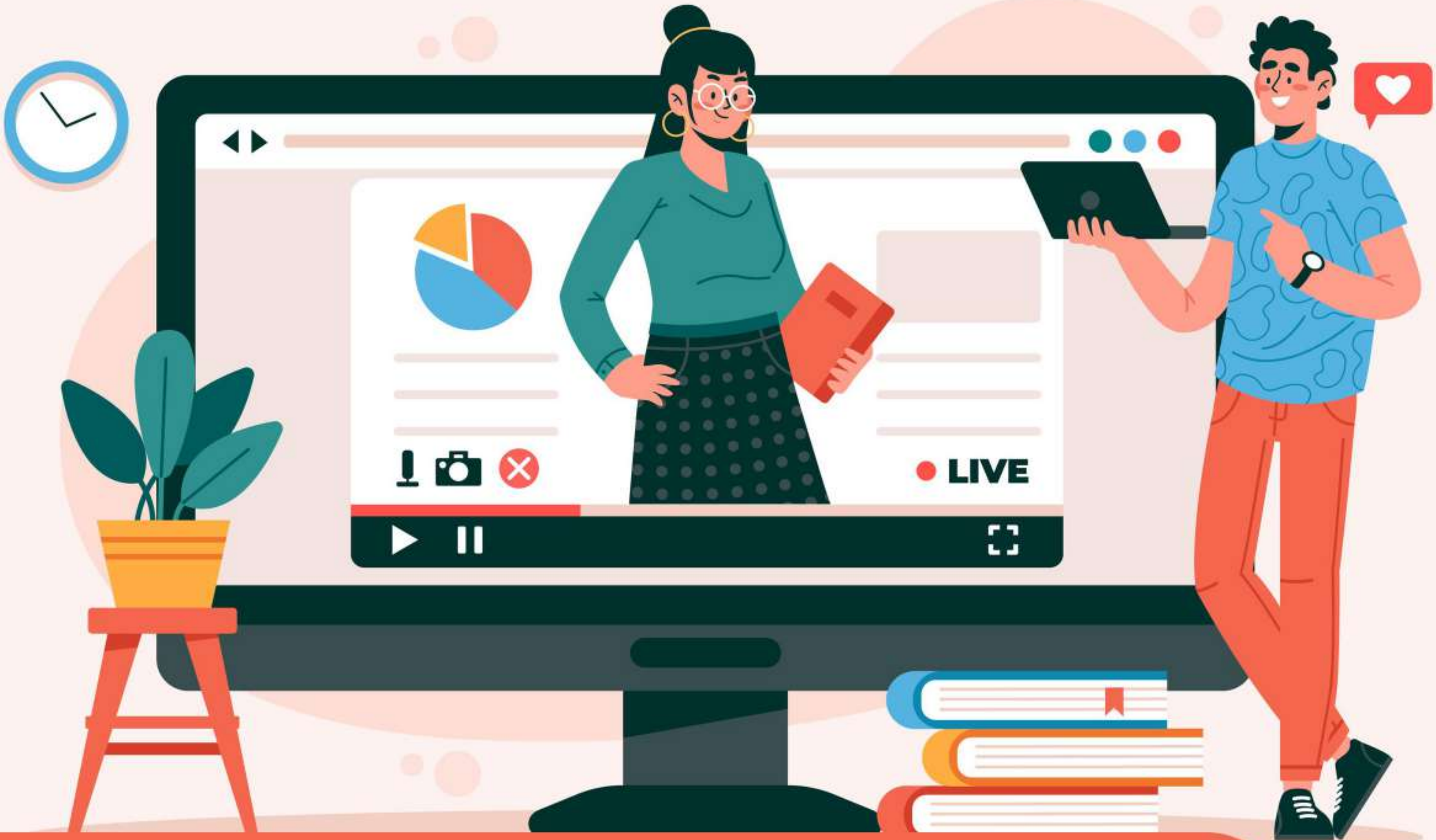
Certified Chief Information Security Officer (CCISO)

Zetlan Technologies



Learn without Leaving Home..!

