Online kursus
365 dage **DKK 8.499**
Nr. 72845 P ekskl. moms

Certified Information Security Manager (CISM 2022)

Dette kursus lærer dig om rollen som Certified Information Security Manager og de tilhørende principper. Kurset er på engelsk og foregår online, når det passer dig. Du har adgang til online kursuspakken i 365 dage.

Nemt og fleksibelt **Spar penge** **Spar tid** **Høj kvalitet**

Forstå rammerne for strategier til informationssikkerhed

Information Security Governance er en stor del af rollen som Information Security Manager. Med denne kursussamling undersøges vigtigheden af information Security governance i virksomheder og behovet for ledelsesstøtte til den politik og de procedurer, der indføres. Målet med information security governance er at etablere og vedligeholde et framework, der skal sikre at strategierne for informationssikkerhed er på linje med virksomhedens målsætninger og i overensstemmelse med gældende love og regler.

Deltagerprofil

Kurset henvender sig til IT-fagfolk med fokus på sikkerhed, der gerne vil øge deres kendskab til styring, design og tilsyn med en virksomheds informationssikkerhed.

Udbytte

- Lær at identificere opgaver inden for informationssikkerhedsstyring jobområdet
- Identificer opgaverne inden for informations risikostyring
- Få den rette viden til at anerkende resultaterne af informationssikkerhedsstyring
- Forstå forskellen mellem corporate governance og information security governance
- Forstå hvordan analyse, afbødning og monitorering spiller en vigtig rolle inden for risikostyring og compliance
- Bliv klar over forskellene mellem policies, standards, procedures og guidelines
- Beskriv opgaverne i Information Security Program Development and Management jobområdet

Det får du på arrangementet

- Undervisning på engelsk

Indhold

Information Security Governance

- Discover the key concepts covered in this course
- Recognize how the business model for information security encompasses information security planning, implementation, and management
- Identify and classify assets for proper data governance based on value to the business
- Recognize how to apply security criteria when evaluating third-party vendors
- Identify personnel security issues related to hiring, background checks, and exit interviews
- Recognize components constituting an effective program including balanced scorecards
- Review cloud service-level agreements (SLAs) to ensure alignment with security policies
- Outline enterprise change management procedures to ensure risks have been evaluated
- Identify enterprise configuration management procedures and terms such as CMS, CMDB, an CI
- Outline various types of security policies, including acceptable use, and their constituents as well as management buy-in
- Recognize how an IT maturity model provides an assessment as to whether technology is effectively securely meeting business needs through a gap analysis
- Distinguish between capital and operating expenses when budgeting
- Recognize the importance of securing evidence including during and after collection
- Recognize how to ensure effective security governance through security awareness and business executive involvement
- Identify how the Control Objectives for Information Technologies (COBIT) framework applies to IT governance
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 40 Minutes

Business Cotinuity &amp; Security

- Discover the key concepts covered in this course
- Identify common characteristics of a business continuity plan (BCP), business impact analysis (BIA) and related insurance options
- Identify common characteristics of a disaster recovery plan (DRP) including recovery time objective (RTO) and recovery point objective (RPO)

- Recognize data roles such as owner and custodian to enable accountability
- List common IT security roles such as privacy officers, security policy staff, chief information officer (CIO), chief information security office (CISO), and security engineers
- Outline how to determine contract details such as right-to-audit clause and communicate security policies to other parties
- Recognize which factors influence the crafting of various security baselines
- Use a data collector set to establish a Windows performance baseline
- Configure alert rules and action group notifications for performance metrics
- Outline methods of securing assets using physical controls
- Identify types of security controls including detective, preventative, compensating, technical, corrective, and administrative
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 13 Minutes

Incident Response

- Discover the key concepts covered in this course
- Describe common characteristics of an incident response plan, including a communication plan
- Determine when and how specific incidents, such as with cloud providers, are escalated
- Recall how security incidents can be eradicated through threat removal and restoration of services
- Recall how security incidents can be contained to limit further damage
- Benefit from lessons learned during incident response
- Configure triggers to automate incident response
- Summarize the key concepts covered in this course
- Course duration: 42 Minutes

