Hewlett Packard Enterprise

Education Services
ISACA: Certified Information Security Manager (CISM)

Kursnummer: H1RZ4S, Dauer: 4 Tage

In unserer 4-tägigen CISM-Schulung erwerben IT-Sicherheitsexperten mit Management-Verantwortung im Bereich der Informationssicherheit das nötige Wissen, um die Prüfung zum Certified Information Security Manager (CISM) abzulegen.
CISM ist eine IT-Sicherheits-Zertifizierung. Es soll erfahrenen Führungs- und Fachkräften die Möglichkeit gegeben werden, ihre Qualifikation hinsichtlich der Planung, der Umsetzung sowie der Steuerung und der Überwachung von IT-Sicherheitskonzepten nachzuweisen.

Das Examen richtet sich an IT-Sicherheitsexperten, die eine fundierte Berufserfahrung durch umfassende Tätigkeiten auf dem Gebiet der betrieblichen Informationssicherheit erworben haben.

Teilnehmer

Die CISM-Zertifizierung ist für Personen konzipiert, welche die Informationssicherheit (IS) eines Unternehmens konzipieren, überwachen und/oder beurteilen. Die CISM-Zertifizierung vermittelt international anerkannte Methoden und Praktiken und bietet so der Geschäftsleitung die Sicherheit, dass Mitarbeiter mit dieser Qualifikation die erforderliche Erfahrung und das Wissen haben, um effektives Sicherheitsmanagement bereitzustellen. Die CISM-Berufspraktik definiert außerdem eine globale Berufsbeschreibung für den Informationssicherheitsmanager und eine Methode zur Beurteilung des vorhandenen Personals oder zum Vergleich bei zukünftigen Neueinstellungen.

Voraussetzungen

Die CISM-Zertifizierung ist für Informationssicherheitsprofis, -manager und sonstige Sicherheitsanbieter gedacht, die über 3-5 Jahre Praxisnähe oder Managementerfahrungen im Sicherheitsbereich verfügen. Sie müssen ein Minimum von fünf Jahren Berufserfahrung mit Informationssicherheit oder mindestens drei Jahre Tätigkeit im Bereich Informations-sicherheitsmanagement in drei oder mehr der Arbeitspraxis-Analysebereiche nachweisen können.

Die folgenden sicherheitsbezogenen Zertifizierungen und Erfahrungen im Informationssystem-management werden als ausreichend im Bereich Informationssicherheit angesehen:

Zwei Jahre Berufserfahrung:

- Zertifizierter Informationssystem-Auditor (CISA)
- Zertifizierter Informationssystemsicherheits-Experte (CISSP)
- Akademischer Grad in Informationssicherheit oder einem verwandten Bereich (z.B. Unternehmensverwaltung, Informationssysteme, Informationssicherung).

Ein Jahr Berufserfahrung:

- Erfahrung im Informationssystemmanagement
- Auf Fähigkeiten beruhende Zertifizierungen (z. B. SANS Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security +).

ISACA: Certified Information Security Manager (CISM) – Kursinhalte

Modul 1: Informationssicherheit-Governance

- Informationssicherheitskonzepte
- Die Beziehung zwischen Informationssicherheit und Geschäftsbetriebstechniken, die benutzt werden, um das Engagement der Geschäftsleitung und die Unterstützung des Informationssicherheitsmanagements zu gewährleisten
- Methoden zur Integration der Informationssicherheits-Governance in das Gesamtrahmenwerk der Unternehmens-Governance
- Praktiken in Verbindung mit einer Gesamtansatzdirektive, die auf die Geschäftsführung ausgerichtet ist
- Niveauausrichtung und Erwartung in Bezug auf Informationssicherheit durch Grundsteinlegung für das Informationssicherheitsmanagement innerhalb einer Organisation
- Eine Informationssicherheits-Lenkungsgruppenfunktion
- Aufgaben, Verantwortungen und Organisationsstruktur des Informationssicherheitsmanagements
- Governance-Bereiche (z. B. Risikomanagement, Datenklassifizierungsmanagement, Netzwerksicherheit, Systemzugriff)
- Zentralisierte und dezentralisierte Ansätze für die Koordination der Informationssicherheit
- Gesetzliche und behördliche Angelegenheiten in Verbindung mit Internetgeschäften, globalen Übertragungen und grenzüberschreitenden Datenströmen (z. B. Geheimhaltung, Steuerrecht und -tarife, Datenimport/-exportbeschränkungen, Verschlüsselungsbeschränkungen, Gewährleistungen, Patente, Urheberrechte, Berufsgeheimnisse, nationale Sicherheit)
- Gemeinsame Versicherungspolicen und auferlegte Bedingungen (z. B. Kriminalitäts- oder Veruntreuungsversicherung, Geschäftsunterbrechungen)
- Die Anforderungen für Inhalt und Retention von Geschäftsunterlagen und Compliance
- Der Prozess, Ansätze mit den Geschäftszielen des Unternehmens zu verbinden
- Funktion und Inhalt wesentlicher Elemente eines Informationssicherheitsprogramms (z. B. Ansatzdarlegungen, Verfahren und Richtlinien)
- Techniken zur Entwicklung eines Informationssicherheitsprozess-Verbesserungsmodells für nachhaltige und wiederholbare Informationssicherheitsansätze und -verfahren
- Verbesserung des Informationssicherheitsprozesses und seiner Beziehung zum traditionellen Prozessmanagement
- Verbesserung des Informationssicherheitsprozesses und seiner Beziehung zur Sicherheitsarchitekturentwicklung und -modellierung
- Verbesserung des Informationssicherheitsprozesses und seiner Beziehung zur Sicherheits-Infrastruktur
- Allgemein akzeptierte internationale Standards für das Informationssicherheitsmanagement und verwandte Prozessverbesserungsmodelle
- Die Schlüsselkomponenten von Kosten-Nutzen-Analyse und Unternehmenstransformations-/migrationsplänen (z. B. architektonische Ausrichtung, organisatorische Positionierung, Änderungsmanagement, Benchmarking, Markt/Wettbewerbsanalyse)
- Methodologie für Geschäftsfallentwicklung und Berechnung des Unternehmenswertvorschlags

