CISM CERTIFICATION

Content

DOMAIN 1 – INFORMATION SECURITY GOVERNANCE

- Organizational Culture
- Legal, Regulatory and Contractual Requirements
- Organizational Structures, Roles and Responsibilities
- Information Security Strategy Development
- Information Governance Frameworks and Standards
- Strategic Planning (e.g., Budgets, Resources, Business Case)

DOMAIN 2 – INFORMATION SECURITY RISK MANAGEMENT

- Emerging Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Assessment and Analysis
- Risk Treatment / Risk Response Options
- Risk and Control Ownership
- Risk Monitoring and Reporting

DOMAIN 3 – INFORMATION SECURITY PROGRAM

- Information Security Program Resources (e.g., People, Tools, Technologies)
- Information Asset Identification and Classification
- Industry Standards and Frameworks for Information Security
- Information Security Policies, Procedures and Guidelines
- Information Security Program Metrics
- Information Security Control Design and Selection
- Information Security Control Implementation and Integrations
- Information Security Control Testing and Evaluation
- Information Security Awareness and Training
- Management of External Services (e.g., Providers, Suppliers, Third Parties, Fourth Parties)
- Information Security Program Communications and Reporting

DOMAIN 4 – INCIDENT MANAGEMENT

- Incident Response Plan
- Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Incident Classification/Categorization
- Incident Management Training, Testing and Evaluation
- Incident Management Tools and Techniques
- Incident Investigation and Evaluation
- Incident Containment Methods
- Incident Response Communications (e.g., Reporting, Notification, Escalation)

- Incident Eradication and Recovery
- Post-Incident Review Practices