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Certified Chief Information Security Officer (CCISO)

Course Modules

1. **Governance**
    - Define, implement, manage and maintain an info security gvrnanc
    - Align info security governance framework with organizational
    - Establish information security management structure.
    - Establish a framework for info security governance monitoring
    - Understd standards, procedures, directives, policies, regulations
    - Understand the enterprise info security compliance program
    - Analyze all the external laws, regulatns, standards, & best practic
    - Understd the various provisns of the laws that affct the organzatn
    - Mngmnt Act, Clinger-Cohen Act, Privacy Act, Sarbanes-Oxley, etc.
    - Be familiar with the different standards such as ISO 27000 series
    - Understand the federal and organization specific published doc
    - Assess the major enterprise risk factors for compliance.
    - Coordinate the app of info security strategies, plans, policies
    - Understand the importance of regulatory information security
    - Understand the info security changes, trends, & best practices.
    - Manage enterprise compliance program controls.
    - Understand the info security compliance process & procedures.
    - Compile, analyze, and report compliance programs.
    - Understand the compliance auditing and certification programs.
    - Follow organizational ethics.

2. Management Controls and Auditing Management

- Identify the organization’s operational process and objectives
- Design info systems controls in alignment with the optnal needs
- Identify & select the resources required to effectively implement
- Supervise the information systems control process to ensure time
- Design and implement information systems controls to mitigat
- Design and conduct testing of information security controls
- Design processes to appropriately remediate deficiencies & evalt
- Assess and implement tools and techniques to automate info
- Produce information systems control status reports

3. Auditing Management

- Undstd the IT audit process and be familiar with IT audit standrds.
- Apply information systems audit principles, skills and techniques
- Execute the audit process in accordance with established stadrds
- Effectively evaluate audit results, weighg the relevancy, accuracy
- Assess the exposures resulting from ineffective or missing control
- Develop an IT audit documentation process and share reports
- Ensure that the necessary changes based on the audit findings

4. Management Projects and Operations

- For each info systms project develop a clear project scope statmt
- Define activities needed to successfully execute the info systems
- Develop, manage and monitor the info systems program budget
- Identify, negotiate, acquire and manage the resources needed
- Acquire, develop and manage information security project team.
- Assign clear info securty personnel job functions & provide contns
- Direct information security personnel and establish communcatns
- Resolve personnel & teamwork issues within time, cost, & quality .
- Identify, negotiate & manage vendor agreement & communicatn.
- Participate with vendors & stakeholders to review/assess rcomnd
- Evaluate the project management practices and controls
- Develop a plan to continuously measure the effectiveness of info
- Identify stakeholders, manage stakeholders' expectations
- Ensure that necessary changes and improvements to the info.

Information Security Core Competence

5. Access Control

- Identify the criteria for mandatory & discretionary access control
- Implement and manage an access control plan in alignment
- Different access control systems such as ID cards and biometrics.
- Understand the importance of warning banners for implementing
- Develop procedures to ensure systm users are aware of their IA

6. Social Engineering, Phishing Attacks, Identity Theft

- Understand various social engineering concepts and their role
- Design a response plan to identity theft incidences.
- Identify and design a plan to overcome phishing attacks.

7. Physical Security

- Identify standards, procedures, directives, policies, regulations
- Determine the value of physical assets & the impact if unavailable.
- Resources needed to effectively implemnt a physical security plan.
- Design, implement & manage a coherent, coordinated, & holistic
- Establish objectives for personnel security to ensure alignment
- Design and manage the physical security audit and update issues.
- Establish a physical security performance measurement system.

Certified Chief Information Security Officer (CCISO)

8. Risk Management

- Risk mitigation & risk treatment processes & understand concept
- Identify resource requrmnts for risk management plan implemnt
- Design a systematic & structured risk assessment process
- Develop, coordinate and manage risk management teams.
- Establish relationships between the incident response team
- Develop an incident mngmnt measurement program and manag
- Understand the residual risk in the information infrastructure.
- Assess threats & vulnerabilities to identify security risks, & regulrly
- Identify changes to risk management policies and processes
- Determine if security controls & processes are adequately intgrtd