Modul 2: Risikomanagement

- Informationsressourcen, die zur Unterstützung der Geschäftsabläufe benutzt werden
- Bewertungsmethodologien für Informationsressourcen
- Informationsklassifizierung
- Prinzipien zur Entwicklung von Basislinien und ihre Beziehung zu risikobasierten Beurteilungen von Kontrollanforderungen
- Prinzipien und Praktiken des lebenszyklusbasierten Risikomanagements
- Gefahren, Schwachstellen und Risikoanfälligkeit in Verbindung mit Vertraulichkeit, Integrität und Verfügbarkeit von Informationsressourcen
- Quantitative und qualitative Methoden zur Bestimmung von Sensitivität und Wichtigkeit von Informationsressourcen und die Auswirkung ungünstiger Ereignisse
- Benutzung der Marktlückenanalyse zur Beurteilung allgemein akzeptierter Standards für Good Practice beim Informationssicherheitsmanagement im Vergleich zum gegenwärtigen Zustand
- Amortisationsdauerziele (RTO) für Informationsressourcen und die Bestimmung von RTO und in welchem Verhältnis diese zur betrieblichen Kontinuität und den Zielen und Prozessen der Notfallplanung stehen
- Risikomilderungsstrategien, die bei der Definierung der Sicherheitsanforderungen für Informationsressourcen zur Unterstützung von Unternehmensanwendungen benutzt werden
- Kosten-Nutzen-Analysetechniken zur Beurteilung von Optionen zur Abschwächung von Risiken, Bedrohungen und Risikoanfälligkeit auf ein annehmbares Niveau
- Management und Reporting des Status identifizierter Risiken

Hewlett Packard Enterprise

ISACA: Certified Information Security Manager (CISM) – Kursinhalte

Modul 3: Informationssicherheitsprogramm-management

- Methoden zur Entwicklung eines Implementierungsplans, der den in der Risikoanalyse identifizierten Sicherheitsanforderungen entspricht
- Methoden und Techniken für das Projektmanagement
- Die Komponenten eines Informationssicherheits-Governance-Rahmenwerks zur Integration von Sicherheitsprinzipien, -praktiken, -management und -bewusstsein in alle Aspekte und Ebenen des Unternehmens
- Sicherheits-Basislinien und Konfigurationsmanagement bei Design und Management von Geschäftsanwendungen und der Infrastruktur
- Informationssicherheitsarchitekturen: (z.B. Einzelanmeldung, regelbasierte im Gegensatz zu listenbasierter Systemzugriffskontrolle für Systeme, beschränkte System-verwaltungspunkte)
- Informationssicherheitstechnologien (z.B. Verschlüsselungstechniken und Digitalunterschriften, um der Geschäftsleitung die Wahl entsprechender Kontrollvorrichtungen zu ermöglichen)
- Sicherheitsverfahren und Richtlinien für Geschäftsabläufe und Infrastrukturaktivitäten Systementwicklungs-Lebens-zyklusmethodologien (z.B. traditionelles SDLC, Prototypisierung)
- Planung, Durchführung, Reporting und Weiterverfolgung von Sicherheitstests
- Zertifizierung und Akkreditierung der Übereinstimmung der Geschäftsanwendungen und Infrastruktur mit dem Informationssicherheits-Governance-Rahmenwerk des Unternehmens
- Arten, Vorteile und Kosten physischer, verwaltungstechnischer und technischer Kontrollen
- Planung, Design, Entwicklung, Überprüfung und Implementierung der Informationssicherheitsanforderungen in die Geschäftsabläufe eines Unternehmens
- Design, Entwicklung und Implementierung von Sicherheits-metriksystemen
- Methoden und Techniken für das Akquisitionsmanagement (z. B. Beurteilung von Lieferanten-Leistungsumfangsvereinbarungen, Vorbereitung von Verträgen)

