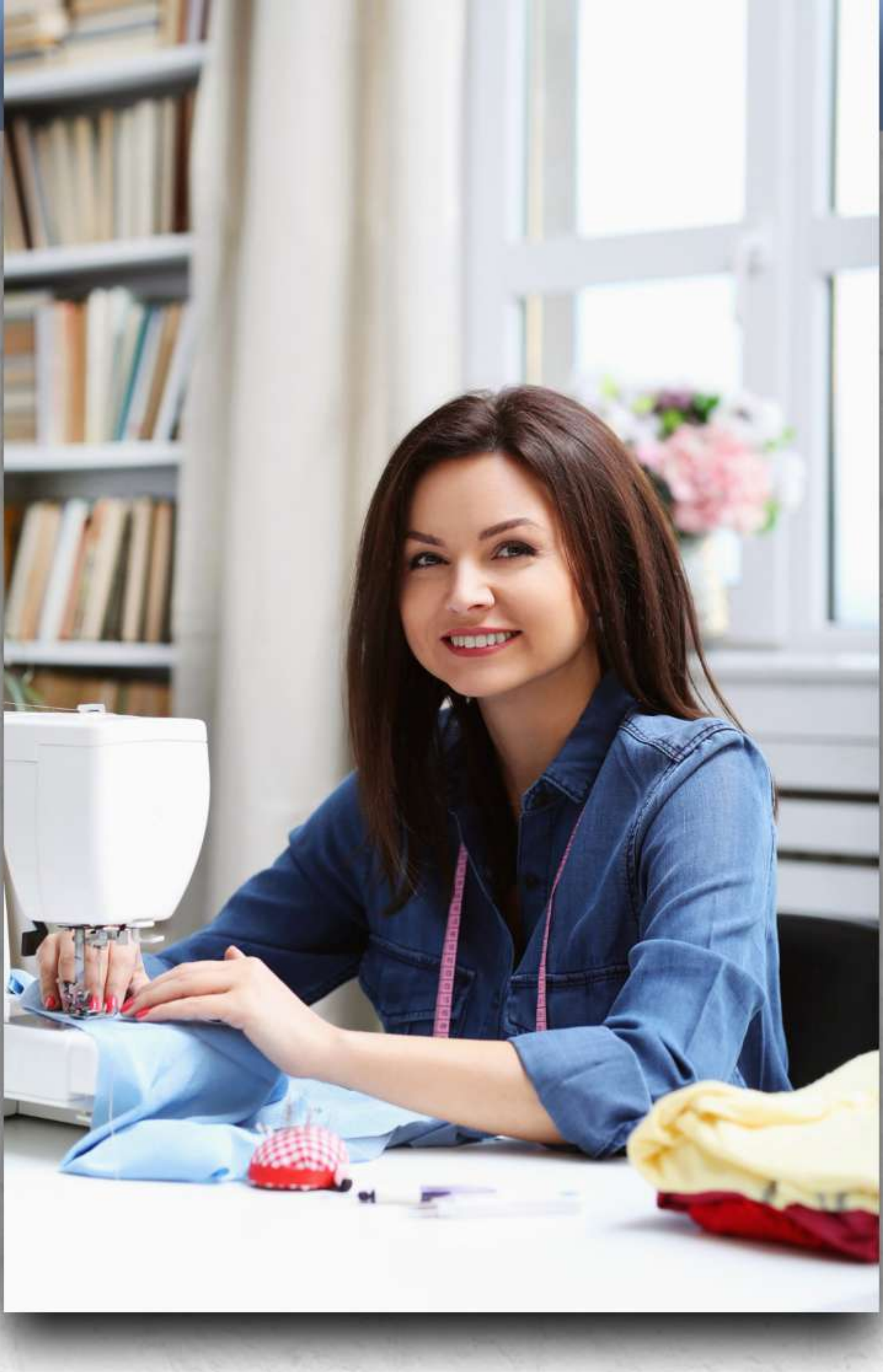

Information Systems Security Architecture Professional

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

Architect for Governance, Compliance and Risk Management

1. **Determine legal, regultory, organiztnal & industry rqurmnts**
    - Determine applicable info security standards & guidelines
    - Identify third-party and contractual obligations
    - Applicable sensitive/persnl data stndrds, guidelines & privacy
    - Design for auditability (e.g., determine regulatory, legislative..)
    - Coordinate with external entities (e.g., law enforcement., etc.,)

2. **Manage Risk**
    - Identify and classify risks
    - Assess risk
    - Recommend risk treatmt (e.g., mitigate, transfer, accept, avoid)
    - Risk monitoring and reporting

Security Architecture Modeling

3. Identify security architecture approach

- Types & scope (e.g., enterprise, network, Service-Oriented ,etc)
- Frameworks (e.g., Sherwood Applied Business Security Architctur
- Reference architectures and blueprints
- Security configuration (e.g., baselines, benchmarks, profiles)
- Network configuration (e.g., physical, logical, high availability)

4. Verify and validate design (e.g., Functional Acceptance Testing

- Validate results of threat modeling (e.g., threat vectors, impact)
- Identify gaps and alternative solutions
- Independent Verification and Validation (IV&V)