Security Standards

- Discover the key concepts covered in this course
- Outline how General Data Protection Regulation (GDPR) assures data privacy
- Recognize how International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards can result in proper IT governance
- Outline how Health Insurance Portability and Accountability Act (HIPAA) protects sensitive medical information
- Recognize how Federal Risk and Authorization Management Program (FedRAMP) standards are used to secure U.S. government information
- Recognize how Payment Card Industry Data Security Standard (PCI DSS) standards protect cardholder information
- Outline how to implement controls in accordance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) data privacy legislation
- Outline how to implement controls in accordance with China's Personal Information Protection Law (PIPL) data privacy legislation
- Recognize the role that the Cloud Controls Matrix (CCM) plays in establishing cloud security controls
- Summarize the key concepts covered in this course
- Course duration: 53 Minutes

Managing Risk

- Discover the key concepts covered in this course
- Outline how risk management can improve business operations including minimizing residual risk
- Determine the annual loss expectancy (ALE) value using an online ALE calculator
- Identify the most relevant risks and record them in a risk register
- Determine when residual risk is acceptable
- Recognize how risk avoidance fits into the corporate risk appetite
- Identify when risk should be outsourced to other parties
- Recognize that risk cannot always entirely be eliminated
- Summarize the key concepts covered in this course
- Course duration: 50 Minutes

Data Privacy

- Discover the key concepts covered in this course
- Provide examples of personally identifiable information (PII) and how it can affect privacy impact statements
- Identify factors that influence where data physically resides
- Determine when DLP solutions should be used for data privacy
- Discover and classify sensitive data in Amazon Web Services
- Enable data classification in the Azure cloud
- Configure data classification using Windows Server File Server Resource Manager
- Apply cloud resource tags for classifying cloud services
- Configure a Microsoft Azure storage account with a customer-managed key
- Summarize the key concepts covered in this course
- Course duration: 57 Minutes

Assesing Risk

- Discover the key concepts covered in this course
- Recognize how vulnerability assessments can be used to assess risk
- Use the free Nessus tool to execute a vulnerability scan
- Use OWASP ZAP to scan a web site for vulnerabilities
- Recognize how gap analysis results serve as input for information security strategies
- Recognize how penetration testing provides value to the security program
- Use Azure Policy to view cloud resource compliance
- Summarize the key concepts covered in this course
- Course duration: 46 Minutes

Managing Authentication

- Discover the key concepts covered in this course
- Discuss the role authentication plays to allow resource access
- Create AWS Identity and Access Management (IAM) users and groups
- Create Azure Active Directory (AD) users and groups
- Create Linux users and groups
- Create Windows users and groups
- Enable multi-factor authentication (MFA) for AWS IAM user accounts
- Configure Windows password policies
- Recognize the role of identity federation across organizations
- Summarize the key concepts covered in this course
- Course duration: 54 Minutes

Implementing Access Control

- Discover the key concepts covered in this course
- Identify the role authorization plays in allowing resource access
- Recognize access control models used to ensure least privilege, such as ABAC, RBAC, DAC, and MAC
- Use resource and Active Directory attributes to conditionally grant file system permissions
- Determine group memberships and permissions through user attributes
- Assign roles to the Microsoft Azure hierarchy
- Implement DAC with Windows file system permissions
- Implement DAC with Linux file system permissions
- Configure auditing for Windows file system events
- Use the control wizard delegation to enable others to manage AD objects
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 2 Minutes

Network Security

- Discover the key concepts covered in this course
- List the main characteristics of each OSI layer
- Outline how network switching works, including the use of VLANs

- Create a VMware Workstation disconnected virtual network switch
- State the security aspects of DHCP and DNS usage
- Harden DHCP and DNS services
- List various ways to authenticate to a Wi-Fi network
- Recognize where honeypots and honeynets can be used to monitor malicious traffic
- Implement and configure a honeypot
- Open and analyze a packet capture using Wireshark
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 11 Minutes

Network Attack Mitigation

- Discover the key concepts covered in this course
- Recognize the different types of firewalls, their placement, and when they should be used
- Configure Windows Defender Firewall settings
- Configure Linux network firewall settings
- Configure firewall rules in an Azure NSG
- Configure various types of firewall settings in Azure Firewall
- Identify the role played by forward and reverse proxy servers
- Outline how IDS and IPS solutions address security issues
- Install and configure the Snort IDS tool
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 2 Minutes

