CISA

LAST MINUTE STUDY GUIDE

ALL DOMAINS!

ONE

DESTINATION!

MOS

CISA? Sounds Boring, Right?

CISA?
Information Systems Auditing?
Let's be honest — it *sounds* boring.

Too boring to read.
Too boring to understand.
Too boring to even start with.
You've probably heard it's *all about controls, frameworks, and policies*.

And your first thought?

"Nope. Not for me."

But wait — if it's really that boring...
then what are *we* doing here? 🤔

Are we just here to give you gyaan and throw frameworks at you?
No, not at all.

We're here to show you *what CISA truly is* —
how it shapes your mindset as an auditor,
how every domain connects to real-world scenarios,
and how you can actually *enjoy learning* what most people fear.

So buckle up — this isn't another dull study guide.
This is CISA made human. CISA made simple. CISA made fun.

And here's a pro tip before we even begin:

CISA isn't boring — you've just never seen it explained right.

CISA? THAT'S THE AUDIT THING, RIGHT? SOUNDS BORING.
YOU'VE CLEARLY NEVER READ MY STUDY GUIDE.
MOS STUDY GUIDE

What Does CISA Cover?

Alright, so now that we've agreed CISA isn't boring -
let's get into what it *actually* includes.

The CISA certification is built around **5 core domains**, and each one focuses on a different part of IT auditing.

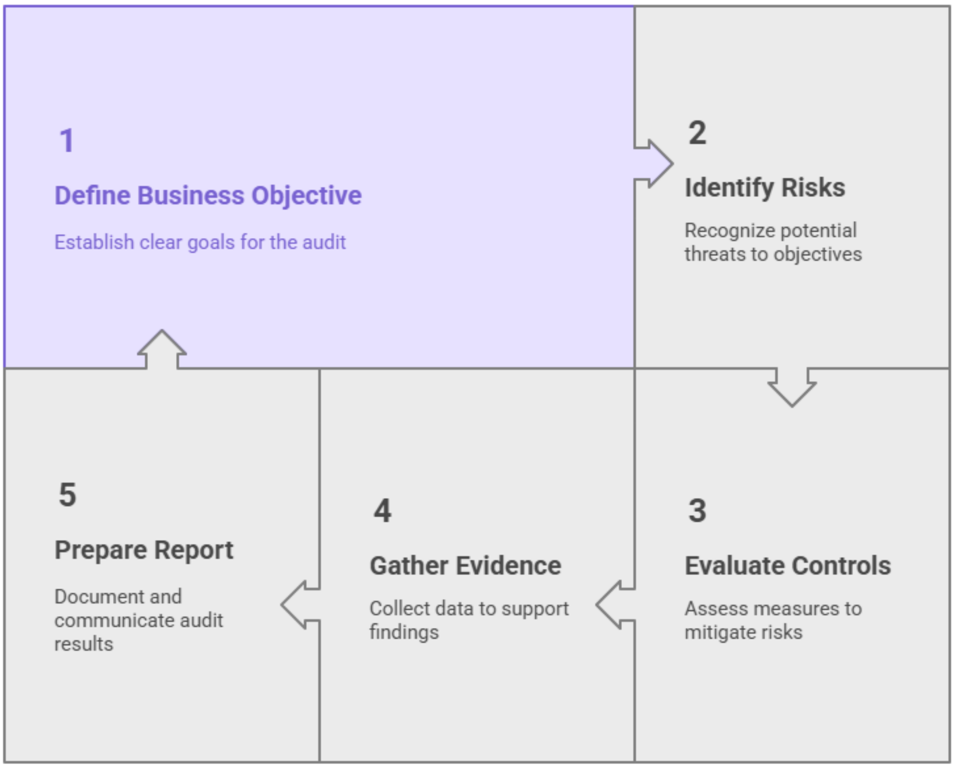
Here's how they're divided ⬇️

Domain	Weightage
1️⃣ Information System Auditing Process	**21%**
2️⃣ Governance and Management of IT	**17%**
3️⃣ Information Systems Acquisition, Development and Implementation	**12%**

Let's deep delve in each domain in detail!!

DOMAIN 1: Information Systems Auditing Process

How an Auditor Thinks


1
Define Business Objective
Establish clear goals for the audit
2
Identify Risks
Recognize potential threats to objectives
3
Evaluate Controls
Assess measures to mitigate risks
4
Gather Evidence
Collect data to support findings
5
Prepare Report
Document and communicate audit results

CHAPTER 1 — The IS Audit Function and Its Environment

Learning Objectives

- Understand the purpose, scope, and objectives of the IS audit function.
- Explain how IS auditing supports enterprise governance, risk, and compliance.
- Understand the auditor's ethical and professional responsibilities.
- Identify and apply ISACA's IT Audit and Assurance Standards.

1.1 Definition and Purpose of IS Auditing

Information Systems (IS) Auditing involves the collection and evaluation of evidence to determine whether an organization's information systems:

1. Safeguard assets
2. Maintain data integrity
3. Operate effectively to achieve business goals
4. Comply with relevant laws and regulations

Objectives

- Provide independent assurance to stakeholders.
- Identify and assess risks and control weaknesses.
- Recommend risk mitigation and process improvement.
- Support effective IT governance.

1.2 IS Auditing vs. Other Audit Types

Audit Type	Focus Area	Example
Financial Audit	Accuracy of financial reporting	Review of GL and accounting controls
Operational Audit	Efficiency and effectiveness	Evaluating IT incident management
Compliance Audit	Adherence to laws and regulations	GDPR, HIPAA, SOX

Information Systems Audit	Security, availability, integrity, confidentiality	Auditing backup management system

Integrated audits combine IS and operational/financial components.

1.3 The IS Audit Function in Governance Framework

The IS audit function contributes to governance by:

- Providing assurance that IT supports business goals.
- Validating the effectiveness of risk management.
- Ensuring control systems protect assets and data.

It should be organizationally independent, ideally reporting to:

- The Audit Committee
- The Board of Directors, or
- A Chief Audit Executive (CAE)

This ensures unbiased assessments.

1.4 IT Governance and Framework Integration

Governance ensures decisions are made in alignment with organizational objectives, accountability is defined, and performance is monitored.

Key Frameworks

Framework	Key Focus	Domain Relevance
COBIT 2019	Governance and management of enterprise IT	Core reference framework
COSO ERM	Enterprise Risk Management	Risk alignment
ISO/IEC 27001	Information Security Management Systems	Security assurance
NIST 800-53	Security and Privacy Controls	Control catalog reference

COBIT 2019 Governance System Principles:

1. Provide stakeholder value
2. Holistic governance system
3. Dynamic governance
4. Governance distinct from management
5. Tailored to enterprise needs

COBIT Components → Processes, Organizational Structures, Policies, Information Flows, Culture, Skills, and Services.

1.5 ISACA IT Audit and Assurance Standards

Mandatory professional standards for CISA-certified professionals:

Standard	Summary
1000 – Purpose and Responsibility	Defines IS audit charter, objectives, and authority.
1200 – Independence	Auditor must maintain organizational and mental independence.
1400 – Conduct of Audit Work	Requires proper planning, supervision, and documentation.
2200 – Reporting	Reports must be complete, accurate, objective, and timely.
2400 – Follow-up Activities	Ensures recommendations are implemented effectively.

Guidelines (recommended practices)

- IS auditing guidelines support the application of the standards.
- They aren't mandatory but enhance quality and consistency.

1.6 IS Auditor's Ethics and Responsibilities

ISACA Code of Professional Ethics

1. Support implementation of appropriate standards.

2. Perform duties with due diligence, competence, and objectivity.
3. Maintain confidentiality.
4. Serve stakeholders honestly and fairly.
5. Engage in continuous professional education (CPE).

Auditor Responsibilities

- Plan and conduct audits in alignment with professional standards.
- Maintain professional skepticism.
- Report significant control deficiencies.
- Recommend remediation or mitigation actions.

1.7 Risk Concepts in Auditing

Audit risk is the risk of forming an incorrect conclusion.

Audit Risk = Inherent Risk × Control Risk × Detection Risk

Risk Type	Description	Example
Inherent Risk	Risk existing before controls	Complexity of IT environment
Control Risk	Risk that controls fail	Poor access management
Detection Risk	Risk auditor misses issues	Insufficient testing

Goal: Keep *audit risk* at an acceptably low level.

1.8 Risk-Based Audit Planning

Audits must be prioritized based on risk assessments.

Steps:

1. Identify audit universe (systems, apps, processes).
2. Determine risk ranking (impact × likelihood).
3. Select high-risk areas for focus.
4. Define audit objectives, criteria, and scope.
5. Develop risk-based audit plan.

Risk Assessment Inputs

- Regulatory requirements
- Past audit findings
- Emerging threats
- Management priorities
- System changes

1.9 Evidence, Sampling, and Documentation

Type of Evidence	Examples
Physical	Site visits, access control checks
Documentary	Policies, logs, configs
Analytical	Ratio, trend, variance analysis
Testimonial	Interviews, walkthroughs

Audit evidence must be:

- Sufficient
- Reliable
- Relevant
- Useful

Sampling Techniques

- **Statistical Sampling:** Random, systematic, stratified.
- **Non-statistical Sampling:** Judgmental, block, haphazard.

Documentation Requirements:

- Audit scope and objectives
- Work performed
- Evidence collected
- Findings and recommendations
- Sign-offs and approvals

1.10 Quality Assurance and Audit Supervision

Quality assurance ensures:

- Adherence to standards
- Adequate supervision
- Peer review
- Continuous improvement

Supervisors ensure audit trail, cross-referencing, and review notes are maintained.

Chapter 2: Audit Planning

2.1 Purpose of Audit Planning

Audit planning ensures that the audit engagement is carried out efficiently, effectively, and in accordance with applicable standards.
It establishes the foundation for all subsequent audit activities by defining what is to be audited, why it is being audited, and how the audit will be executed.

Objectives of planning:

- Ensure appropriate audit scope and objectives are defined.
- Identify significant risk areas requiring detailed testing.
- Allocate resources and time effectively.
- Coordinate with auditees and avoid duplication of effort.
- Ensure compliance with ISACA IT Audit and Assurance Standard 1400 (Conduct of Audit Work).

Audit planning must result in a formal audit plan, audit program, and audit work papers that guide fieldwork.

2.2 Inputs to Audit Planning

Effective planning depends on accurate and comprehensive information about the environment being audited. Key inputs include:

1. **Enterprise mission, vision, and strategy**
   – Understanding organizational goals ensures the audit aligns with business priorities.
2. **IT strategy and architecture**
   – Identifies critical applications, technologies, and dependencies.
3. **Regulatory and compliance requirements**
   – Determines applicable laws and standards (e.g., SOX, GDPR, HIPAA, PCI DSS).
4. **Previous audit results and open issues**
   – Highlights recurring risks or control deficiencies.
5. **Risk assessment reports**
   – Provide prioritization of high-risk areas to guide resource allocation.
6. **Management concerns and emerging risks**
   – Reflect business priorities, acquisitions, migrations, or technology transitions.