9. Disaster Recovery and Business Continuity Planning

- Develop, implement & monitor business continuity plans in case
- Define the scope of the enterprise continuity of operatns progrm
- Resourcs & roles of difft stakeholders in busins continuity prgrms.
- Identify and prioritize critical business functions and consequently
- Direct contingency planning, operatns, & programs to mange risk.
- Understand the importance of lessons learned from test, training
- Design documentation process as part of the continuity of opratn
- Design and execute a testing and updating plan for the continuity
- Understd the importance of integration of IA requirements COOP
- Measures to increase the level of emergncy preparedness

10. Firewall, IDS/IPS and Network Defense Systems

- Identify the appropriate intrusion detection & prevention systems
- Design a program to monitor firewalls & identify firewall config
- Understand perimeter defense systems such as grid sensors
- Identify the basic network architecture, models, protocols
- Understand the concept of network segmentation.
- Manage DMZs, VPN & telecomm technologies such as PBX & VoIP.
- Identify network vulnerabilities and explore network security
- Support, monitor, test, & tshoot issues wth hardware & software.
- Manage accounts, network rights, & access to systems & equipmt

11. Wireless Security

- Identify vulnerability and attacks associated with wireless netwrks

12. Virus, Trojans and Malware Threats

- Assess the threat of virus, Trojan & malware to organizatial scurty
- Deploy and manage anti-virus systems.
- Develop process to counter virus, Trojan, and malware threats.

13. Secure Coding Best Practices and Securing Web Applications

- Develop & maintain software assurance programs in alignment
- Understand various system-engineering practices.
- Configure and run tools that help in developing secure programs.
- Understand the software vulnerability analysis techniques.
- Install and operate the IT systems in a test configuration manner
- Identify web application vulnerabilities and attacks and web app

14. Hardening OS

- Identify various OS vulnerabilities and attacks & develop a plan
- Understand system logs, patch management process and config

15. Encryption Technologies

- Understand the concept of encryption & decryptn, digital certifct
- Identify the different components of a cryptosystem.
- Develop a plan for information security encryption techniques.

16. Vulnerability Assessment and Penetration Testing

- Design, develop & implement a penetration testing program basd
- Identify different vulnerabilities associated with info systems
- Develop pre and post testing procedures.
- Develop a plan for pen test reporting and implementation
- Develop vulnerability management systems

17. Computer Forensics and Incident Response

- Develop a plan to identify a potential security violation
- Comply with system termination procedures & incident reporting
- Assess potential security violatns to determine the netwrk securty
- Diagnose and resolve IA prblms in response to reported incidnts.
- Design incident response procedures.
- Develop guidelines to determine whether a security incident
- Identify the volatile and persistent system information.
- Understand various digital media devices, e-discovery principles
- Develop and manage an organizational digital forensic program.
- Establish, develop and manage forensic investigation teams.
- Design investigation processes such as evidence collection
- Identify the best prctics to acquire, store & procss digital evidnce.
- Configure and use various forensic investigation tools.
- Design anti-forensic techniques.

Strategic Planning and Finance

18. Strategic Planning

- Design, develop & maintain enterprise info security architecture
- Perform external analysis of the organization
- Identify & consult with key stakeholders to ensure understanding
- Define a forward-looking, visionary and innovative strategic plan
- Define key performance indicators and measure effectiveness
- Assess and adjust IT investments to ensure they are on track
- Monitor & update activities to ensure accountability & progress.

19. Finance

- Analyze, forecast & develop the operatnal budget of the IT dptmt.
- Acquire and manage the necessary resources for implementation
- Allocate financial resources to projects, processes & units within
- Monitor and oversee cost management of information security
- Identify and report financial metrics to stakeholders.
- Balance the IT security investment portfolio based on EISA
- Understand the acquisition life cycle & determine the importance
- Different procurement strategies & understand the importance
- Understand the basic procurement concepts such as Statement
- Collaborate with various stakeholders(which may internal client)
- Ensure the inclusion of risk-based IT security requirements
- Design vendor selection process and management policy.
- Develop contract administration policies that direct the evaluatn
- Develop measures and reporting standards to measure & report
- Understand the IA security requirements to be included in statmt

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474