IT Service &amp; Data Availability

- Discover the key concepts covered in this course
- Define how high availability applies to a multitude of IT and business processes
- Describe how load balancing can improve service performance and increase availability
- Enable application load balancing in the cloud
- Outline backup types and describe how data backups and the Recovery Point Objective (RPO) apply to various services
- Configure a backup schedule using Windows Backup
- Use Azure Backup to achieve data availability goals
- Identify common redundant array of inexpensive disks (RAID) level characteristics
- Configure RAID on Windows
- Configure RAID on Linux
- Enable cloud storage account replication to a secondary region
- Replicate a cloud-based virtual machine to an alternate region
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 17 Minutes

Common Network Security Threats

- Discover the key concepts covered in this course
- Recognize different sources and motivations for IT threats
- View common vulnerabilities and exposures (CVEs) and incorporate them into a security program
- Use the MITRE ATT&amp;CK knowledge base
- Recognize the importance of the OWASP Top 10 when hardening web applications
- Recognize how bug bounties offer rewards for the identification of flaws in hardware and software
- Identify common Wi-Fi attacks
- Outline the mechanics of a SYN flood attack
- Outline how buffer overflow attacks work and how to mitigate them
- Outline how APTs are executed
- Recognize how to mitigate DDoS attacks
- Use VPNs for anonymity and install and use the Tor browser
- Summarize the key concepts covered in this course

- Course duration: 1 Hour, 15 Minutes

Common Network Security Attacks

- Discover the key concepts covered in this course
- Scan a network using Nmap to determine which devices are present
- Use the Browser Exploitation Framework (BeEF) tool to hack a web browser
- Run a SQL injection attack
- Recall how reverse shells works and how to mitigate this risk
- Use hping3 to forge network traffic
- Run a distributed denial-of-service (DDoS) attack against a website
- Use the Hydra tool to brute force a Windows remote desktop protocol (RDP) connection
- Summarize the key concepts covered in this course
- Course duration: 50 Minutes

Cloud Computing &amp; Coding

- Discover the key concepts covered in this course
- Recognize cloud deployment models such as public and private clouds
- Recognize cloud service models such as infrastructure as a service (IaaS) and platform as a service (PaaS)
- Outline various cloud-based security solutions
- Create a repeatable compliant sandbox testing environment in the cloud
- Recognize how security applies to all Software Development Life Cycle (SDLC) phases
- Identify common secure coding practices
- Outline ways in which security should integrate with development and operations, such as testing, deployment, and patching
- Summarize the key concepts covered in this course
- Course duration: 50 Minutes

Data Protection with Cryptography

- Discover the key concepts covered in this course
- Outline how the CIA triad enhances IT security
- Outline how cryptography protects data
- Recognize network and file integrity solutions such as digital signatures, hashes, and checksums
- Outline how hardware security modules (HSMs) are used for encryption offloading and the storage of cryptographic secrets
- Recognize how a trusted platform module (TPM) provides a local device cryptographic store
- Recognize how transport layer security (TLS) supersedes secure sockets layer (SSL) for network security
- Recognize how virtual private networks (VPNs) provide encrypted tunnels to remote networks
- Outline how the IPsec network security protocol suite protects network traffic
- Recognize how public key infrastructure (PKI) certificates are issued and used
- Identify the stages of the PKI certificate lifecycle
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 6 Minutes

Applied Cryptography

- Discover the key concepts covered in this course
- Generate Linux file system hashes
- Generate Windows file system hashes
- Configure an HTTPS binding for a web application
- Create a Windows-based private CA
- Manage Windows public key infrastructure certificate templates
- Acquire a PKI certificate
- Configure a web app to require client PKI certificates
- Configure EFS file encryption
- Configure Microsoft BitLocker to protect data at rest

- Configure Linux file system encryption to protect data at rest
- Configure a user VPN to the Azure cloud
- Configure IPsec in a Windows environment
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 16 Minutes