2.3 Establishing Audit Objectives

Audit objectives define the purpose and intended outcome of the audit engagement. They must be specific, measurable, achievable, relevant, and time-bound (SMART).

Typical audit objectives:

- Evaluate the effectiveness and efficiency of IT controls.

- Assess compliance with internal policies, procedures, and legal mandates.
- Determine adequacy of risk mitigation mechanisms.
- Validate data integrity, confidentiality, and availability.
- Identify process improvement opportunities.

Audit objectives are derived from the risk assessment and control framework used (COBIT, COSO, ISO 27001, etc.).

2.4 Defining Audit Scope and Criteria

Scope defines the boundaries and extent of the audit.
It includes systems, business units, geographical locations, and time period under review.

The **audit scope** should state:

- Systems, applications, and processes covered.
- Interfaces and third-party dependencies.
- Exclusions (out-of-scope components).
- Audit period or transactions reviewed.

Audit criteria are the benchmarks against which evidence is evaluated.
They may be based on:

- Organizational policies and procedures.
- Industry best practices (COBIT, ISO 27001, NIST SP 800-53).
- Legal or contractual obligations.
- Management-approved standards.

2.5 Performing Risk Assessment for Audit Planning

A **risk-based approach** ensures that limited audit resources are directed toward areas of greatest potential impact.

Risk Assessment Steps

1. **Identify auditable entities** – applications, systems, processes, or business units.
2. **Determine inherent risks** – risks before considering controls.

3. **Evaluate control risk** – effectiveness of existing controls.
4. **Assess residual risk** – remaining exposure after controls.
5. **Prioritize entities** based on risk ranking (high, medium, low).
6. **Select audit topics** accordingly.

Factors to consider:

- Business impact and financial materiality.
- Volume and sensitivity of information processed.
- Complexity of technology and change frequency.
- Past incidents or audit findings.
- Regulatory significance.

The risk assessment results form the basis for the annual audit plan and the individual engagement plan.

2.6 Developing the Audit Plan

The audit plan (often called the annual or strategic plan) documents all audit engagements scheduled within a given cycle, typically one year.

Elements of an audit plan:

- Audit universe and ranking.
- Planned audits with schedule and resource estimate.
- Risk level and rationale for selection.
- Audit team members and required skills.
- Dependencies, assumptions, and constraints.
- Management approval and communication schedule.

The audit plan should be dynamic, reviewed periodically, and updated when significant business or IT changes occur.

2.7 Establishing the Audit Charter

The **Audit Charter** is a formal document that defines the purpose, authority, and responsibility of the audit function.
It is approved by senior management and the board or audit committee.

Contents of the audit charter:

- Mission and scope of internal audit.
- Organizational independence and reporting structure.
- Rights of access to records, systems, and personnel.
- Responsibility for maintaining confidentiality.
- Standards and methodologies followed (ISACA Standards, COBIT, etc.).
- Authority to communicate findings and recommendations.

The charter legitimizes the auditor's role and ensures unrestricted access for performing the audit.

2.8 Resource and Time Management

Effective planning includes estimation and allocation of resources:

Key components:

- **Skill assessment** – Ensure auditors possess required technical and business knowledge.
- **Budgeting** – Estimate time and cost for each audit phase.
- **Scheduling** – Coordinate with operational cycles to minimize disruption.
- **Tools** – Identify required automated audit tools (CAATs, data-analytics platforms).
- **Coordination** – Plan collaboration with external auditors or assurance providers.

Resource constraints must be documented, justified, and approved.

2.9 Audit Engagement Planning and Preliminary Survey

Before fieldwork begins, auditors perform a preliminary survey to understand the audit area.
This involves reviewing policies, procedures, organizational charts, and system documentation.

Activities include:

- Interviewing key stakeholders.
- Understanding process flows and control points.
- Identifying information systems supporting the process.
- Assessing internal control design.
- Determining data availability for testing.

Based on this, the auditor develops the audit program, a detailed list of procedures and tests to be performed.

2.10 Coordination, Communication, and Approval

Planning concludes with management communication and approval.

Key deliverables:

- Draft audit plan and scope statement.
- Audit objectives and schedule.
- Resource plan.
- Request for auditee cooperation.
- Approval from the CAE or audit committee.

Once approved, the plan becomes the official roadmap for audit execution.

2.11 Common Pitfalls in Audit Planning

- Scope too broad or vague, causing ineffective coverage.
- Lack of updated risk assessment or outdated control references.
- Insufficient coordination with stakeholders leading to scheduling conflicts.
- Overlooking regulatory or contractual obligations.
- Failing to consider emerging technologies (cloud, DevOps, AI systems).

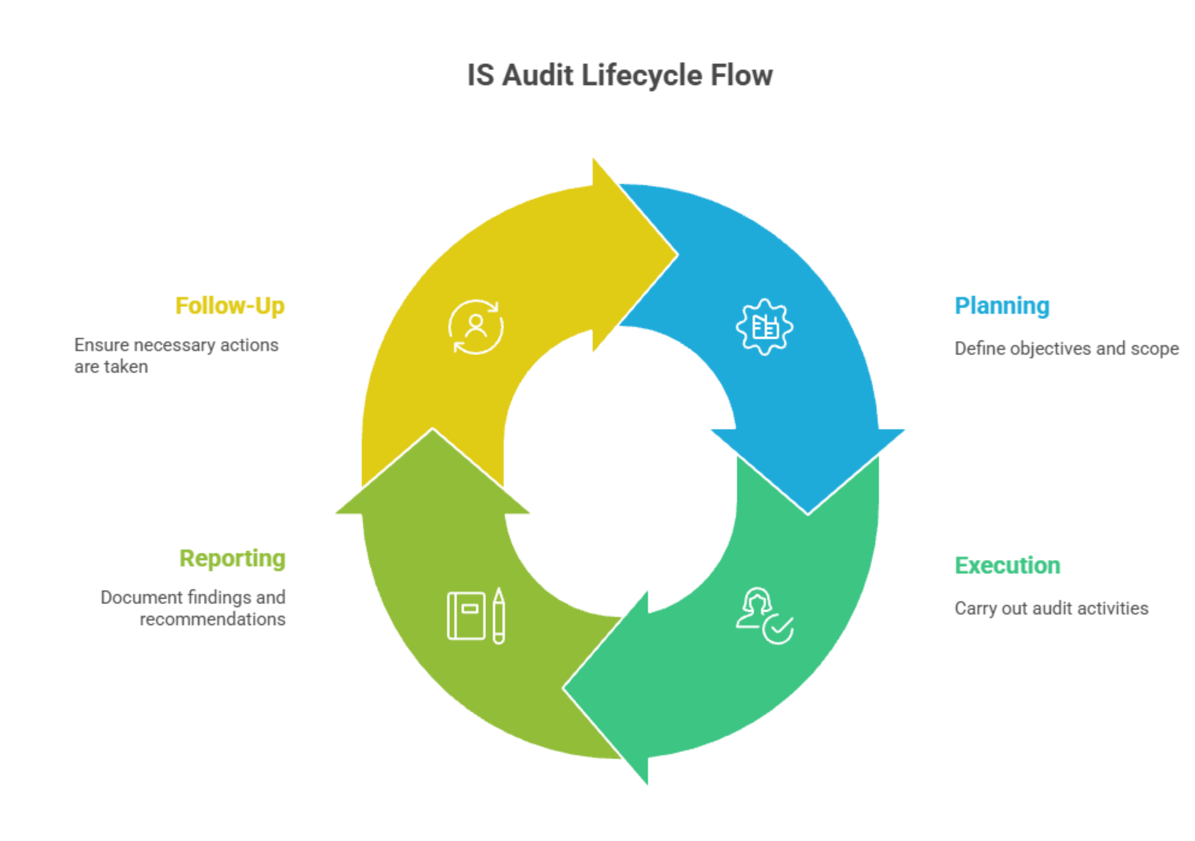
2.12 Deliverables of Audit Planning

- Audit Charter (if new function)

- Annual Risk-Based Audit Plan
- Individual Engagement Plan
- Detailed Audit Program
- Resource Allocation Document
- Preliminary Risk Assessment Report

All deliverables must be approved, documented, and archived for reference and quality assurance reviews.

Chapter 3 — Audit Execution (Fieldwork and Testing)


IS Audit Lifecycle Flow
Follow-Up
Ensure necessary actions are taken
Planning
Define objectives and scope
Reporting
Document findings and recommendations
Execution
Carry out audit activities

3.1 Purpose

Audit execution (also called fieldwork) involves performing the procedures defined in the audit plan and program to collect and evaluate evidence, determine whether controls are designed and operating effectively, and reach conclusions regarding the objectives set during planning.

3.2 Conducting Fieldwork

Fieldwork begins after management approval of the plan and notification to auditees. Key activities include:

1. **Kick-off meeting:** Confirm objectives, scope, timeframe, logistics, and communication paths.
2. **Walkthroughs:** Trace sample transactions through the process to understand control flow.
3. **Observation and inquiry:** Observe operations, interview personnel, and identify control gaps.
4. **Control testing:** Verify the existence, design, and operation of key controls.
5. **Evidence evaluation:** Correlate results across multiple tests and data sources.

All activities must be documented in work papers and linked to specific audit objectives.

3.3 Evidence Collection and Evaluation

Evidence qualities: sufficient, reliable, relevant, and useful.

Evidence Type	Example	Evaluation Method
Physical	Data-center walkthrough, inventory of devices	Observation
Documentary	Policies, change-tickets, logs	Inspection
Testimonial	Staff interviews	Corroboration
Analytical	Data correlations, trend analysis	Computation

The auditor must cross-verify evidence types to strengthen assurance.

3.4 Audit Testing Methods

1. **Compliance Testing** – Determines whether controls are operating as designed. *Example:* Check whether access reviews are performed quarterly.
2. **Substantive Testing** – Verifies the accuracy and integrity of data or transactions. *Example:* Reconcile sample accounting entries with source documentation.
3. **Analytical Procedures** – Identify anomalies through ratios, trends, or variance analysis.

4. **Re-performance and Observation** – Auditor replicates control actions to confirm function.
5. **Inquiry and Confirmation** – Obtain representations or confirmations from management or third parties.

3.5 Computer-Assisted Audit Techniques (CAATs)

CAATs allow auditors to analyze large datasets efficiently and independently.

Categories:

- **Data Extraction and Analysis Tools:** ACL, IDEA, SQL, Python scripts.
- **Test Data:** Use of fictitious transactions to validate application controls.
- **Parallel Simulation:** Auditor processes real data through a validated program to compare results.
- **Integrated Test Facility (ITF):** Permanent test environment within production system.
- **Continuous Auditing and Monitoring:** Automated, near-real-time control verification.

Benefits: completeness of testing, early detection, efficiency, independence.
Risks: data integrity issues, access security, and misinterpretation if poorly designed.

3.6 Sampling Techniques

Sampling enables conclusions on an entire population from limited data.

Sampling Type	Description	Example
Statistical	Random, systematic, or stratified; allows extrapolation	Random selection of 50 transactions
Non-statistical	Based on auditor judgment	Targeted review of high-value payments

Key parameters: population size, expected error rate, tolerable error rate, confidence level.

