CISA Certification Study Notes

Code:

Audit Process

Domain 1: Information Systems Auditing Process (21%)

IS Audit Planning

- Risk Assessment: Identify and prioritize audit areas based on risk
- Audit Universe: Complete inventory of all auditable entities
- Audit Charter: Defines authority, scope, and responsibilities
- Audit Planning: Develop audit program and resource allocation
- Engagement Letter: Documents scope, objectives, and responsibilities

Evidence Collection

- Sufficient: Enough evidence to support findings and conclusions
- Reliable: Evidence from authoritative, credible sources
- Relevant: Directly relates to audit objectives
- Useful: Helps the auditor reach conclusions

Audit Methodologies

Method	Description	When to Use
Risk-based	Focus on higher-risk areas	Limited resources, prioritization needed
Control-based	Evaluate control effectiveness	Assess internal control framework
Process-based	Review end-to-end processes	Understand business workflows
Compliance-based	Verify adherence to requirements	Regulatory or policy compliance

Exam Focus Areas

Exam Tips for Domain 1:

- Know the IS audit standards (ISACA framework)
- Understand evidence hierarchy: observation > confirmation > inquiry
- Remember audit independence is paramount
- Follow-up is part of the audit cycle - don't forget it!

IT Governance

Domain 2: Governance and Management of IT (16%)

IT Governance Frameworks

- COBIT: Framework for IT governance and management
- ISO/IEC 38500: International standard for IT governance
- ITIL: Service management best practices

- Val IT: Framework for value delivery from IT investments

IT Strategy Alignment

- Strategic Alignment: IT strategy supports business strategy
- Value Delivery: Optimize IT investments for business value
- Risk Management: Manage IT-related risks appropriately
- Resource Management: Use IT resources efficiently
- Performance Measurement: Monitor and report on IT performance

Key Governance Concepts

- **Governance**: Ensures objectives are achieved (Board/Executive responsibility)
- **Management**: Plans, builds, runs, and monitors (Day-to-day responsibility)
- **Steering Committee**: Prioritizes IT projects and resources
- **Enterprise Architecture**: Blueprint for aligning IT with business

SDLC & Development

Domain 3: IS Acquisition, Development and Implementation (18%)

SDLC Phases

- Feasibility Study: Assess technical and economic viability
- Requirements: Define functional and technical requirements
- Design: Create system architecture and detailed design
- Development: Code and build system components
- Testing: Verify system meets requirements
- Implementation: Deploy to production environment

- Post-implementation: Evaluate and maintain

Testing Types

Test Type	Purpose	Responsibility
Unit Testing	Test individual components	Developers
Integration Testing	Test component interactions	QA Team
System Testing	Test complete system	QA Team
UAT	Validate business requirements	End Users
Parallel Testing	Compare new vs old system	Business Users

Key SDLC Audit Points

- User requirements must be documented and approved
- Segregation of duties in development (dev ≠ prod access)
- Change management controls prevent unauthorized changes
- User acceptance testing is critical before go-live

Operations & BCP

Domain 4: IS Operations and Business Resilience (20%)

IT Operations Management

- Service Level Management: Monitor and report on SLA performance
- Capacity Management: Ensure adequate resources for demands
- Availability Management: Maximize system uptime and reliability
- Incident Management: Restore services quickly after disruptions
- Problem Management: Identify and address root causes
- Change Management: Control implementation of changes

BCP/DR Components

- BIA: Business Impact Analysis identifies critical functions
- RTO: Recovery Time Objective - maximum acceptable downtime
- RPO: Recovery Point Objective - maximum acceptable data loss
- Hot Site: Fully equipped, ready for immediate use
- Warm Site: Partially equipped, ready within days
- Cold Site: Empty facility, ready within weeks

Exam Focus Areas

Exam Tips for Domain 4:

- RTO and RPO are critical metrics for DR planning
- BCP testing should occur regularly (annual minimum)
- Incident response should be documented and rehearsed
- Change management prevents unauthorized modifications

Asset Protection

Domain 5: Protection of Information Assets (25%)

Access Control

- Identification: Claiming an identity (username)
- Authentication: Proving identity (password, biometrics)
- Authorization: Granting access rights (permissions)
- Accountability: Logging actions for audit trail
- Least Privilege: Minimum access necessary for duties
- Need to Know: Access only to relevant information

Network Security

Control	Purpose	Implementation
Firewall	Filter network traffic	Stateful inspection, packet filtering
IDS/IPS	Detect/prevent intrusions	Signature-based, anomaly-based
VPN	Secure remote access	Encrypted tunnels, authentication
DMZ	Isolate public services	Dual-firewall architecture
NAC	Control device access	Pre-admission, post-admission checks

Cryptography Basics

- Symmetric: Same key for encryption/decryption (AES, DES)
- Asymmetric: Public/private key pairs (RSA, ECC)
- Hashing: One-way function for integrity (SHA-256, SHA-3)

- Digital Signature: Authenticity and non-repudiation
- PKI: Public Key Infrastructure for certificate management

Security Control Types

- **Preventive**: Stop incidents before they occur (firewalls, encryption)
- **Detective**: Identify incidents when they occur (IDS, logs)
- **Corrective**: Fix issues after incidents (patches, restoration)
- **Deterrent**: Discourage potential attackers (warnings, policies)
- **Compensating**: Alternative control when primary is unavailable