Zetlan Technologies

Certified Information Systems Security Professional

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

Security and Risk Management

1. Understand, adhere to, and promote professional ethics

- ISC2 Code of Professional Ethics
- Organizational code of ethics

2. Understand and apply security concepts

- Confidentiality, integrity, and availability, authenticity, and nonrepudiation

3. Evaluate and apply security governance principles

- Alignmnt of the security function to business strategy, goals, mission, & objectivs
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
- Organizational roles and responsibilities
- Security control frameworks (e.g., International Organization for Standardization
- Due care/due diligence

4. Understand legal, regulatory, and compliance issues that pertain to info security

- Cybercrimes and data breaches
- Licensing and Intellectual Property requirements
- Import/export controls
- Transborder data flow
- Issues related to privacy (e.g., General Data Protection Regulation (GDPR), etc.,)
- Contractual, legal, industry standards, and regulatory requirements

Understand requirements for investigation types (i.e., administrative, criminal, civil, etc.,)

5. **Develop, document, and implement security policy, standards, procedures, & guidelines**
    - Alignment of the security function to business strategy, goals, mission, and objectives
    - Organizational processes (e.g., acquisitions, divestitures, governance committees)
    - Organizational roles and responsibilities
    - Security cntrl frameworks (e.g., International Organizatn for Standardizatn (ISO), (NIST), etc)
    - Due care/due diligence

6. **Identify, analyze, assess, prioritize, & implement Business Continuity (BC) requirements**
    - Business impact analysis (BIA)
    - External dependencies

7. **Contribute to and enforce personnel security policies and procedures**
    - Candidate screening and hiring
    - Employment agreements and policy driven requirements
    - Onboarding, transfers, and termination processes
    - Vendor, consultant, and contractor agreements and controls

8. **Understand and apply risk management concepts**
    - Threat and vulnerability identification
    - Risk analysis, assessment, and scope
    - Risk response and treatment (e.g., cybersecurity insurance)
    - Applicable types of controls (e.g., preventive, detection, corrective)
    - Control assessments (e.g., security and privacy)
    - Continuous monitoring and measurement and Reporting (e.g., internal, external)
    - Continuous improvement (e.g., risk maturity modeling)
    - Risk frameworks (e.g., Intrnatnal Organzatn for Standrdzatn (ISO), (NIST), (COBIT), (SABSA))

Understand and apply threat modeling concepts and methodologies

9. Apply Supply Chain Risk Management (SCRM) concepts

- Risks associated with the acquisition of products and services from suppliers and providers
- Risk mitigations (e.g., third-party assessment & monitoring, minimum security rquirmnts, etc)

10. Establish and maintain a security awareness, education, and training program

- Methods & techniques to increase awareness & training (e.g., social engineering, phishing, etc)
- Periodic content reviews to include emerging technologies and trends
- Program effectiveness evaluation

Asset Security

11. Identify and classify information and assets

- Data classification
- Asset Classification

Establish information and asset handling requirements

12. Provision information and assets securely

- Information and asset ownership
- Asset inventory (e.g., tangible, intangible)
- Asset management

13. Manage data lifecycle

- Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
- Data collection and Data location
- Data maintenance
- Data retention
- Data remanence
- Data destruction

Ensure appropriate asset retention (e.g., End of Life (EOL), End of Support)

14. Determine data security controls and compliance requirements

- Data states (e.g., in use, in transit, at rest)
- Scoping and tailoring
- Standards selection
- Data protection methods (e.g., Digital Rights Mngmnt (DRM), (DLP), (CASB))

Security Architecture and Engineering

15. Research, implement and manage engineering processes using secure design principles

- Threat modeling
- Least privilege
- Defense in depth
- Secure defaults
- Fail securely
- Segregation of Duties (SoD)
- Keep it simple and small
- Zero trust or trust but verify
- Privacy by design
- Shared responsibility
- Secure access service edge

Undrstd the fundamental concpts of security models (e.g., Biba, Star Model, Bell-LaPadula)

Select controls based upon systems security requirements

Understand security capabilities of Information Systems (IS)