3.7 Control Evaluation

Auditors must determine:

- **Control Design Effectiveness:** Whether control is appropriately designed to mitigate risk.
- **Control Operating Effectiveness:** Whether control operates as intended over time.

Results are typically rated (Effective / Partially Effective / Ineffective) and mapped to risks.

3.8 Documentation and Work Papers

Work papers provide audit trail and evidence of compliance with standards.
They must include:

- Objectives, scope, and methodology.
- Detailed test steps and results.
- Cross-references to evidence.
- Conclusions and reviewer sign-off.

Retention should follow the organization's audit-document policy and regulatory requirements.

3.9 Supervision and Review

Supervisors ensure:

- Audit work aligns with plan and standards.
- Evidence supports conclusions.
- Deviations are justified and approved.
- Review notes are cleared before finalization.

3.10 Interim Communications

When significant findings arise during fieldwork, auditors must promptly inform management to enable timely remediation rather than waiting for the final report.

Chapter 4 — Audit Reporting and Communication

4.1 Purpose

The audit report communicates findings, conclusions, and recommendations to stakeholders and serves as the basis for corrective action and governance oversight.

4.2 Report Objectives

- Provide clear, factual, and unbiased results.
- Relate findings to business risks and impacts.
- Recommend practical, risk-based remediation.
- Promote accountability and improvement.
- Fulfil ISACA Standard 2200 (Reporting).

4.3 Structure and Content of Audit Report

Typical sections:

1. **Executive Summary:** Key observations, risk rating, overall opinion.
2. **Background:** Context, systems, processes audited.
3. **Scope and Objectives:** Boundaries and focus areas.
4. **Methodology:** Audit techniques and period.
5. **Detailed Findings and Recommendations:**
   - Condition (what was found)
   - Criteria (standard or policy violated)
   - Cause (why issue occurred)
   - Effect (impact or risk)
   - Recommendation (proposed corrective action)
6. **Management Response:** Agreed action, owner, target date.
7. **Auditor's Conclusion:** Overall assessment.
8. **Appendices:** Supporting data, definitions, risk scales.

4.4 Communication Process

1. **Draft Report Preparation** – Based on validated findings.

2. **Exit Meeting** – Discuss results, confirm accuracy, and address disputes.
3. **Final Report Issuance** – Distributed to management, board, or audit committee.
4. **Follow-up and Closure** – Verify implementation of corrective actions.

Communication must be timely, precise, and documented.

4.5 Rating and Prioritization of Findings

Findings are categorized by:

- **Severity:** High / Medium / Low
- **Impact:** Financial, regulatory, operational, reputational
- **Likelihood:** Probability of occurrence

Prioritization ensures management focuses on the most critical risks.

4.6 Handling Disagreements and Conflicts

If management disputes findings:

- Provide supporting evidence.
- Re-validate facts collaboratively.
- Escalate unresolved issues to audit management or the audit committee.
- Document all discussions and final resolution.

4.7 Audit Follow-Up

Follow-up ensures recommendations are implemented and effective.

Activities:

- Request progress updates and supporting evidence.
- Perform verification testing where required.
- Update issue-tracking logs.
- Report unresolved issues to senior management.

4.8 Quality Review of Audit Reports

Audit managers perform quality review to confirm:

- Accuracy, completeness, and balance.
- Consistency with fieldwork evidence.
- Compliance with internal reporting templates and ISACA Standards.

Chapter 5 — Audit Risk and Quality Management

5.1 Audit Risk Concepts

Audit risk is the risk that the auditor expresses an inappropriate conclusion.

Audit Risk = Inherent Risk × Control Risk × Detection Risk

Component	Meaning	Example
Inherent Risk	Susceptibility of area to error or fraud	Complex automated calculations
Control Risk	Risk controls fail to prevent/detect	Weak segregation of duties
Detection Risk	Risk auditor fails to detect	Insufficient sampling or testing

Audit procedures should minimize detection risk to maintain overall acceptable audit risk.

5.2 Managing Audit Risk

- Use risk-based approach throughout audit lifecycle.
- Reassess risk continuously as new information emerges.
- Document rationale for risk judgments.
- Design testing to achieve reasonable assurance, not absolute certainty.

5.3 Audit Quality Management

A robust Quality Assurance and Improvement Program (QAIP**)** ensures continuous adherence to standards and improvement in audit performance.

Key components:

- Internal Quality Reviews – Periodic peer review of completed engagements.

- External Assessments – Independent evaluation at least every five years.
- Continuous Improvement – Capture lessons learned, training needs, and process enhancements.
- Performance Metrics – Timeliness, budget adherence, client satisfaction, implementation rate.

5.4 Compliance with ISACA Standards

Auditors must conform to:

- IT Audit and Assurance Standards (1000-series).
- ISACA Guidelines and Tools.
- Organizational policies and applicable laws.

Non-compliance must be documented and justified.

5.5 Professional Competence and Independence

Auditors should:

- Maintain professional competence through CPE and training.
- Observe independence and objectivity both organizationally and mentally.
- Avoid conflicts of interest or self-review threats.
- Use external specialists when required while retaining overall responsibility.

5.6 Quality Control During Engagement

Supervisory reviews should confirm:

- Audit objectives achieved.
- Evidence supports conclusions.
- Documentation complete and traceable.
- Any deviations approved and explained.

5.7 Continuous Improvement and Lessons Learned

Post-engagement review captures:

- Effectiveness of planning, testing, and communication.
- Stakeholder feedback.
- Opportunities to refine methodology and tools.

Improvements are integrated into future audit programs.

5.8 Final Deliverables of Domain 1

- Approved audit charter and plan
- Completed audit program and work papers
- Final audit report and management responses
- Follow-up and closure documentation
- QAIP reports and performance metrics

DOMAIN 2 — GOVERNANCE AND MANAGEMENT OF IT

Chapter 1: IT Governance Framework

1.1 Definition and Purpose of IT Governance

- IT Governance ensures alignment between IT strategy and enterprise goals, optimizing value creation and risk management.
- It involves decision-making structures, accountability mechanisms, and performance measurement to ensure IT supports business objectives.

1.2 Key IT Governance Frameworks

1. **COBIT (Control Objectives for Information and Related Technologies)**
   - Developed by ISACA.
   - Focuses on five principles:
     1. Meeting stakeholder needs.
     2. Covering the enterprise end-to-end.
     3. Applying a single, integrated framework.
     4. Enabling a holistic approach.
     5. Separating governance from management.
   - **Governance objectives**: Evaluate, Direct, Monitor (EDM).
   - **Management objectives**: Plan, Build, Run, Monitor (PBRM).
2. **ITIL (Information Technology Infrastructure Library)**
   - Framework for IT Service Management (ITSM) focusing on service lifecycle (Service Strategy → Design → Transition → Operation → Continual Improvement).
   - Emphasizes **customer satisfaction** and **service quality**.
3. **ISO/IEC 38500:2015**
   - Provides **principles for directors** on the effective, efficient, and acceptable use of IT within organizations.
   - Principles: Responsibility, Strategy, Acquisition, Performance, Conformance, Human Behavior.
4. **COSO (Committee of Sponsoring Organizations)**
   - Broader enterprise risk management (ERM) and internal control framework.

    - Five components: Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring Activities.

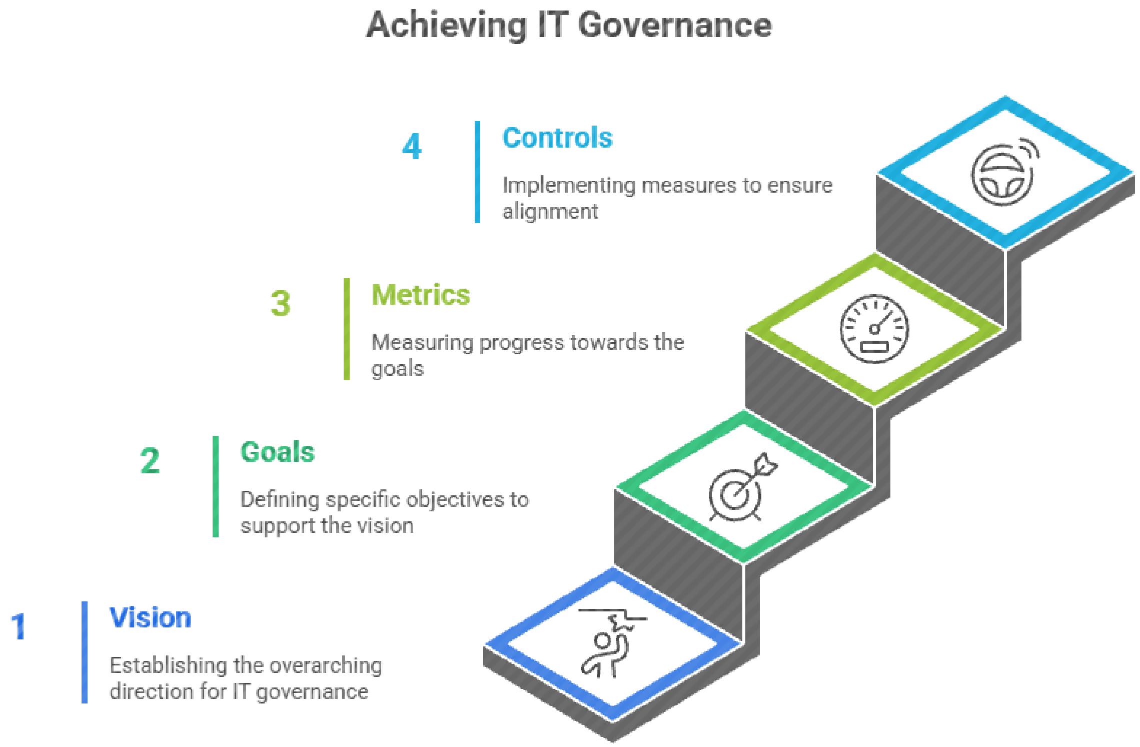
5. **Val IT** (Value from IT Investments)
    - Extends COBIT to focus on realizing business value from IT-enabled investments.
    - Framework for portfolio management, investment management, and value governance.

1.3 Components of an IT Governance Framework

- **Strategic alignment** — Ensures IT initiatives support business strategies.
- **Value delivery** — Ensures IT investments deliver promised benefits.
- **Risk management** — Identifies and manages IT-related business risks.
- **Resource management** — Optimizes IT assets, infrastructure, and human capital.
- **Performance measurement** — Uses KPIs and balanced scorecards to measure efficiency and effectiveness.

1.4 IT Governance Structures

- **IT Steering Committee** — Aligns IT projects with business goals.
- **Risk Committee** — Oversees IT risk management and compliance.
- **Architecture Review Board** — Approves IT designs and standards.
- **Data Governance Board** — Oversees data quality, privacy, and usage compliance.



Achieving IT Governance

4 Controls

Implementing measures to ensure alignment

3 Metrics

Measuring progress towards the goals

2 Goals

Defining specific objectives to support the vision

1 Vision

Establishing the overarching direction for IT governance

Chapter 2: Strategic Planning and Alignment

2.1 IT Strategic Planning

- IT strategy defines long-term technology direction in alignment with corporate goals.
- It identifies priorities, budgets, timelines, and resource requirements.
- The IS auditor evaluates if:
  - IT strategy supports business strategy.
  - Planning involves business stakeholders.
  - Metrics are defined to measure strategic outcomes.

