CISM Certification Study Notes

Code: cism

Security Governance

Domain 1: Information Security Governance (17%)

Security Governance Framework

Strategic Alignment

Ensure security activities support business objectives and enterprise strategy

Value Delivery

Optimize security investments to support organizational objectives

Risk Management

Ensure risks are appropriately managed within acceptable levels

Resource Management

Use security knowledge and infrastructure efficiently and effectively

Performance Measurement

Monitor and report on security processes to ensure objectives are achieved

Roles and Responsibilities

Role	Primary Responsibility	Accountability
Board of Directors	Oversight and governance	Ultimate accountability
Executive Management	Strategic direction and support	Operational accountability
CISO	Security program leadership	Program implementation
Information Security Manager	Day-to-day operations	Tactical execution
Business Process Owners	Risk decisions for their processes	Process-level security

Security Policies

- Policies: High-level statements of management intent and direction
- Standards: Mandatory requirements that support policies
- Procedures: Step-by-step instructions for implementing standards
- Guidelines: Recommendations and best practices (not mandatory)
- Baselines: Minimum security configurations for systems

Governance Metrics

KPIs

Key Performance Indicators measure operational effectiveness

KRIs

Key Risk Indicators provide early warning of increasing risk

KGIs

Key Goal Indicators measure progress toward objectives

CSFs

Critical Success Factors define what must go well for success

Risk Management

Domain 2: Information Risk Management (20%)

Risk Assessment Process

- Asset Identification: Identify and classify information assets
- Threat Assessment: Identify potential threats to assets
- Vulnerability Assessment: Identify weaknesses that could be exploited
- Impact Analysis: Determine potential business impact
- Risk Calculation: Likelihood × Impact = Risk Level
- Risk Prioritization: Rank risks for treatment decisions

Risk Treatment Options

Option	Description	When to Use
Mitigate	Implement controls to reduce risk	When cost-effective controls available
Transfer	Shift risk to third party	Insurance, outsourcing, contracts

Option	Description	When to Use
Avoid	Eliminate the risk source	When risk exceeds acceptable levels
Accept	Acknowledge and monitor risk	When within risk appetite

Risk Analysis Methods

Quantitative

Uses numerical values: ALE = ARO × SLE. Provides monetary values for decision making

Qualitative

Uses descriptive scales (High/Medium/Low). Faster but less precise

Semi-quantitative

Combines both approaches. Assigns numerical values to qualitative ratings

Key Risk Formulas

- **SLE** (Single Loss Expectancy) = Asset Value × Exposure Factor
- **ALE** (Annual Loss Expectancy) = SLE × ARO (Annual Rate of Occurrence)
- **Risk** = Threat × Vulnerability × Impact
- **Residual Risk** = Inherent Risk - Control Effectiveness

Security Program

Domain 3: Information Security Program Development and Management (33%)

Program Development Lifecycle

- Define scope and objectives aligned with business goals
- Obtain executive sponsorship and management commitment
- Develop security strategy and roadmap
- Establish organizational structure and reporting
- Define roles, responsibilities, and accountability
- Implement continuous improvement processes

Security Controls

Control Type	Purpose	Examples
Preventive	Stop incidents from occurring	Firewalls, access controls, encryption
Detective	Identify incidents when they occur	IDS, logging, monitoring, audits
Corrective	Limit damage and restore operations	Backups, incident response, patches
Deterrent	Discourage potential attackers	Warning banners, security guards
Compensating	Alternative when primary fails	Manual processes, additional monitoring

Security Architecture

Defense in Depth

Multiple layers of security controls to protect assets

Least Privilege

Grant minimum access required to perform job functions

Separation of Duties

Divide critical functions among multiple people

Zero Trust

Never trust, always verify - regardless of location

Security Awareness and Training

- Awareness: General security knowledge for all employees
- Training: Role-specific skills development
- Education: In-depth understanding for security professionals
- Measure effectiveness through testing and metrics
- Regular updates based on emerging threats

Incident Management

Domain 4: Information Security Incident Management (30%)

Incident Response Phases

- Preparation: Develop plans, train team, acquire tools
- Identification: Detect and determine if an incident occurred
- Containment: Limit the scope and impact of the incident
- Eradication: Remove the cause of the incident

- Recovery: Restore systems to normal operation
- Lessons Learned: Document and improve processes

Incident Classification

Severity	Description	Response Time
Critical	Business-critical systems affected	Immediate
High	Significant impact to operations	Within 1 hour
Medium	Limited impact, workaround available	Within 4 hours
Low	Minimal impact to operations	Within 24 hours

Business Continuity

BIA

Business Impact Analysis identifies critical processes and recovery requirements

RTO

Recovery Time Objective - maximum acceptable downtime

RPO

Recovery Point Objective - maximum acceptable data loss

MTPD

Maximum Tolerable Period of Disruption before severe impact

Disaster Recovery

Site Type	Description	Recovery Time
Hot Site	Fully operational duplicate facility	Minutes to hours
Warm Site	Partially equipped facility	Hours to days
Cold Site	Basic facility, no equipment	Days to weeks
Mobile Site	Portable/containerized facility	Hours to days

Incident Response Best Practices

- Maintain chain of custody for evidence collection
- Document all actions taken during incident response
- Communicate appropriately with stakeholders
- Test incident response plans regularly
- Update plans based on lessons learned

Exam Tips

CISM Exam Preparation Tips

Exam Focus Areas

- Focus on management perspective - CISM is about managing security, not technical implementation
- Understand the relationship between business objectives and security strategy
- Know the difference between governance and management responsibilities

- Study risk assessment methodologies and be able to apply them
- Understand incident response phases and business continuity planning
- Remember: The best answer supports business objectives while managing risk

⚖️ Domain Weights

Domain	Weight	Focus Areas
Domain 1: Information Security Governance	17%	Strategy, policies, roles, metrics
Domain 2: Information Risk Management	20%	Risk assessment, treatment, monitoring
Domain 3: Security Program	33%	Controls, architecture, awareness
Domain 4: Incident Management	30%	Response, BCP, DRP

Key Exam Strategies

- **Think like a manager:** Focus on oversight, not technical details
- **Business alignment:** Security must support business objectives
- **Risk-based approach:** Decisions should be based on risk assessment
- **Cost-benefit:** Consider ROI of security investments
- **Compliance:** Know regulatory and legal requirements