Infrastructure Security Architecture

5. Develop infrastructure security requirements

- On-premise, cloud-based, hybrid
- Internet of Things (IoT), zero trust

6. **Design defense-in-depth architecture**
    - Management networks
    - Industrial Control Systems (ICS) security
    - Network security
    - Operating systems (OS) security
    - Database security
    - Container security
    - Cloud workload security
    - Firmware security
    - User security awareness considerations

7. **Secure shared services**
    - Wireless
    - e-mail
    - Voice over Internet Protocol (VoIP)
    - Unified Communications (UC)
    - Domain Name System (DNS)
    - Network Time Protocol (NTP)

8. **Integrate technical security controls**
    - Design boundary protection (firewalls, Virtual Private Network)
    - Secure device managemnt (e.g., Bring Your Own Device (BYOD)

9. Design and integrate infrastructure monitoring

- Network visibility (e.g., sensor placement, time reconciliation)
- Active/Passive collection solutins (e.g., span port, port mirroring)
- Security analytics (e.g., Security Info & Event Managemnt (SIEM))

Infrastructure Security Architecture

10. Design infrastructure cryptographic solutions

- Determine cryptographic design considerations and constraints
- Cryptographic implmntatn (e.g., in-transit, in-use, at-rest)
- Plan key mngmnt lifecycle (e.g., generation, storage, distribution)

11. Design secure network and communication infrastructure

- Virtual Private Network (VPN)
- Internet Protocol Security (IPsec)
- Transport Layer Security (TLS)

12. Evaluate physical and environmental security requirements

- Map physical security requirements to organizational needs
- Validate physical security controls

Identity and Access Management (IAM) Architecture

12. Design identity management and lifecycle

- Establish and verify identity
- Assign identifiers (e.g., to users, services, processes, devices)
- Identity provisioning and de-provisioning
- Define trust relationships (e.g., federated, stand-alone)

13. Design access control management and lifecycle

- Access control concepts and principles (e.g., discretionary)
- Access control configs (e.g., physical, logical, administrative)
- Authorization process & workflow (e.g., governance, issuance..)

14. Design identity and access solutions

- Access control protocols and technologies
- Credential management technologies (e.g., password managmnt)
- Centralized Identity & Access Management (IAM) architecture
- Define authentication methods (e.g., Multi-Factor Authenticatn
- Authentication protocols and technologies
- Roles, rights, and responsibilities related to system, app, & DAM
- Management of privileged accounts
- Authorizatn (e.g., Single Sign-On (SSO), rule-based, role-based..)
- Decentralized Identity and Access Management (IAM) .
- Privileged Access Management (PAM) implementation

15. Design identity and access solutions

- Access control protocols and technologies
- Credential management technologies (e.g., password mangmnt)
- Centralized Identity and Access Management (IAM) architecture
- Define authentication methods (e.g., Multi-Factor Authentication
- Authentication protocols and technologies
- Roles, rights, and responsibilities related to system, application..
- Management of privileged accounts
- Authoriztn (e.g., Single Sign-On (SSO), rule-based, role-based, etc.
- Decentralized Identity and Access Management (IAM)
- on-premise, hybrid)
- Privileged Access Management (PAM) implementation
- Accounting (e.g., logging, tracking, auditing)

Architect for Application Security

16. Integrate Software Development Life Cycle (SDLC) with application security architecture (e.g., Requirements Traceability Matrix (RTM), security architecture documentation, secure coding)

- Assess code review methodology (e.g., dynamic, manual, static)
- Assess the need for application protection (e.g., (WAF),etc..)
- Determine encryption requiremnts (e.g., at-rest, in-transit, in-use)
- Assess the need for secure communications between applications
- Leverage secure code repository

Determine application security capability requirements & strategy

17. Cloud Service Providers (CSP), Software as a Service (SaaS) /Infrastructure as a Service(IaaS)/ Platform as a Service (PaaS) environments)

- Review security of apps (e.g., custom, Commercial Off-the-Shelf)
- Determine app cryptographic solns (e.g., cryptographic App
- Evaluate applicability of security controls for system components

Identify common proactive controls for applications (e.g., Open Web Application Security Project (OWASP))

Security Operations Architecture

18. Gather security operations

- Legal
- Compliance
- Organizational
- Business Requirements

19. Design information security monitoring

- Security Information and Event Management (SIEM)
- Insider threat
- Threat Intelligence
- User behaviour analytics
- Incident Response (IR) procedures
- Detection and analysis
- Proactive and automated security monitoring and remediation

20. Design Business Continuity (BC) and resiliency solutions

- Incorporate Business Impact Analysis (BIA)
- Determine recovery and survivability strategy
- Identify continuity and availability solutns (e.g., cold, warm, hot)
- Define processing agreement requirements
- Establish Recovery Time Objectives (RTO) & Recovery Point Objct
- Design secure contingency communication for operations

21. Validate Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) architecture Design Incident Response (IR) management

- Preparation (e.g., communication plan, Incident Response Plan)
- Identification
- Containment
- Eradication
- Recovery
- Review lessons learned

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