2.2 Strategic Planning Process

1. **Understand Business Objectives** — Identify mission, vision, and goals.
2. **Assess Current IT Capabilities** — Evaluate existing systems, resources, and competencies.
3. **Identify Gaps and Opportunities** — Analyze where IT can add value or where deficiencies exist.

4. **Develop Strategic Initiatives** — Define key IT programs and projects.
5. **Create Implementation Roadmap** — Define timelines, resource allocations, and governance.
6. **Monitor and Review** — Regularly review alignment with changing business conditions.

2.3 Tools for Strategic Alignment

- **Balanced Scorecard (BSC)** — Converts strategy into performance metrics across financial, customer, internal, and innovation perspectives.
- **Portfolio Management** — Ensures the right mix of IT projects aligned with business priorities.
- **Enterprise Architecture (EA)** — Provides a holistic view of business processes, data, applications, and technology.

2.4 IS Auditor's Role

- Verify IT strategy is documented, approved, and communicated.
- Review if IT investments are prioritized based on business benefits.
- Ensure change in business strategy triggers review of IT strategy.
- Assess key performance indicators (KPIs) for tracking IT performance.

Chapter 3: IT Policies, Standards, and Procedures

3.1 Hierarchy of IT Governance Documentation

1. **Policies** — High-level principles defining management intent (e.g., "All systems must enforce MFA").
2. **Standards** — Specific, mandatory rules to implement policies (e.g., "Minimum 12-character password length").
3. **Procedures** — Step-by-step instructions for operational execution.
4. **Guidelines** — Recommended best practices or non-mandatory suggestions.

3.2 Importance of Policies and Standards

- Ensure consistency, compliance, and control in IT operations.
- Facilitate auditing, risk mitigation, and governance transparency.
- Serve as a foundation for accountability.

3.3 Policy Development Process

1. Identify business and regulatory requirements.
2. Draft and review policies with stakeholders.
3. Obtain management approval.
4. Communicate and implement organization-wide.
5. Periodically review and update policies.

3.4 Key Policy Areas

- **Information Security Policy** — Defines objectives for confidentiality, integrity, and availability.
- **Acceptable Use Policy (AUP)** — Specifies user responsibilities and prohibited activities.
- **Data Classification Policy** — Defines data sensitivity levels and handling requirements.
- **Access Control Policy** — Specifies rules for identity management and access rights.
- **Change Management Policy** — Controls modifications to IT systems.
- **Incident Response Policy** — Guides detection, response, and escalation procedures.

3.5 IS Auditor's Perspective

- Verify policies are aligned with laws, regulations, and standards.
- Confirm version control and approval documentation exist.
- Ensure staff are aware of and trained on key IT policies.
- Review policy enforcement mechanisms and exception handling.

Chapter 4: IT Risk Management

4.1 IT Risk Management Overview

- IT risk management is the **systematic process** of identifying, assessing, and mitigating risks to information assets to ensure that IT supports business objectives.

- It integrates **risk identification**, **risk analysis**, **response**, and **monitoring** into the overall enterprise risk management (ERM) process.

4.2 Key Components of IT Risk Management

1. **Risk Identification**
   - Recognize threats, vulnerabilities, and potential impacts.
   - Sources of risk: internal (human error, system failure) and external (cyberattacks, natural disasters).
   - Risk register is developed and maintained.
2. **Risk Assessment and Analysis**
   - **Qualitative Assessment:** Based on expert judgment, using scales like High/Medium/Low.
   - **Quantitative Assessment:** Uses numerical values (Annual Loss Expectancy = SLE × ARO).
   - **Hybrid Approach:** Combination of both.
3. **Risk Response / Treatment Options**
   - **Avoidance:** Eliminate the activity causing the risk.
   - **Mitigation:** Implement controls to reduce likelihood or impact.
   - **Transfer:** Shift risk to third parties (e.g., insurance, outsourcing).
   - **Acceptance:** Acknowledge and tolerate the residual risk.
4. **Risk Monitoring and Review**
   - Continuous tracking of risk indicators and control effectiveness.
   - Regular updates to the risk register and reporting to senior management.
   - Use of **Key Risk Indicators (KRIs)** and dashboards.

4.3 Risk Management Frameworks

- **ISO/IEC 27005:** Provides structured guidance for information security risk management.
- **NIST SP 800-30:** Detailed steps for risk assessment.

- **COSO ERM:** Enterprise-level risk governance model integrating IT risk.
- **FAIR Model (Factor Analysis of Information Risk):** Quantifies cyber risk in financial terms.

4.4 IS Auditor's Role

- Verify a documented risk management process exists.
- Assess adequacy of risk identification and analysis techniques.
- Ensure risk appetite and tolerance are clearly defined by management.
- Review risk treatment plans, monitoring mechanisms, and reporting structures.
- Confirm that residual risks are accepted at the appropriate level of authority.

Chapter 5: Resource Management

5.1 Overview

- IT resource management ensures efficient and effective use of organizational IT assets, including people, infrastructure, applications, and data.
- Aligns IT resource planning and allocation with strategic objectives.

5.2 Key IT Resources

1. **Human Resources (HR):** Skills, roles, and responsibilities of IT personnel.
2. **Information Resources:** Data and knowledge assets.
3. **Infrastructure Resources:** Hardware, networks, facilities.
4. **Application Resources:** Software systems supporting business processes.
5. **Financial Resources:** Budget allocations and cost optimization.

5.3 Human Resource Management in IT

- **Staffing:** Ensures qualified personnel for IT operations.
- **Training and Development:** Continuous upskilling in emerging technologies and compliance.

- **Succession Planning:** Minimizes risk of key person dependency.
- **Separation of Duties (SoD):** Prevents conflict of interest and fraud.
- **Job Rotation and Mandatory Vacations:** Helps detect irregularities and improve oversight.

Auditor's Focus:

- Review job descriptions and role-based access assignments.
- Verify training programs exist for IT and security staff.
- Evaluate employee background checks and termination procedures.

5.4 IT Resource Optimization

- **Capacity Planning:** Ensure IT infrastructure meets demand efficiently.
- **Asset Management:** Track lifecycle of hardware, software, and licenses.
- **Outsourcing and Vendor Management:** Define SLAs, monitor compliance, and ensure risk controls.
- **Cloud Resource Management:** Ensure governance over usage, cost, and security under shared-responsibility models.

5.5 Financial Resource Management

- Evaluate cost-effectiveness of IT operations.
- Use Chargeback Models to distribute IT costs transparently.
- Apply Total Cost of Ownership (TCO) and Return on Investment (ROI) metrics for IT spending decisions.

5.6 IS Auditor's Role

- Ensure resource allocation aligns with organizational priorities.
- Review vendor and outsourcing governance controls.
- Evaluate HR policies for competency, integrity, and accountability.
- Confirm IT budgeting and spending are properly approved and tracked.

Chapter 6: Performance Monitoring and Reporting

6.1 Purpose

- Performance monitoring ensures IT services deliver value, reliability, and efficiency consistent with business goals.
- Establishes mechanisms to measure, monitor, and report IT performance metrics.

6.2 Key Performance Frameworks

1. **COBIT Performance Management (CPM):**
    - Uses maturity and capability levels to assess IT governance effectiveness.
    - Levels: 0 (Incomplete) → 5 (Optimizing).
2. **Balanced Scorecard (BSC):**
    - Translates strategy into measurable objectives across four perspectives: Financial, Customer, Internal Process, Learning & Growth.
3. **Key Performance Indicators (KPIs):**
    - Metrics that show achievement of IT goals. Example: % of projects delivered on time, system uptime.
4. **Key Goal Indicators (KGIs):**
    - High-level measures of goal achievement. Example: Reduction in incident response time.
5. **Critical Success Factors (CSFs):**
    - Essential conditions required for achieving objectives. Example: Executive support for IT governance.

6.3 IT Performance Metrics

- **Operational Metrics:** Availability, incident rates, response times.
- **Financial Metrics:** ROI, cost per transaction, cost savings.
- **Security Metrics:** Number of vulnerabilities, patch compliance percentage.
- **Compliance Metrics:** Audit findings closed, control maturity scores.

6.4 Monitoring Tools and Techniques

- **Dashboards:** Visualize KPIs and trends for decision-makers.
- **Service Level Agreements (SLAs):** Define expected performance between IT and business.
- **Continuous Monitoring Systems:** Use SIEM, NOC/SOC dashboards, and automated alerts.
- **Benchmarking:** Compare IT performance with industry standards.

6.5 IS Auditor’s Role

- Verify performance metrics are aligned with strategic and operational objectives.
- Assess the accuracy, completeness, and timeliness of performance reports.
- Ensure corrective actions are implemented for underperformance.
- Confirm regular review of KPIs and alignment with changing business goals.

DOMAIN 3 — INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND IMPLEMENTATION

When projects skip governance chaos takes over.
With governance and SDLC — order, quality, and confidence
Who approved this feature?
NO DOCUM-NTATION!
W10
NES
We're right on schedule — thanks to SDLC controls!
SDLC
☑ PLANNING
☑ DESIGN
☑ DEVELOPMENT
☑ TESTING
☑ DEPLOYMENT

Chapter 1: Business Case and Feasibility Analysis

1.1 Overview

- The business case provides justification for initiating an information system or project by evaluating expected benefits, costs, and risks.
- The IS auditor evaluates whether the business case is complete, realistic, and aligned with organizational objectives.

1.2 Business Case Components

1. **Business Need Identification**
   - Defines the problem or opportunity the project aims to address.
   - Includes current system deficiencies or new capabilities required.
   - Should align with the organization's strategic goals and IT roadmap.
2. **Cost–Benefit Analysis**
   - Identifies and quantifies expected benefits and costs.
   - **Types of benefits:**

        - *Tangible:* Reduced processing time, lower maintenance costs, increased revenue.
        - *Intangible:* Improved decision-making, customer satisfaction, employee morale.
    - **Methods:**
        - *Net Present Value (NPV)*, *Internal Rate of Return (IRR)*, *Payback Period*.

3. **Risk Assessment**
    - Identifies project and operational risks (technical, schedule, cost, compliance).
    - Includes risk mitigation and contingency plans.
4. **Impact Assessment**
    - Examines organizational, technical, and operational impacts.
    - Considers resource needs, training, process changes, and data migration.
5. **Feasibility Study**
    - Evaluates project viability across multiple dimensions:
        - **Technical feasibility:** Availability of technology and expertise.
        - **Operational feasibility:** Compatibility with existing processes and readiness for adoption.
        - **Economic feasibility:** Financial viability.
        - **Legal/Regulatory feasibility:** Compliance with laws and standards.
        - **Schedule feasibility:** Reasonable timelines and deliverables.

1.3 IS Auditor’s Role

- Verify that the business case is formally documented and approved by management.
- Ensure cost–benefit analysis includes all significant costs (including maintenance and support).
- Confirm feasibility analysis covers all critical aspects and assumptions are realistic.