Secure Device &amp; OS Management

- Discover the key concepts covered in this course
- Outline various methods of hardening mobile devices such as bring your own device (BYOD), consistent security configurations, and containerization
- Recall when and how mobile devices get remotely wiped
- Use Microsoft Intune to centrally manage devices
- Delete a disk partition using a wiping tool
- Apply group policy settings to secure Windows stations
- Disable SSLv3 on Windows Server
- List common digital forensic hardware and software solutions
- List methods of securing a SAN
- Enable Azure Bastion for secure remote virtual machine (VM) management
- enable a VM managed identity for resource access
- Describe various methods of hardening network devices and device OSs
- Harden a Wi-Fi router
- Harden a network printer
- Identify the importance of hardware and software patches
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 39 Minutes

Social Engineering &amp; Malware

- Discover the key concepts covered in this course
- Recognize how social engineering uses deception to acquire sensitive information
- List the characteristics of common malware types
- Determine when email messages are fraudulent for phishing and spear phishing attacks
- Use the Social-Engineer Toolkit (SET) to execute social engineering attacks
- Configure Microsoft Windows virus and threat protection
- Upload infected files for analysis to a scanning service
- Summarize the key concepts covered in this course
- Course duration: 43 Minutes

Security Monitoring

- Discover the key concepts covered in this course
- Enable and view cloud server security recommendations
- Monitor Windows host performance
- View, search, and filter Windows logs
- Configure Windows Event Viewer log forwarding
- Monitor Linux host performance
- View, search, and filter Linux logs
- Configure the Linux syslog daemon for log forwarding
- Analyze web server access logs
- Monitor performance metrics in a cloud computing environment
- Describe true positives and negatives as well as false positives and negatives
- Recall how a SIEM solution serves as a central ingestion point for security analysis
- Recall how a SOAR solution serves as a method of automating security incident remediation
- Configure Microsoft Sentinel for data ingestion
- Summarize the key concepts covered in this course
- Course duration: 1 Hour, 24 Minutes

Tidsforbrug

Kursuspakken består af 20 kurser. Hele kursuspakken kan gennemføres på ca. 22 timer.

Form

Denne online kursuspakke består af flere forskellige kurser, som du ved tilmelding har adgang til i 365 dage. Hvert enkelt kursus er opdelt i flere kursusmoduler, som du via en oversigtsmenu kan tage i den rækkefølge, du ønsker. Modulerne indeholder lyd, billeder og tekst, der gennemgår kursusindholdet. Nogle moduler indeholder små videofilm med scenarier og cases. Ved hvert kursus har du mulighed for at teste din forståelse af indholdet med tests, som du kan tage både før, under og efter kurset. Du gennemfører kursusmodulerne via din computer eller tablet med lyd og adgang til Internettet. Du kan selv styre, hvornår du vil tage modulerne – og de kan sættes på pause undervejs.

Læs mere om vores online kurser og se svar på dine spørgsmål (FAQ)

Certificering

Vær venligst opmærksom på, at der er overensstemmelse mellem den certificeringsversion, du har forberedt dig på og den version, du bestiller eksamen i. Kurset leder hen mod certificeringen Certified Information Security Manager (CISM). Eksamen bestilles og betales særskilt. Kontakt www.isaca.org for flere informationer. Vi henviser til certificeringsudbyderens hjemmeside for nærmere information om aktuelle betingelser for at opnå certificering. I forbindelse med nogle certificeringer skal du selv oprette dig på udbyderens hjemmeside for at få adgang til eksamen.

Søgte du et andet online kursus?

Vi tilbyder en bred vifte af forskellige kurser inden for mange områder. Kontakt os på tlf. 7220 3000 eller kurser@teknologisk.dk, så vi kan hjælpe med at imødekomme dit behov.

Se desuden listen over vores udvalgte online kurser

Køb online kurser til flere

Er I en afdeling, en hel virksomhed eller blot flere personer, der ønsker adgang til online kurser, så kontakt os og få et tilbud på tlf. 7220 3000 eller kurser@teknologisk.dk

Har du faglige spørgsmål så kontakt

Malene Kjærsgaard
+45 72202523
mch@teknologisk.dk