# CISM: Certified Information Security Manager

## Domain 1: Information Security Governance (17%)

### Part A: Enterprise Governance

- Importance of Information Security Governance
- Organizational Culture
- Legal, Regulatory and Contractual Requirements
- Organizational Structures, Roles and Responsibilities

### Part B: Information Security Strategy

- Information Security Strategy Development
- Information Governance Frameworks and Standards
- Strategic Planning

## Domain 2: Information Security Risk Management (20%)

### Part A: Information Risk Assessment

- Emerging Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Analysis, Evaluation and Assessment

### Part B: Information Risk Response

- Risk Treatment/Risk Response Options
- Risk and Control Ownership
- Risk Monitoring and Reporting

## Domain 3: Information Security Program (33%)

### Part A: Information Security Program Development

- Information Security Program Overview
- Information Security Program Resources
- Information Asset Identification and Classification
- Industry Standards and Frameworks for Information Security
- Information Security Policies, Procedures and Guidelines
- Defining an Information Security Program Road Map
- Information Security Program Metrics

### Part B: Information Security Program Management

- Information Security Control Design and Selection
- Information Security Control Implementation and Integration
- Information Security Control Testing and Evaluation
- Information Security Awareness and Training
- Integration of the Security Program with IT Operations
- Management of External Services and Relationships
- Information Security Program Communications and Reporting

## Domain 4: Incident Management (30%)

### Part A: Incident Management Readiness

- Incident Management and Incident Response Overview
- Incident Management and Incident Response Plans
- Business Impact Analysis
- Business Continuity Plan
- Disaster Recovery Plan
- Incident Classification/Categorization
- Incident Management Training, Testing and Evaluation

### Part B: Incident Management Operations

- Incident Management Tools and Technologies
- Incident Investigation and Evaluation
- Incident Containment Methods
- Incident Response Communications
- Incident Eradication and Recovery
- Post-Incident Review Practices