- Check that risk mitigation strategies are identified and aligned with risk appetite.
- Review post-implementation benefits tracking mechanisms.

Chapter 2: Project Governance and Management

2.1 Overview

- IT project governance provides oversight and accountability to ensure that projects align with business objectives, deliver expected value, and manage risks effectively.
- The IS auditor focuses on whether project governance structures and practices ensure control, transparency, and compliance.

2.2 Project Governance Framework

1. **Project Governance Objectives**
   - Ensure strategic alignment with business goals.
   - Provide stakeholder accountability.
   - Maintain effective risk, issue, and change control.
   - Support informed decision-making and performance tracking.
2. **Governance Bodies**
   - **Project Steering Committee:** Provides strategic direction, approves budgets, and monitors progress.
   - **Project Management Office (PMO):** Defines standards, templates, and performance metrics for project management.
   - **Project Sponsor:** Provides executive-level support and resources.
   - **Project Manager:** Responsible for day-to-day project execution.

2.3 Project Management Process Groups

Aligned with **PMBOK (Project Management Body of Knowledge)**:

1. **Initiation**

   - Define project objectives, scope, and stakeholders.
   - Approve the project charter.
2. **Planning**
   - Develop project management plans (scope, schedule, cost, quality, risk, communication, procurement).
3. **Execution**
   - Coordinate people and resources to perform planned activities.
4. **Monitoring and Controlling**
   - Track performance, manage risks, and control scope or schedule changes.
5. **Closure**
   - Verify deliverables, document lessons learned, and formally close the project.

2.4 Project Management Controls

- **Scope Management:** Prevent scope creep by formal change control procedures.
- **Schedule Management:** Use milestones and critical path methods to track progress.
- **Cost Management:** Apply earned value management (EVM) to compare planned vs. actual performance.
- **Risk Management:** Identify, analyze, and monitor project risks.
- **Quality Management:** Ensure deliverables meet defined acceptance criteria.

2.5 Project Documentation

- **Project Charter:** High-level authorization and objective statement.
- **Project Plan:** Defines scope, timelines, resources, and deliverables.
- **Risk Register:** Tracks identified risks and mitigation actions.
- **Issue Log:** Records and monitors project issues and resolutions.
- **Change Log:** Documents approved or rejected changes.

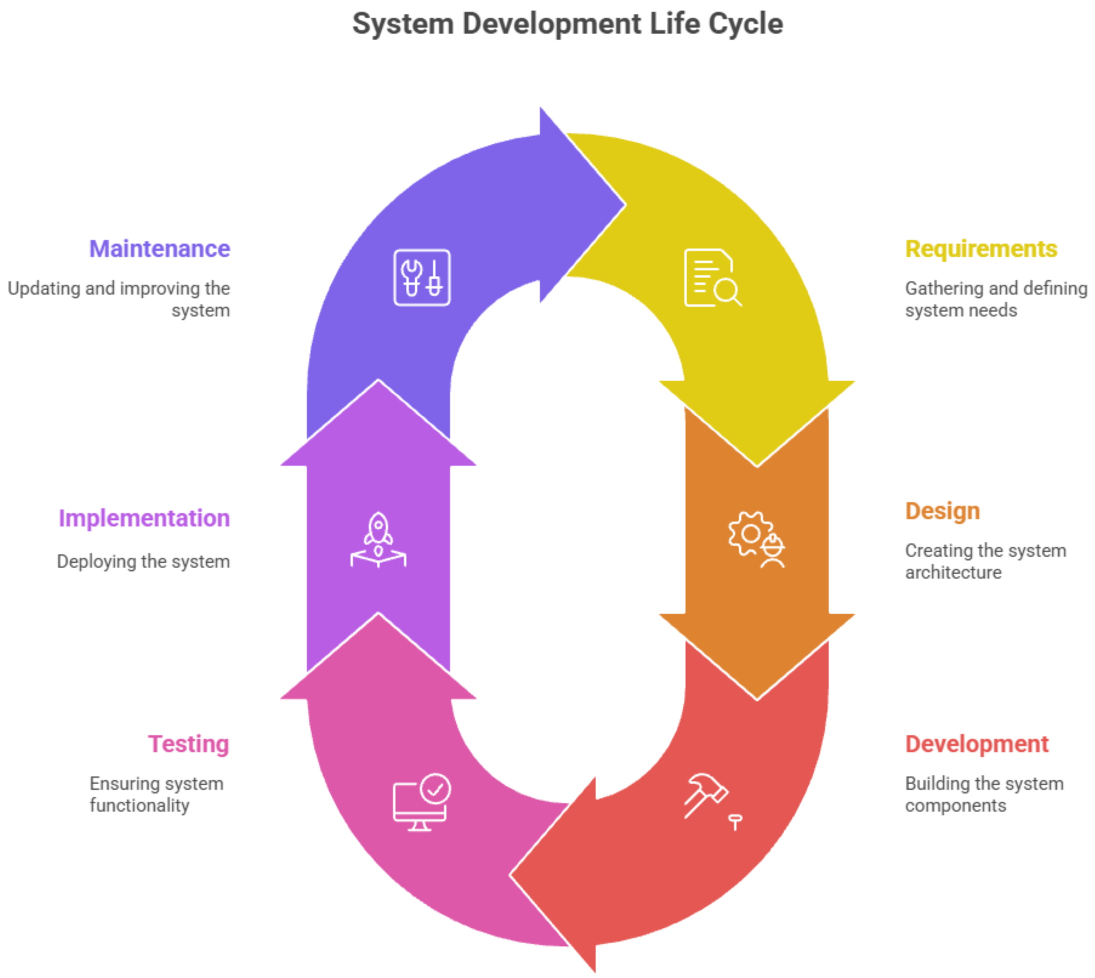
2.6 IS Auditor’s Role

- Confirm existence of a formal governance structure and clear accountability.
- Evaluate if project roles and responsibilities are defined and approved.
- Review the adequacy of project management methodologies (e.g., Agile, Waterfall).
- Assess whether risks, issues, and changes are managed and reported appropriately.
- Verify that project closure includes lessons learned and benefit realization reviews.

Chapter 3: System Development Methodologies

3.1 Overview

- System Development Life Cycle (SDLC) defines structured phases for developing and maintaining information systems.
- The IS auditor ensures that appropriate controls are embedded throughout the SDLC to ensure quality, security, and compliance.


System Development Life Cycle
Maintenance
Updating and improving the system
Requirements
Gathering and defining system needs
Implementation
Deploying the system
Design
Creating the system architecture
Testing
Ensuring system functionality
Development
Building the system components

3.2 SDLC Phases

1. **Initiation and Feasibility**
   - Identify business needs and feasibility (technical, financial, operational).
2. **System Design**
   - Define system architecture, components, inputs, outputs, and interfaces.
3. **Development**
   - Code and configure system components.
4. **Testing**
   - Verify functionality, performance, and security.
5. **Implementation**
   - Deploy the system and migrate data.
6. **Maintenance**

    - Perform ongoing updates, patches, and user support.

7. **Disposal**
    - Decommission system securely when retired.

3.3 Development Methodologies

1. **Waterfall Model**
    - Sequential phases; rigid and document-driven.
    - Strengths: Clarity, defined deliverables, simple tracking.
    - Weaknesses: Limited flexibility and high cost of changes.
2. **Agile Development**
    - Iterative and incremental approach.
    - Uses sprints, scrum teams, and continuous feedback.
    - Benefits: Rapid delivery, adaptability, customer involvement.
    - Risks: Scope volatility, dependency on skilled teams.
3. **DevOps and DevSecOps**
    - Integrates development, operations, and security.
    - Automates deployment and testing for continuous delivery.
    - Focus: Collaboration, automation, and resilience.
4. **Prototyping**
    - Builds quick models for feedback before final development.
    - Risk: User expectations may not align with final product.
5. **Rapid Application Development (RAD)**
    - Focuses on speed using reusable components and iterative design.
    - Risk: Limited scalability for large, complex systems.
6. **Spiral Model**
    - Combines iterative development with systematic risk analysis at each iteration.

3.4 Controls in System Development

- **Segregation of Duties:** Developers should not promote code directly to production.
- **Change Management:** All modifications must follow formal approval and testing.
- **Code Review:** Peer or automated review ensures adherence to standards.
- **Configuration Management:** Maintains version control and integrity.
- **Security Integration:** Security requirements embedded early (shift-left security).

3.5 IS Auditor’s Role

- Ensure an approved SDLC methodology exists and is consistently followed.
- Review project documentation at each SDLC phase for completeness and accuracy.
- Evaluate adequacy of testing and QA controls before deployment.
- Confirm segregation of duties and change management are enforced.
- Assess post-implementation review to verify benefit realization and control adequacy.

Chapter 4: Control Design, Development, and Testing

4.1 Overview

This phase ensures that the controls within the system—whether automated or manual—are designed, developed, and tested effectively before implementation.
An IS auditor’s primary goal here is to ensure that control objectives are met and system integrity is not compromised.

4.2 Control Objectives in Systems Development

Each control serves one or more of the following objectives:

1. **Confidentiality:** Protection of sensitive data from unauthorized access.
2. **Integrity:** Ensuring data accuracy, completeness, and consistency.

3. **Availability:** Ensuring systems are reliable and accessible when needed.
4. **Accountability:** Ensuring actions can be traced to responsible individuals.
5. **Auditability:** Ensuring that sufficient logs and records are available for review.

4.3 Types of Controls

Control Type	Description	Example
Preventive	Avoid occurrence of errors or irregularities	Access control, input validation
Detective	Identify errors or unauthorized activities	Log monitoring, reconciliation
Corrective	Rectify issues once detected	Patch management, rollback procedures
Compensating	Alternate controls used when primary ones are missing	Supervisory review in place of segregation of duties

4.4 Control Design Considerations

- Controls must be integrated early in the system design phase (shift-left approach).
- The principle of least privilege should be applied to all users and applications.
- Ensure segregation of duties (SoD):
  - Developers ≠ Testers ≠ Production operators.
- Ensure input, processing, and output controls are adequate:
  - **Input Controls:** Data validation, edit checks, control totals.
  - **Processing Controls:** Run-to-run totals, sequence checks, error handling.
  - **Output Controls:** Distribution lists, access restrictions, reconciliation reports.

4.5 Testing Controls

1. **Unit Testing**

  - Performed by developers to test individual modules or components.
  - Ensures logic and functions work as intended.

2. **Integration Testing**
   - Tests how modules interact and whether data flows correctly between them.
3. **System Testing**
   - Validates end-to-end system functionality and compliance with requirements.
   - Includes performance, load, and stress testing.
4. **User Acceptance Testing (UAT)**
   - Conducted by business users to verify the system meets business needs.
   - A **UAT sign-off** is required before production deployment.
5. **Regression Testing**
   - Ensures that new changes don't impact existing functionality.
6. **Security Testing**
   - Identifies vulnerabilities, misconfigurations, or weak access controls.
   - May include penetration testing and code review.

