur Datenverarbeitung
» Passwortrichtlinie
» Richtlinien zur korrekten Nutzung (Acceptable Use Policy, AUP)
» Bring your own device (BYOD)-Richtlinie
» Richtlinien für das Änderungsmanagement (z. B. Dokumentation, Genehmigung, Rollback)
» Datenschutzrichtlinie

5.4 Verstehen von Schulungen zum Sicherheitsbewusstsein

» Zweck/Konzepte (z. B. Social Engineering, Passwortschutz)
» Bedeutung

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 www.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 www.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