16. Assess and mitigate the vulnerabilities of security architectures, designs, and solution

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems (e.g., Software as a Service (SaaS), (IaaS), Platform as a Service (PaaS))
- Distributed systems
- Internet of Things (IoT)
- Microservices (e.g., application programming interface (API))
- Containerization
- Serverless
- Embedded systems
- High-Performance Computing systems
- Edge computing systems
- Virtualized systems

17. Select and determine cryptographic solutions

- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- Public key infrastructure (PKI) (e.g., quantum key distribution

18. Understand methods of cryptanalytic attacks

- Brute force
- Ciphertext only
- Known plaintext
- Frequency analysis
- Chosen ciphertext

- Implementation attacks
- Side-channel
- Fault injection
- Timing
- Man-in-the-Middle (MITM)
- Pass the hash
- Kerberos exploitation
- Ransomware

Apply security principles to site and facility design

19. Design site and facility security controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- Environmental issues (e.g., natural disasters, man-made)
- Fire prevention, detection, and suppression
- Power (e.g., redundant, backup)

20. Manage the information system lifecycle

- Stakeholders needs and requirements
- Requirements analysis
- Architectural design
- Development /implementation
- Integration
- Verification and validation

Communication and Network Security

21. Apply secure design principles in network architectures

- Open System Interconnection (OSI) & Transmissn Control Protocol/Internet Protocol models
- Internet Protocol (IP) version 4 and 6 (IPv6) (e.g., unicast, broadcast, multicast, anycast)
- Secure protocols (e.g., Internet Protocol Security (IPSec), Secure Shell (SSH), (SSL)/ (TLS))
- Implications of multilayer protocols
- Converged protocols (e.g., Internet Small Computer Systems Interface (iSCSI), (VoIP))
- Transport architecture (e.g., topology, data/control plane, cut-through/store-and-forward)
- Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)
- Traffic flows (e.g., north-south, east-west)
- Physical segmentation (e.g., in-band, out-of-band, air-gapped)
- Logical segmentatn (e.g., virtual local area networks (VLANs), virtual private networks (VPNs))
- Micro-segmentation (e.g., network overlays/encapsulation; distributed firewalls, routers, etc.,)
- Edge networks (e.g., ingress/egress, peering)
- Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, satellite)
- Cellular/mobile networks (e.g., 4G, 5G)
- Content distribution networks (CDN)
- Software defined networks (SDN), (e.g., (API), Software-Defined Wide- Area Network,,)
- Virtual Private Cloud (VPC)
- Monitoring and management (e.g., network observability, traffic flow/shaping, etc.,)

22. Secure network components

- Operation of infrastructure (e.g., redundant power, warranty, support)
- Transmission media (e.g., physical security of media, signal propagation quality)
- Network Access Control (NAC) systems (e.g., physical, and virtual solutions)
- Endpoint security (e.g., host-based)

23. Implement secure communication channels according to design

- Voice, video, and collaboration (e.g., conferencing, Zoom rooms)
- Remote access (e.g., network administrative functions)
- Data communications (e.g., backhaul networks, satellite)
- Third-party connectivity (e.g., telecom providers, hardware support)

Identify and Access Management (IAM)

24. Control physical and logical access to assets

- Information
- Systems
- Devices
- Facilities
- Applications & Services

25. Design identification and authentication strategy (e.g., people, devices, and services)

- Groups and Roles
- Authentication, Authorization & Accounting (AAA) (e.g., multi-factor authentication (MFA),.)
- Session management
- Registration, proofing, and establishment of identity
- Federated Identity Management (FIM)
- Credential management systems (e.g., Password vault)
- Single sign-on (SSO)
- Just-In-Time

26. Federated identity with a third-party service

- On-premise
- Cloud
- Hybrid

27. Implement and manage authorization mechanisms

- Role-based access control (RBAC)
- Rule based access control
- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Attribute-based access control (ABAC)
- Risk based access control
- Access policy enforcement (e.g., policy decision point, policy enforcement point)

28. Manage the identity and access provisioning lifecycle

- Account access review (e.g., user, system, service)
- Provisioning and deprovisioning (e.g., on /off boarding and transfers)
- Role definition and transition (e.g., people assigned to new roles)
- Privilege escalation (e.g., use of sudo, auditing its use)
- Service accounts management