4.6 Change Management and Configuration Control

- **Change Request:** Initiated formally, evaluated for impact, and approved before execution.
- **Version Control:** Tracks all versions of code, scripts, or configurations.
- **Promotion Control:** Code should move from dev → test → production through approval gates.
- **Rollback Procedures:** Should exist in case deployment fails.

4.7 IS Auditor's Role

☑ Review whether system controls align with business and regulatory requirements.
☑ Verify control testing results and ensure UAT evidence is documented.
☑ Confirm segregation of environments (dev, test, prod).

☑ Ensure changes are authorized, tested, and logged before migration.
☑ Evaluate completeness of test plans, test results, and defect resolution reports.
☑ Assess security testing and verify vulnerabilities were mitigated before go-live.

Chapter 5: System Implementation and Post-Implementation Review

5.1 Overview

Implementation is when the system is migrated into the production environment and becomes operational.
The IS auditor ensures that all preconditions for go-live are satisfied, controls are active, and post-implementation review confirms success.

5.2 System Implementation Process

1. **Implementation Planning**
   - Define cutover strategy (big bang vs. phased rollout).
   - Prepare data migration plans and validation steps.
   - Identify rollback or contingency procedures.
2. **Data Conversion**
   - Ensure data migration is complete, accurate, and validated.
   - Reconcile pre- and post-migration totals.
   - Retain old data for audit trail if needed.
3. **Training and Communication**
   - Train end users and administrators.
   - Communicate changes to stakeholders and define new procedures.
4. **System Migration and Deployment**
   - Ensure migration scripts and tools are tested.
   - Validate system performance in production.
   - Monitor closely during initial operational period.
5. **Acceptance and Go-Live Authorization**

- Obtain sign-off from business owners and key stakeholders.
- Ensure backup and recovery procedures are established.

5.3 Post-Implementation Review (PIR)

Performed after stabilization (usually 30–90 days post-go-live) to evaluate:

1. **Achievement of Objectives**
   - Did the system meet business needs and expected benefits?
2. **Cost and Schedule Performance**
   - Were timelines and budgets met?
3. **Control Effectiveness**
   - Are implemented controls functioning as designed?
4. **Security and Compliance**
   - Any new vulnerabilities or compliance gaps introduced?
5. **User Feedback**
   - Satisfaction, usability, and performance issues.
6. **Lessons Learned**
   - For future improvements and project templates.

5.4 Common Implementation Risks

Risk	Mitigation
Incomplete data migration	Data validation and reconciliation checks
Lack of user training	Comprehensive training plan before go-live
Missing rollback plan	Documented and tested fallback strategy
Poor change control	Formal approval workflows for changes
Performance degradation	Load testing and performance tuning

5.5 IS Auditor’s Role During Implementation

- Review go-live checklist and approvals.

- Verify that migration activities were tested and signed off.
- Ensure backup, recovery, and rollback plans exist and were tested.
- Confirm UAT completion and stakeholder acceptance.
- Evaluate data migration accuracy and completeness.
- Check system security configuration (access rights, encryption, etc.).
- Assess whether all identified issues are tracked to closure.

5.6 IS Auditor's Role During Post-Implementation Review

☑ Ensure PIR was performed formally and independently.
☑ Verify achievement of business and control objectives.
☑ Review benefit realization reports vs. business case.
☑ Assess ongoing control operation effectiveness.
☑ Recommend corrective actions or control enhancements.

5.7 Key Audit Deliverables

- Implementation Review Report
- Configuration & Access Review Checklist
- Data Migration Validation Report
- Post-Implementation Review Summary
- Lessons Learned Register

Chapter 6: System Maintenance and Change Management

6.1 Overview

Once systems are in production, they require ongoing maintenance to correct defects, enhance functionality, and respond to environmental or business changes.
The IS auditor's focus is to ensure that change management controls are designed and functioning effectively to prevent unauthorized or untested changes from compromising the system.

6.2 Types of System Maintenance

1. **Corrective Maintenance**
   - Fixes defects identified during operation.
   - Example: Bug fix after users report calculation errors.
2. **Adaptive Maintenance**
   - Adjusts the system to work in a new environment.
   - Example: Software updated after OS or database upgrade.
3. **Perfective Maintenance**
   - Enhances functionality or performance to meet new business needs.
   - Example: Adding a dashboard to improve analytics reporting.
4. **Preventive Maintenance**
   - Performed to avoid potential future issues.
   - Example: Refactoring code to remove deprecated libraries or reduce technical debt.

6.3 Change Management Objectives

The objective of change management is to introduce changes in a controlled and authorized manner while maintaining system integrity, security, and availability.

Key Objectives:

- Prevent unauthorized, untested, or unapproved changes.
- Maintain system stability and integrity.
- Ensure all changes are documented and traceable.
- Facilitate rollback if change fails.
- Ensure appropriate segregation of duties.

6.4 Change Management Process

A robust change management process generally includes the following stages:

1. **Change Request Initiation**

   - Formal request documenting the nature, reason, and impact of the change.
   - Initiator: user, developer, or system administrator.
   - Logged in a Change Management System (CMS) or ticketing tool.

2. **Impact Analysis**
   - Evaluate effects on system security, operations, and data integrity.
   - Assess dependencies, performance impact, and rollback feasibility.

3. **Change Approval**
   - Reviewed by a Change Advisory Board (CAB) or Change Control Board (CCB).
   - Approval based on risk assessment, testing results, and business priority.

4. **Change Development & Testing**
   - Performed in development/test environments only.
   - Verified through regression and user acceptance testing (UAT).

5. **Change Implementation**
   - Executed during maintenance windows or low-traffic hours.
   - Accompanied by implementation checklists and backout plans.

6. **Documentation & Review**
   - Update change logs, configuration records, and system documentation.
   - Conduct post-implementation review to validate expected outcomes.

6.5 Segregation of Environments

A key security principle in change management is to maintain separation between environments:

- **Development Environment:** For building and coding.
- **Test Environment:** For verification and quality assurance.
- **Production Environment:** For live business operations.

Developers should not have access to production data or the ability to deploy code directly into production without review and approval.

6.6 Configuration Management

Configuration management ensures that system components (software, hardware, network, and documentation) are identified, recorded, and tracked through their lifecycle.

Key Components:

- **Configuration Item (CI):** Any system component (file, program, device, etc.) managed under change control.
- **Configuration Management Database (CMDB):** Repository that stores and tracks all CIs and their relationships.
- **Baseline Configuration:** Officially approved version of a system, used as a reference for future comparisons.

6.7 Emergency Change Management

Some changes are urgent, such as those required to fix critical production incidents or vulnerabilities.

Controls for emergency changes:

- Documented emergency procedure.
- Post-implementation review required.
- Approval may be retrospective (after implementation).
- Limited personnel authorized to execute emergency changes.

6.8 IS Auditor’s Role in Change Management

- Verify formal change request and approval workflows exist.
- Ensure segregation of duties between developers, testers, and deployers.
- Review testing evidence, rollback procedures, and documentation updates.
- Confirm emergency changes are tracked, reviewed, and approved retrospectively.
- Evaluate completeness of configuration management records (CMDB accuracy).
- Ensure audit trails exist for all changes.

Chapter 7: Auditing the System Development Life Cycle (SDLC)

7.1 Overview

Auditing the SDLC ensures that systems are developed, implemented, and maintained according to organizational standards and control requirements.
The IS auditor evaluates whether security, quality, and business requirements are properly addressed across each phase of the SDLC.

7.2 SDLC Audit Objectives

1. Assess whether the development process aligns with organizational policies and procedures.
2. Verify that controls are integrated into each phase.
3. Ensure proper documentation, testing, and approvals exist.
4. Evaluate effectiveness of project governance and quality assurance.
5. Confirm post-implementation reviews and lessons learned are conducted.

7.3 Audit Approach

A. Risk-Based Auditing

- Focus on high-risk systems or modules.
- Evaluate risk management at each SDLC phase.

B. Phased Auditing Approach

- Conduct audits progressively across phases (planning, design, development, etc.).
- Verify completeness and quality before proceeding to next phase.

C. Controls Testing

- Review evidence that controls operate effectively.
- Re-perform sample control activities where applicable.

7.4 Audit Scope

Typical SDLC audit scope includes:

- Project management and governance.
- Requirement and design documentation.
- Control and security specifications.
- Testing and quality assurance evidence.
- Change and configuration management records.
- Post-implementation results.

7.5 SDLC Audit Techniques

Technique	Purpose
Review of Documentation	Verify existence and completeness of records (plans, policies, logs).
Interviews and Walkthroughs	Understand process flow and control implementation.
Observation	Witness testing or deployment activities.
Reperformance	Independently test control operations or data validation.
Data Analysis	Analyze system logs, change records, and test results.

7.6 Common SDLC Audit Findings

Area	Typical Issue	Risk
Project Governance	Missing approvals, unclear roles	Project failure, control gaps
Requirements	Lack of business/user validation	System misalignment
Design	No threat modeling, weak architecture	Security vulnerabilities

Testing	Incomplete or unverified test results	Undetected defects in production
Change Management	Unapproved code deployments	Unauthorized changes
Post-Implementation	No benefit realization review	Ineffective outcomes

7.7 Key IS Auditor Responsibilities

- Verify SDLC methodology is defined, approved, and consistently applied.
- Confirm project governance ensures accountability and segregation.
- Review whether security and control requirements were addressed early in design.
- Evaluate adequacy of test plans and testing outcomes.
- Assess the change management process post-deployment.
- Review documentation completeness and version control.
- Issue findings and recommend improvements in SDLC process controls.

7.8 Reporting and Follow-Up

- Prepare an audit report summarizing findings, risks, and recommendations.
- Classify findings by severity and business impact.
- Follow up to verify implementation of corrective actions.
- Evaluate maturity level of SDLC processes for continuous improvement.

☑ Domain 3 — Key Takeaway Summary

Focus Area	Auditor’s Objective
Project Governance	Ensure accountability and oversight
Control Design & Testing	Confirm integration of preventive and detective controls

Change & Configuration Management	Maintain system integrity and traceability
SDLC Auditing	Verify adherence to policies, documentation, and security controls
Post-Implementation Review	Evaluate benefits, effectiveness, and lessons learned

DOMAIN 4 — INFORMATION SYSTEMS OPERATIONS AND BUSINESS RESILIENCE

This domain assesses the auditor's ability to evaluate the effectiveness, efficiency, and reliability of IT operations, and the organization's ability to ensure continuity and resilience in the face of disruptions.

Chapter 1: IT Operations Management and Control Framework

1.1 Objectives of IT Operations

IT operations provide the essential support for daily business processes. The main objectives include:

- **Service Delivery:** Ensure consistent, reliable IT services.
- **Operational Efficiency:** Optimize resource utilization.
- **Security and Compliance:** Protect information and ensure regulatory adherence.
- **Change Enablement:** Facilitate controlled technology change without business disruption.
- **Performance Measurement:** Monitor and improve service levels through KPIs and SLAs.

1.2 IT Operations Management Structure

Operations are generally structured under an IT Operations Manager who oversees:

- **Data Center / Infrastructure Teams** – servers, storage, backup.
- **Network Operations** – connectivity, bandwidth, security.
- **Application Support Teams** – business system maintenance.
- **Help Desk / Service Desk** – user support and incident logging.
- **Job Scheduling / Batch Operations** – automation of routine processes.

