CISSP-ISSAP - Information Systems Security Architecture Professional

Course Outline

1) Architect for Governance, Compliance, and Risk Management

- Determine Legal, Regulatory, Organizational, and Industry Requirements
- Determine Applicable Information Security Standards and Guidelines
- Determine Applicable Sensitive/Personal Data Standards, Guidelines, and Privacy Regulations
- Design Systems for Auditability
- Manage Risk
- Overview of Risk Treatment
- Risk Monitoring

2) Security Architecture Modeling

- Identify Security Architecture Approach
- Review Physical Security Requirements
- Verify and Validate Design

3) Infrastructure Security Architecture

- Develop Infrastructure Security Requirements
- Design Defense-in-Depth Architecture
- Review Secure Shared Services
- Design Boundary Protection with Enterprise Security Requirements Considered
- Design Infrastructure Monitoring
- Review Introduction to Cryptographic Principles
- Design Infrastructure Cryptographic Solutions
- Asymmetric Algorithms
- Internet Protocol Security (IPSec)

4) Identity and Access Management (IAM) Architecture

- Evaluate Enterprise Identity Management Requirements
- Access Control Concepts and Principles
- Design Identity and Access Solutions

5) Architect for Application Security

- Assess and Align Application Security with the Enterprise
- Assess Code Review Methodology and Testing
- Determine Application Security Capability Requirements and Strategy
- Identify Common Proactive Controls for Applications

6) Security Operations Architecture

- Gather Security Operations Requirements
- Design Information Security Monitoring
- Design Business Continuity (BC) and Resiliency Solutions

- Validate Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) Architecture