Certified in Cybersecurity

An (ISC)² Certification

Gliederung der **Zertifizierungsprüfung**

Gültig ab: 29. August 2022

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

Über die Zertifizierung “Certified in Cybersecurity”

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. Er zeigt, dass Sie die grundlegenden bewährten Sicherheitspraktiken, -richtlinien und -verfahren verstehen und in der Lage sind, mehr zu lernen und sich beruflich weiterzuentwickeln.

Die Prüfung erstreckt sich auf fünf Bereiche.

- Sicherheitsgrundsätze
- Konzepte der Strategie für Geschäftskontinuität (BC) / Notfallwiederherstellung (DR)
- Konzepte der Zugangskontrolle
- Netzwerksicherheit
- Sicherheitsabläufe

Anforderungen bezüglich der Erfahrung

Für die Teilnahme an der Prüfung sind keine besonderen Voraussetzungen erforderlich. Es wird empfohlen, dass Kandidaten über Grundkenntnisse der Informationstechnologie (IT) verfügen. Es ist keine Berufserfahrung im Bereich der Cybersicherheit oder ein formaler Bildungsabschluss erforderlich. Der nächste Schritt in der Laufbahn des Kandidaten wäre der Erwerb einer (ISC)²-Expertenzertifizierung, für die Erfahrung in diesem Bereich erforderlich ist.

Analyse der Arbeitsaufgaben (JTA)

(ISC)² ist gegenüber seinen Mitgliedern verpflichtet, die Relevanz von CC aufrechtzuerhalten. Die in regelmäßigen Abständen durchgeführte Job Task Analysis (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 heutiger Informationssicherheitsexperten relevant sind.

Informationen zur CC-Prüfung

Dauer der Prüfung	2 Stunden
Anzahl der Aufgaben	100
Aufgabenformat	Multiple-Choice
Punkte zum Bestehen	700 von 1000 Punkten
Prüfungsverfügbarkeit	Englisch, Chinesisch, Deutsch, Koreanisch, Japanisch, Spanisch
Prüfungszentrum	Pearson-VUE-Prüfungszentrum

Gewichtungen bei CC-Prüfungen

Bereich	Durchschnittliche Gewichtung
1. Sicherheitsgrundsätze	26%
2. Geschäftskontinuität (Business Continuity, BC), Notfallwiederherstellung (Disaster Recovery, DR) und Konzepte für die Reaktion auf Vorfälle (Incident Response)	10%
3. Konzepte der Zugangskontrolle	22%
4. Netzwerksicherheit	24%
5. Sicherheitsabläufe	18%
Insgesamt:	**100%**

Bereich 1:
Sicherheitsgrundsätze

1.1 Verständnis der Sicherheitskonzepte der Informationssicherung

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

1.2 Verständnis des Risikomanagementprozesses

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

1.3 Verständnis von Sicherheitskontrollen

» Technische Kontrollen
» Administrative Kontrollen
» Physische Kontrollen

1.4 Verständnis des (ISC)²-Ethikkodex

» Professioneller Verhaltenskodex

1.5 Verständnis von Governance-Prozessen

» Richtlinien
» Verfahren
» Standards
» Regulierungen und Gesetze

Bereich 2:

Geschäftskontinuität (Business Continuity, BC), Notfallwiederherstellung (Disaster Recovery, DR) und Konzepte für die Reaktion auf Vorfälle (Incident Response)

2.1 Verständnis von Geschäftskontinuität (Business Continuity, BC)

» Zweck
» Bedeutsamkeit
» Bestandteile

2.2 Verständnis der Notfallwiederherstellung (Disaster Recovery, DR)

» Zweck
» Bedeutsamkeit
» Bestandteile

2.3 Verständnis von Reaktionen auf Vorfälle

» Zweck
» Bedeutsamkeit
» Bestandteile

Bereich 3:

Konzepte der Zugangskontrolle

3.1 Verständnis von physischen Zugangskontrollen

» Physische Sicherheitskontrollen (z. B. Ausweissysteme, Zugangstore, Umgebungsgestaltung)
» Überwachung (z. B. Sicherheitspersonal, Videoüberwachung, Alarmsysteme, Protokolle)
» Autorisiertes und nicht autorisiertes Personal

3.2 Verständnis von logischen Zugangskontrollen

» Prinzip des geringsten Privilegien
» Aufgabentrennung
» Diskretionäre Zugriffskontrolle (Discretionary Access Control, DAC)
» Obligatorische Zugriffskontrolle (Mandatory Access Control, MAC)
» Rollenbasierte Zugriffskontrolle (Role-based Access Control, RBAC)

Bereich 4: Netzwerksicherheit

4.1 Verständnis 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), WLAN)

» Ports

» Anwendungen

4.2 Verständnis von Netzwerkbedrohungen und Angriffen

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

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

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

4.3 Verständnis von Netzsicherheitsinfrastrukturen

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

» Konzeption (z. B. Netzwerksegmentierung (demilitarisierte Zone (Demilitarized Zone, DMZ), virtuelles lokales Netzwerk (VLAN), virtuelles privates Netzwerk (VPN), Mikrosegmentierung), Defense in Depth, Netzwerkzugriffskontrolle (NAC) (Segmentierung für eingebettete Systeme, Internet der Dinge (IoT))

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

Bereich 5:
Sicherheitsabläufe

5.1 Verständnis von Datensicherheit

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

5.2 Verständnis von Systemhärtung

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

5.3 Verständnis von bewährten Sicherheitsrichtlinien (Best Practices)

» Richtlinien zum Umgang mit Daten
» Passwort-Richtlinien
» Richtlinien zur akzeptablen Nutzung (Acceptable Use Policy, AUP)
» BYOD-Richtlinie (Bring your own device)
» Richtlinien für das Change Management (z. B. Dokumentation, Genehmigung, Rollback)
» Datenschutzrichtlinien

5.4 Verständnis von Schulungen zum Sicherheitsbewusstsein

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

Zusätzliche Informationen zur Prüfung

Prüfungsrichtlinien und -verfahren

(ISC)² empfiehlt, dass CC-Kandidaten die Prüfungsrichtlinien und -verfahren vor der Registrierung überprüfen. Lesen Sie die umfassende Aufschlüsselung dieser wichtigen Informationen unter www.isc2.org/Register-for-Exam.

Rechtliche Informationen

Wenn Sie Fragen zu den Rechtsgrundsätzen von (ISC)² haben, wenden Sie sich bitte an die Rechtsabteilung von (ISC)² via legal@isc2.org.

Noch Fragen?

Wenden Sie sich an den (ISC)²-Kandidatenservice in Ihrer Region:

Nord- und Südamerika

Telefon: +1-866-331-ISC2 (4722)
E-Mail: info@isc2.org

Asien-Pazifik

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

Europa, Mittlerer Osten und Afrika

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