Effective IT operations depend on defined responsibilities, segregation of duties, and well-documented processes.

1.3 Control Frameworks in Operations

IT operations must align with control frameworks that ensure reliability and compliance:

- **COBIT 2019:** Provides a governance structure for managing IT processes and resources.
- **ITIL v4:** Defines best practices for service delivery and operational management.
- **ISO/IEC 20000:** Standard for IT Service Management (ITSM).
- **ISO 27001:** Focus on operational security and continuous improvement.
- **NIST SP 800-53:** Provides technical control baselines for federal systems.

IS auditors should ensure operations adopt appropriate frameworks and conduct **periodic self-assessments**.

1.4 Operations Policies and Procedures

Key operational policies:

- **Job Scheduling:** Timely execution of batch processes.
- **Incident and Problem Management:** Defined reporting and resolution.
- **Backup and Restore:** Regular, tested backups with off-site retention.
- **Capacity and Performance Monitoring:** Track utilization and forecast demand.
- **System Maintenance and Patch Management:** Regular updates under change control.

Documentation should be current, accessible, and approved by management.

1.5 Key Controls in Operations Management

Area	Control Focus
Access Controls	Restrict operator access to authorized systems only
Monitoring & Logging	Track operations activities and anomalies
Job Control	Enforce sequencing, verification, and completion tracking
Data Integrity	Ensure validation and reconciliation of processed data
Separation of Duties	Prevent conflicts between development and operations
Third-Party Management	Assess service providers' operational controls

1.6 Auditor's Review

An IS auditor should:

- Assess the adequacy of documented operational policies.
- Review SLAs and OLAs to confirm measurable performance.
- Evaluate incident trends and problem resolution timeliness.

- Confirm periodic reconciliation and validation controls.
- Test access rights and operator privileges.
- Verify evidence of continuous service improvement reviews.

Chapter 2: Job Scheduling, Processing, and Data Management Controls

2.1 Job Scheduling

Batch processing remains critical in mainframe and enterprise environments.

- **Scheduling Tools:** AutoSys, Control-M, IBM Tivoli Workload Scheduler.
- **Controls:**
  - Jobs must run under least-privilege credentials.
  - Dependencies and sequences are predefined.
  - Jobs automatically logged; exceptions flagged.
  - Changes follow formal change management.

Auditor Focus: Verify automated job scheduling and monitoring prevent omissions, duplications, or unauthorized executions.

2.2 Input Controls

Input controls ensure only accurate, complete, and authorized data enters systems.

- **Authorization Checks**
- **Data Validation Rules** (format, range, completeness)
- **Batch Totals / Hash Totals**
- **Exception Reports** for anomalies
- **Logging and Error Handling**

Audit Testing:

- Trace sample inputs through processing.
- Compare source documentation to input logs.
- Validate existence of error handling procedures.

2.3 Processing Controls

These ensure data integrity during transformation.

- **Run-to-Run Totals** – detect record loss or duplication.
- **Audit Trails** – enable traceability.
- **Exception Handling** – capture and correct abnormal conditions.
- **Reconciliation Procedures** – verify internal consistency between input, processing, and output.

Auditor Focus: Confirm processing logic enforces integrity, and that all exceptions are logged, investigated, and closed.

2.4 Output Controls

Output controls maintain confidentiality and accuracy of distributed results.

- **Distribution Lists:** Ensure only authorized recipients.
- **Output Reconciliation:** Validate totals, checksums, or control numbers.
- **Sensitive Report Handling:** Encryption, shredding, or access logs.
- **Archival Controls:** Retain output as per retention policy.

Audit Testing:

- Review sample output logs and user acknowledgment.
- Verify automated reconciliation and output delivery security.

2.5 Data Management Controls

Include activities ensuring data consistency, accuracy, and security throughout its lifecycle.

- **Data Classification:** Determines handling sensitivity.
- **Data Retention and Disposal:** Aligned to legal/regulatory requirements.
- **Database Maintenance:** Indexing, optimization, and access monitoring.
- **Data Reconciliation:** Between subsystems and general ledger.

Auditor Focus:

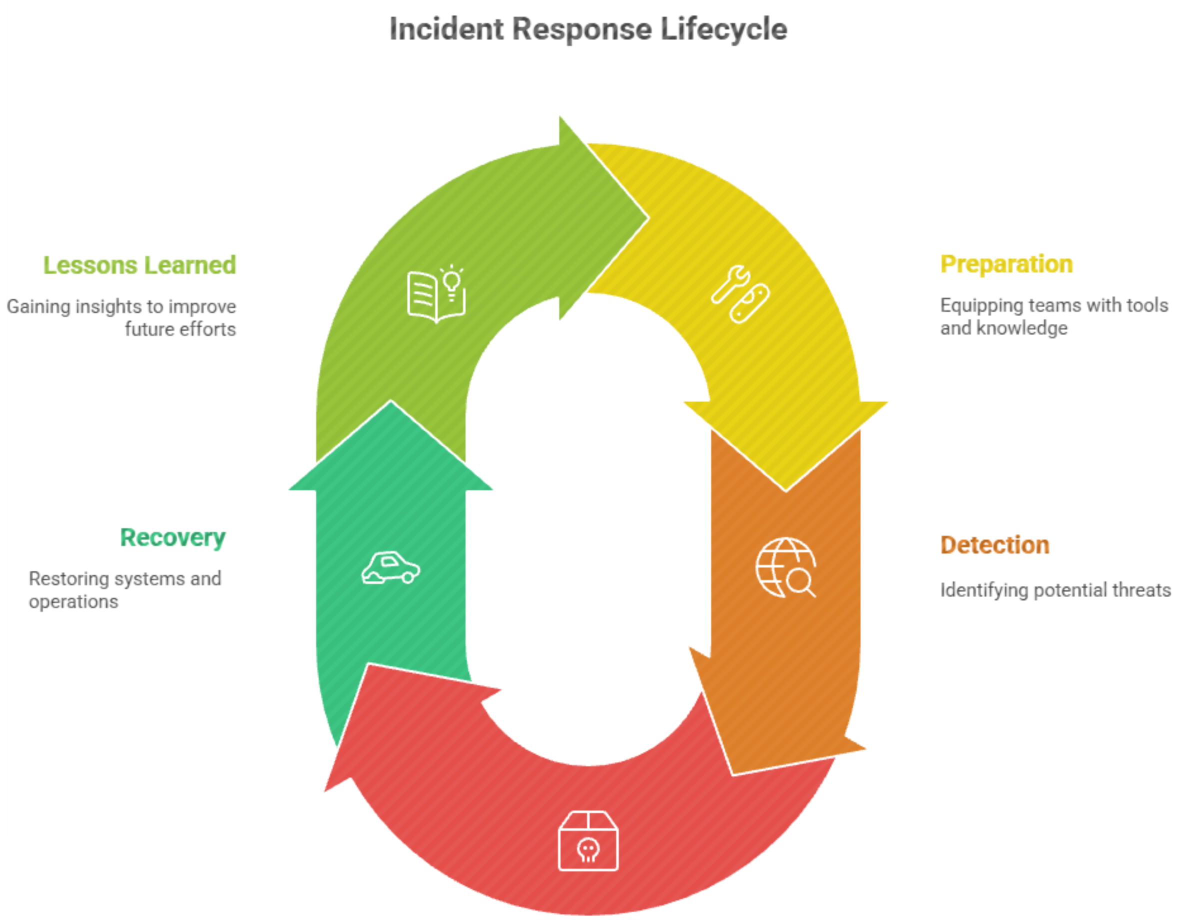
- Confirm backup and archival processes align with retention schedules.
- Verify use of encryption for confidential data at rest and in transit.

Chapter 3: Problem and Incident Management

3.1 Problem vs Incident

Term	Definition
Incident	An unplanned interruption or degradation in service.
Problem	The underlying cause of one or more incidents.

Incidents require quick resolution; problems require root-cause analysis and long-term correction.


Incident Response Lifecycle
Lessons Learned
Gaining insights to improve future efforts
Preparation
Equipping teams with tools and knowledge
Recovery
Restoring systems and operations
Detection
Identifying potential threats

3.2 Incident Management Objectives

- Restore normal service operations as quickly as possible.
- Minimize business impact and service downtime.
- Maintain incident records for trend analysis.
- Ensure escalation to higher tiers when required.
- Provide reporting to management and users.

3.3 Incident Management Process

1. **Detection and Recording** – User reports or automated alerts.
2. **Classification and Prioritization** – Based on impact and urgency.
3. **Investigation and Diagnosis** – Identify probable cause.
4. **Resolution and Recovery** – Apply fix or workaround.
5. **Closure** – Verify resolution with the user.
6. **Post-Incident Review** – Identify lessons learned.

Auditor Focus:

- Verify incidents are logged, categorized, and tracked.
- Check escalation procedures and response times.
- Review post-incident reports and SLA compliance.

3.4 Problem Management Process

- **Problem Detection:** From recurring incidents, trend analysis, or monitoring tools.
- **Root Cause Analysis (RCA):** Using methods such as 5 Whys, Ishikawa diagram.
- **Workaround Identification:** Temporary fix until permanent solution deployed.
- **Known Error Database (KEDB):** Repository for previously analyzed problems.
- **Problem Resolution:** Permanent fix implemented under change management.

Auditor Focus:

- Verify problems are prioritized based on business impact.

- Confirm RCA documentation exists for major incidents.
- Assess trend analysis frequency and management reporting.

3.5 Integration with Change and Configuration Management

- Problems often lead to change requests; ensure linkage between problem tickets and change records.
- Configuration management database (CMDB) must reflect updated CIs after resolution.
- Ensure all emergency changes follow retrospective approval.