Implement authentication systems

Security Assessment and Testing

29. Design and validate assessment, test, and audit strategies

- Internal (e.g., within organization control)
- External (e.g., outside organization control)
- Third-party (e.g., outside of enterprise control)
- Location (e.g., on-premises, cloud, hybrid)

30. Conduct security control testing

- Vulnerability assessment
- Penetration testing (e.g., red, blue, and/or purple team exercises)
- Log reviews
- Synthetic transactions/benchmarks
- Code review and testing
- Misuse case testing
- Coverage analysis
- Interface testing (e.g., user interface, network interface, app programming interface (API))
- Breach attack simulations
- Compliance checks

31. Collect security process data (e.g., technical and administrative)

- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data, Training and awareness
- Disaster Recovery (DR) and Business Continuity (BC)

32. Analyze test output and generate report

- Remediation
- Exception handling
- Ethical disclosure

33. Conduct or facilitate security audits

- Internal (e.g., within organization control)
- External (e.g., outside organization control)
- Third-party (e.g., outside of enterprise control)
- Location (e.g., on-premises, cloud, hybrid)

Certified Information Systems Security Professional

Security Operation

34. Understand and comply with investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures
- Artifacts (e.g., data, computer, network, mobile device)

35. Conduct logging and monitoring activities

- Intrusion detection and prevention (IDPS)
- Security Information and Event Management (SIEM)
- Continuous monitoring and tuning
- Egress monitoring
- Log management
- Threat intelligence (e.g., threat feeds, threat hunting)
- User and Entity Behavior Analytics (UEBA)

Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

36. Apply foundational security operations concepts

- Need-to-know/least privilege
- Separation of Duties (SoD) and responsibilities
- Privileged account management
- Job rotation
- Service-level agreements (SLA)

37. Apply resource protection

- Media management
- Media protection techniques
- Data at rest/data in transit

38. Conduct incident management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

39. Operate and maintain detection and preventative measures

- Firewalls (e.g., next generation, web application, network)
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware
- Machine learning and Artificial Intelligence (AI) based tools

Implement and support patch and vulnerability management

Understand and participate in change management processes

40. Implement recovery strategies

- Backup storage strategies (e.g., cloud storage, onsite, offsite)
- Recovery site strategies (e.g., cold vs. hot, resource capacity agreements)
- Multiple processing sites
- System resilience, high availability (HA), Quality of Service (QoS), and fault tolerance

41. Implement Disaster Recovery (DR) processes

- Response
- Personnel
- Communications (e.g., methods)
- Assessment
- Restoration
- Training and awareness
- Lessons learned

42. Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption
- Communications (e.g., stakeholders, test status, regulators)

Participate in Business Continuity (BC) planning and exercises

43. Implement and manage physical security

- Perimeter security controls
- Internal security controls

44. Address personnel safety and security concerns

- Travel
- Security training & awarenss (e.g., insider threat, social media impacts, two-factor authentctn)
- Emergency management
- Duress

Software Development Security

45. Understand and integrate security in the Software Development Life Cycle (SDLC)

- Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framwrk)
- Maturity models (e.g., Capblty Maturity Model (CMM), Softwre Assurnc Maturty Model (SAMM))
- Operation and maintenance
- Change management
- Integrated Product Team

46. Identify and apply security controls in software development ecosystems

- Programming languages
- Libraries
- Tool sets
- Integrated Development Environment
- Runtime
- Continuous Integration and Continuous Delivery (CI/CD)
- Software configuration management (CM)
- Code repositories
- Application security testing (e.g., static application security testing (SAST), (DAST), (IAST))

47. Assess the effectiveness of software security

- Auditing and logging of changes
- Risk analysis and mitigation

48. Assess security impact of acquired software

- Commercial-off-the-shelf (COTS)
- Open source
- Third-party
- Managed services (e.g., enterprise applications)
- Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), (PaaS))

49. Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of application programming interfaces (API)
- Secure coding practices
- Software-defined security

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