CC SM

Certified in Cybersecurity

ISC2 Certification

Zertifizierungs-**Prüfungsübersicht**

Datum des Inkrafttretens: 29. August 2022

ISC2

Über ISC2-Zertifiziert in Cybersicherheit-Zertifizierung

Mit Zertifiziert in Cybersicherheit (CC) weisen Sie gegenüber Arbeitgebern nach, dass Sie über die grundlegenden Kenntnisse, Fähigkeiten und Fertigkeiten verfügen, die für eine Einstiegs- oder Junior-Level-Position im Bereich Cybersicherheit erforderlich sind. Damit zeigen Sie, dass Sie die grundlegenden bewährten Sicherheitspraktiken, -richtlinien und -verfahren verstehen und dass Sie bereit und in der Lage sind, mehr zu lernen und sich beruflich weiterzuentwickeln.

Die Prüfung erstreckt sich auf fünf Bereiche.

- Sicherheitsprinzipien
- Business Continuity (BC), Disaster Recovery (DR) & Incident Response-Konzepte
- Zugangskontrollkonzepte
- Netzwerksicherheit
- Sicherheitsoperationen

Anforderungen an die Erfahrung

Es gibt keine besonderen Voraussetzungen, um die Prüfung abzulegen. Es wird empfohlen, dass die Kandidaten über Grundkenntnisse der Informationstechnologie (IT) verfügen. Es ist keine Berufserfahrung im Bereich Cybersicherheit oder ein formaler Bildungsabschluss erforderlich. Der nächste Schritt in der Karriere des Kandidaten wäre der Erwerb von ISC2-Zertifizierungen auf Expertenebene, die Erfahrung in diesem Bereich voraussetzen.

Job-Task-Analyse (JTA)

ISC2 ist gegenüber seinen Mitgliedern verpflichtet, die Relevanz des CC aufrechtzuerhalten. Die Job-Task-Analyse (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 CC 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 relevant sind.

Informationen zur CC-Prüfung

Dauer der Prüfung	2 Stunden
Anzahl der Fragen	100
Fragenformat	Mehrfachauswahl
Punktzahl zum Bestehen	700 von 1000 Punkten
Prüfungsverfügbarkeit	Englisch, Chinesisch, Japanisch, Deutsch
Testzentrum	Pearson VUE Testzentrum

CC-Prüfungsgewichtungen

Bereiche	Durchschnittliche Gewicht
1. Sicherheitsprinzipien	26 %
2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response-Konzepte	10 %
3. Zugangskontrollkonzepte	22 %
4. Netzwerksicherheit	24 %
5. Sicherheitsoperationen	18 %
Gesamt	**100 %**

Bereich 1: Sicherheitsprinzipien

1.1 Verstehen der Sicherheitskonzepte der Informationssicherung

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

1.2 Verstehen des Prozesses des Risikomanagements

- Risikomanagement (z. B. Risikoprioritäten, Risikotoleranz)
- Identifizierung, Bewertung und Behandlung von Risiken

1.3 Verstehen von Sicherheitskontrollen

- Technische Kontrollen
- Administrative Kontrollen
- Physische Kontrollen

1.4 Verstehen des (ISC)²-Ethikkodex

- Beruflicher Verhaltenskodex

1.5 Verstehen von Governance-Prozessen

- Richtlinien
- Verfahren
- Normen
- Regularien und Gesetze

Bereich 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response-Konzepte

2.1 Verstehen von Geschäftskontinuität (BC)

- Zweck
- Stellenwert
- Komponenten

2.2 Verstehen von Wiederherstellung im Katastrophenfall (DR)

- Zweck
- Stellenwert
- Komponenten

2.3 Antwort auf Zwischenfälle

- Zweck
- Stellenwert
- Komponenten

Bereich 3: Zugangskontrollkonzepte

3.1 Verstehen von physischen Zugriffskontrollen

- Physische Sicherheitskontrollen (z. B. Ausweissysteme, Zugangstore, Umgebungsgestaltung)
- Überwachung (z. b. Sicherheitspersonal, Videoüberwachung (CCTV), Alarmsysteme, Protokolle)
- Autorisiertes versus nicht autorisiertes Personal

3.2 Verstehen von logischen Zugriffskontrollen

- Prinzip des geringsten Privilegs
- 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 Computer-Netzwerken

» 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. Distributed Denial-of-Service (DDoS), Virus, Wurm, Trojaner, Mittelsmann-Angriff (Man-in-the-Middle,MITM), Side-Channel)

» Identifizierung (z. B. Intrusion Detection System (IDS), Host-basiertes Intrusion Detection System (HIDS), Network Intrusion Detection System (NIDS))

» Prävention (z. B. Antivirus, Scans, Firewalls, Intrusion Prevention System (IPS))

4.3 Verstehen der Infrastruktur für Netzwerksicherheit

» Vor-Ort (z. B. Stromversorgung, Rechenzentrum/Schränke, Heizung, Lüftung und Klimaanlage (HLK), Umwelt, Brandbekämpfung, Redundanz, Grundsatzvereinbarung/Partnerschaftsvertrag)

» Entwurf (z. B. Netzwerksegmentierung (demilitarisierte Zone (DMZ), virtuelles lokales Netzwerk (VLAN), virtuelles privates Netzwerk (VPN), Mikrosegmentierung), Verteidigung in der Tiefe, Netzwerkzugangskontrolle (NAC) (Segmentierung für eingebettete Systeme, Internet der Dinge (IoT))

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

Bereich 5: Sicherheitsoperationen

5.1 Verstehen von Datensicherheit

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

5.2 Verstehen von Systemhärtung

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

5.3 Verstehen von Best Practice Sicherheitsrichtlinien

» Richtlinie zum Umgang mit Daten
» Richtlinie für Passwörter
» Richtlinie zur akzeptablen Nutzung (AUP)
» Bring dein eigenes Gerät (BYOD)
» Richtlinien für das Änderungsmanagement (z. B. Dokumentation, Genehmigung, Rollback)
» Datenschutzbestimmungen

5.4 Verstehen von Schulungen zum Sicherheitsbewusstsein

» Zweck/Konzepte (z. B. Sozialtechnik, Passwortschutz)
» Stellenwert

Zusätzliche Informationen zur Prüfung

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

Für Fragen im Zusammenhang mit der ISC2-Rechtspolitik wenden Sie sich bitte an die ISC2-Rechtsabteilung unter legal@isc2.org.

Haben Sie noch Fragen?

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

Nord- und Südamerika

Telefon: +1-866-331-ISC2 (4722)
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