Modul 4: Informationssicherheitsmanagement

- Umsetzung von Informationssicherheitsansätzen in betriebliche Anwendung
- Informationssicherheits-Verwaltungsprozesse und -verfahren
- Methoden zur Verwaltung der Implementierung des Informationssicherheitsprogramms des Unternehmens durch Drittparteien, einschließlich Handelspartnern und Anbietern von Sicherheitsdienstleistungen
- Fortwährende Überwachung der Sicherheitsaktivitäten in der Infrastruktur und den Geschäftsanwendungen des Unternehmens
- Methoden zur Verwaltung von Erfolg/Misserfolg von Informationssicherheitsinvestitionen durch Datenerfassung und periodische Überprüfung von Schlüssel-Leistungsindikatoren
- Aktivitäten des Änderungs- und Konfigurationsmanagements
- Gebotene Sorgfaltsaktivitäten des Informations-sicherheitsmanagements und Überprüfungen der Infrastruktur
- Verbindungsaktivitäten mit internen/externen Versicherungsanbietern, die Informationssicherheitsprüfungen durchführen
- Gebotene Sorgfaltsaktivitäten, Revisionen und damit verbundene Standards für Verwaltung und Kontrolle des Zugriffs auf Informationsressourcen
- Externe Schwachstellen-Reportingquellen, die Informationen liefern, welche Änderungen an der Informationssicherheit von Anwendungen und Infrastruktur erforderlich machen können
- Ereignisse, welche die Sicherheits-Basislinien beeinträchtigen und Risikobeurteilungen sowie Änderungen an den Informationssicherheitsanforderungen in Sicherheitsplänen, Testplänen und Reperfomance erforderlich machen Informationssicherheit-Problemmanagementpraktiken
- Informationssicherheits-Manager übernimmt Aufgaben als Änderungsagent, Ausbilder und Berater
- Die Art und Weise, in der Kultur und kulturelle Unterschiede das Verhalten des Personals beeinflussen
- Die Aktivitäten, die Kultur und Verhalten des Personals verändern können
- Methoden und Techniken zur Schulung und Ausbildung eines Sicherheitsbewusstseins

ISACA: Certified Information Security Manager (CISM) – Kursinhalte

Modul 5: Reaktionsmanagement

- Komponenten einer Zwischenfall-Reaktionsfähigkeit
- Informationssicherheits-Notfallmanagementpraktiken (z.B. Produktionsänderungs-Kontrollaktivitäten, Entwicklung eines Computernotfall-Reaktionsteams)
- Notfallplanung und betriebliche Wiederherstellungsprozesse
- Notfall-Wiederherstellungstests für Infrastruktur und wichtige Geschäftsanwendungen
- Eskalationsprozesse für effektives Sicherheitsmanagement
- Ansätze und Prozesse zum Erkennen von Eindringlingen
- Helpdeskprozesse zur Identifizierung von Zwischenfällen, die von Benutzern gemeldet werden, und Unterscheidung von anderen Angelegenheiten, die vom Helpdesk erledigt werden
- Der Benachrichtigungsprozess bei der Handhabung von Sicherheitszwischenfällen und Wiederherstellung: (z. B. automatische Benachrichtigungs- und Wiederherstellungs-mechanismen, bspw. als Reaktion auf Virenalarm in Echtzeit)
- Die Anforderungen zur Erfassung und Präsentation von Nachweisen; Regeln für Nachweise, Zulässigkeit von Nachweisen, Qualität und Vollständigkeit von Nachweisen
- Revisionen und Weiterverfolgungsverfahren nach dem Zwischenfall

So erreichen Sie uns

Telefon 07031 269 303
E-Mail education.ccc.de@hpe.com

hpe.com/de/education

Prüfungsinhalte

ISACA-Prüfungen werden nur dreimal im Jahr angeboten. Erlangen Sie jetzt Ihre Zertifizierung, um keine weiteren 3 - 6 Monate auf einen Prüfungstermin warten zu müssen. Bitte beachten Sie, daß sich jeder Teilnehmer selbst für die Zertifizierung anmelden muß.

Inhaltsbereich 1: Informationssicherheits-Governance – 24%

Erstellen und Aufrechterhalten eines Rahmenwerks, das gewährleistet, dass die Informationssicherheitsstrategien auf die Geschäftsziele ausgerichtet sind und den geltenden Gesetzen und Bestimmungen entsprechen.

Inhaltsbereich 2: Risikomanagement und Compliance – 33%

Identifizierung und Beseitigung von Gefahren für die Informationssicherheit zum Erreichen der Geschäftsziele.

Inhaltsbereich 3: Informationssicherheitsprogramm-management – 25%

Konzept, Entwicklung und Verwaltung eines Informationssicherheitsprogramms zur Implementierung des Informationssicherheits-Governance-Rahmenwerks.

Inhaltsbereich 4: Informationssicherheitsmanagement – 18%

Überwachen und Anweisen der Informationssicherheitsaktivitäten zur Umsetzung des Informationssicherheitsprogramms.

Hewlett Packard Enterprise

Januar 2016, Rev. 1