3.6 Metrics and Reporting

Typical metrics:

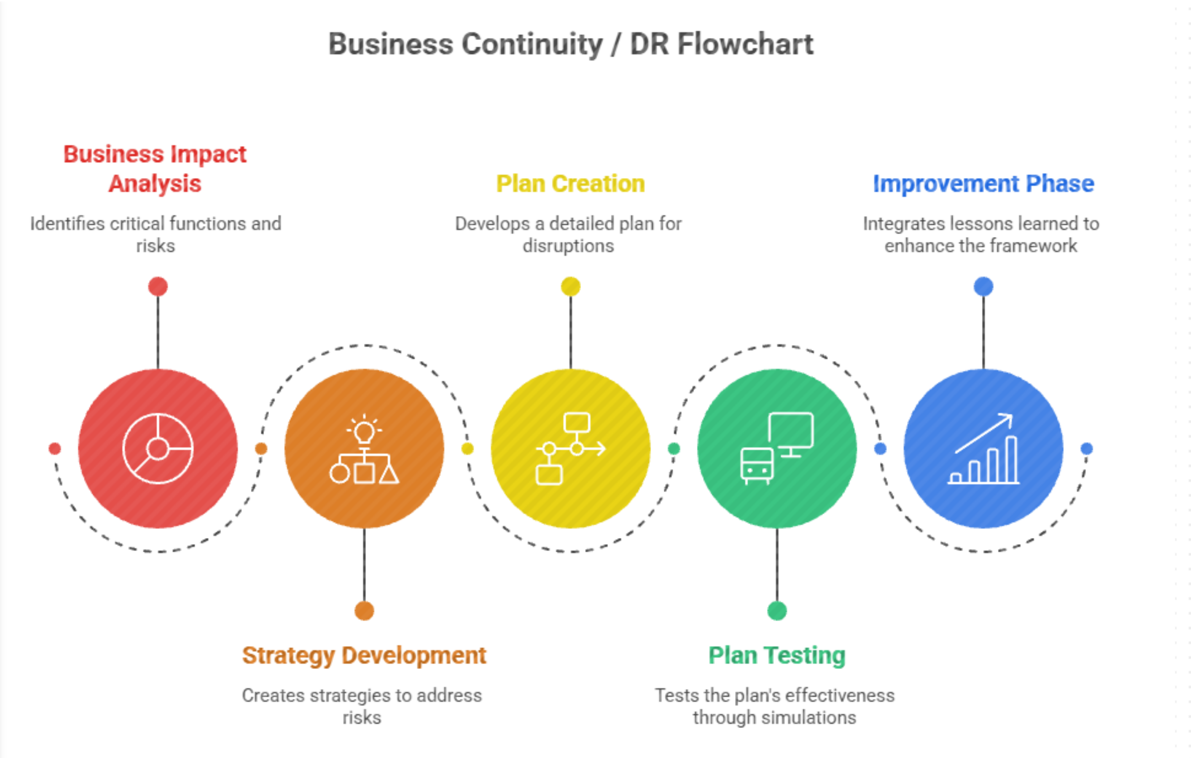
- Mean Time to Detect (MTTD)
- Mean Time to Resolve (MTTR)
- First Contact Resolution Rate
- Incident Recurrence Rate

Auditors review metrics for performance trends and improvement actions.

Chapter 4: Business Continuity and Disaster Recovery (BCP/DR)

1. Overview

Business Continuity (BC) and Disaster Recovery (DR) ensure organizational resilience by preparing for, responding to, and recovering from disruptive incidents.
Objective: To maintain essential business operations and minimize downtime during unforeseen events.
Key components: Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), and supporting processes like Business Impact Analysis (BIA) and Risk Assessment.


Business Continuity / DR Flowchart
Business Impact Analysis
Identifies critical functions and risks
Plan Creation
Develops a detailed plan for disruptions
Improvement Phase
Integrates lessons learned to enhance the framework
Strategy Development
Creates strategies to address risks
Plan Testing
Tests the plan's effectiveness through simulations

2. Business Continuity Planning (BCP) Framework

A comprehensive BCP framework includes:

1. **Governance and Policy:** Define roles, responsibilities, and authority for continuity management.
2. **Business Impact Analysis (BIA):** Identify critical business functions, dependencies, and acceptable downtime (RTO/RPO).
3. **Risk Assessment:** Evaluate threats such as natural disasters, cyberattacks, power failures, or supplier disruptions.
4. **Strategy Development:** Define recovery options—alternate sites, remote access, cloud failover, manual workarounds.
5. **Plan Development:** Document detailed response and recovery procedures for critical processes.
6. **Training and Awareness:** Ensure employees understand their roles during disruptions.
7. **Testing and Maintenance:** Conduct periodic testing, update plans post-test, and reflect organizational changes.

Audit focus: Verify that BIA and risk assessment are regularly updated and recovery strategies align with business priorities.

3. Disaster Recovery Planning (DRP)

DRP focuses on the **IT and data recovery** aspects after a disruption.
Key DRP components:

- **Data Backup Strategy:** Onsite/offsite or cloud backups with encryption and retention policies.
- **Recovery Site Options:**
  - **Hot Site:** Fully operational, minimal downtime.
  - **Warm Site:** Partially equipped, moderate downtime.
  - **Cold Site:** Basic infrastructure only, long recovery time.
- **System Restoration Procedures:** Steps to restore critical systems, applications, and connectivity.
- **Communication Plan:** Internal and external communication flow during recovery.
- **Testing:** Includes simulation, parallel, or full-interruption testing.

Audit check: Confirm recovery objectives (RTO/RPO) are documented, achievable, and tested.

4. Business Impact Analysis (BIA)

The BIA identifies and prioritizes critical business processes.
Steps:

1. Identify key business processes and dependencies.
2. Determine Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO).
3. Quantify financial and operational impact of downtime.
4. Prioritize recovery of systems based on criticality.

Audit focus: Ensure management-approved BIA results are linked to recovery strategies.

5. BCP and DRP Testing Methods

Testing validates the plan’s effectiveness and readiness.
Common methods:

- **Checklist Review:** Verify documentation completeness.
- **Tabletop Exercise:** Discuss response steps in a controlled environment.
- **Simulation Test:** Mimic actual disruption to validate coordination.
- **Parallel Test:** Run systems at alternate sites without disrupting production.
- **Full Interruption Test:** Actual failover; used rarely due to operational risk.

Audit focus: Review test frequency, scope, outcomes, and follow-up on corrective actions.

6. Roles and Responsibilities

- **BCP/DR Coordinator:** Oversees program implementation and maintenance.
- **Department Heads:** Ensure unit-level procedures are current.
- **IT Teams:** Maintain backup and recovery infrastructure.
- **Communications Officer:** Manages internal/external communication during incidents.
- **Executive Management:** Approves plans, allocates resources, and reviews test reports.

Audit verification: Confirm clear role assignments and escalation paths.

7. Continuous Improvement

- Conduct post-incident reviews to identify lessons learned.
- Update plans after changes in business processes, IT infrastructure, or regulations.
- Integrate BCP/DR with enterprise risk management (ERM) for holistic resilience.

Audit focus: Ensure continuous feedback loop exists between testing, incidents, and plan updates.

8. Auditor’s Role in BCP/DR Review

IS auditors assess whether:

- BCP/DR policies are approved and aligned with organizational strategy.

- Risk assessment and BIA are current and comprehensive.
- Recovery sites and backups meet defined RTO/RPO targets.
- Plans are tested periodically, and results are reviewed by management.
- Communication and escalation procedures are documented and functional.

9. Key Deliverables and Artifacts

Typical BCP/DR documentation includes:

- Business Continuity Policy and Charter
- BIA Report and Risk Assessment Matrix
- Continuity and Recovery Strategies Document
- BCP/DR Plan Manuals
- Test Plans and Test Reports
- Post-Test Review and Corrective Action Logs

10. Summary

Effective BCP/DR planning safeguards business continuity, protects stakeholder confidence, and ensures regulatory compliance.
IS auditors must verify that both business and IT functions are resilient, recovery strategies are tested, and lessons learned are implemented.

Chapter 5: Systems Development Life Cycle (SDLC)

1. Purpose of SDLC

The Systems Development Life Cycle (SDLC) is a structured methodology for planning, creating, testing, and deploying an information system. It ensures that business, control, and security requirements are embedded throughout the system’s life.

Key benefits:

- Improves project management and accountability.
- Enables traceability from requirements to implementation.
- Reduces risks and rework by early identification of issues.
- Promotes integration of information security.

2. Phases of SDLC

Phase	Objectives	Key Audit Focus Areas
1. Feasibility Study / Initiation	Evaluate business need, costs, risks, and technical feasibility.	Verify that business justification and ROI are documented.
2. Requirements Definition	Define functional, security, and control requirements.	Ensure traceability between user needs and requirements.
3. Design	Create system architecture, data models, and control specifications.	Validate that segregation of duties, access control, and encryption are built in.
4. Development / Configuration	Build or configure the system per design specifications.	Ensure version control, secure coding, and change tracking.
5. Testing	Validate performance, functionality, and control effectiveness.	Check test plans, results, and defect resolution.
6. Implementation / Deployment	Move system into production.	Ensure backup, rollback, and go-live approvals are complete.
7. Post-Implementation Review	Assess success, performance, and residual risks.	Review lessons learned and control effectiveness.

3. Types of SDLC Models

- **Waterfall Model:** Sequential approach; each phase must finish before the next begins.
- **V-Model:** Verification and validation-oriented; testing mapped to each development stage.
- **Agile:** Iterative model focusing on incremental delivery and adaptability.
- **DevOps:** Integration of development and operations for continuous integration and deployment (CI/CD).
- **Spiral Model:** Combines iterative development with risk analysis.

Auditor's concern: Whether controls and documentation are maintained consistently in every model.

4. Security Integration in SDLC

- **Initiation:** Include risk assessment and compliance requirements.
- **Design:** Implement security architecture and access models.
- **Development:** Follow secure coding practices and peer reviews.
- **Testing:** Perform security, penetration, and vulnerability tests.
- **Deployment:** Harden systems and monitor post-deployment configurations.

5. SDLC Audit Considerations

- Verify management approvals at each phase.
- Ensure control objectives align with risk appetite.
- Validate change and configuration management processes.
- Assess documentation completeness and traceability.

Chapter 6: Software Acquisition and Vendor Management

1. Acquisition Process Overview

Organizations may build, buy, or lease software. The acquisition process ensures the chosen option aligns with strategic, technical, and financial goals.

Phases of acquisition:

1. Requirement definition
2. Vendor evaluation
3. Contract negotiation
4. Implementation planning
5. Ongoing vendor performance monitoring

2. Software Sourcing Options

- **In-house development:** Greater control, higher cost, longer development time.

- **COTS (Commercial Off-The-Shelf):** Faster, but limited customization and vendor dependency.
- **Open Source:** Cost-effective but requires licensing compliance and security validation.
- **Outsourcing:** Transfers development responsibility to third parties; requires robust SLAs.

3. Vendor Evaluation Criteria

- Technical competence and prior experience.
- Financial stability of vendor.
- Security and compliance maturity (e.g., ISO 27001, SOC 2).
- Service level agreements (SLAs).
- Exit and continuity provisions.

Audit check: Confirm due diligence documentation and vendor risk assessment are available.

4. Contract Management

Contracts should clearly define:

- Scope of work and deliverables.
- Performance measures and penalties.
- Security requirements (data protection, breach reporting).
- Ownership of intellectual property.
- Right-to-audit clauses for IS auditors.

Auditor's role: Ensure the contract includes control responsibilities for both parties.

5. Software Licensing and Compliance

- Validate adherence to license terms to avoid legal risks.
- Periodically review installations versus purchased licenses.
- Ensure asset management systems track software versions and expirations.

6. Vendor Risk Management

- Conduct third-party risk assessments periodically.
- Maintain an updated vendor inventory with risk ratings.
- Monitor compliance with SLAs and regulatory obligations.
- Review SOC 1 / SOC 2 reports for outsourced vendors.

7. Auditing Vendor Management

IS auditors should verify:

- Existence of vendor selection procedures.
- Performance evaluation and renewal processes.
- Termination or exit strategy for transitioning services securely.

Chapter 7: Post-Implementation Review (PIR)

(Already covered above — included here for continuity)

Key areas:

- Evaluate system performance and business alignment.
- Review project cost, scope, and timeline variances.
- Assess user satisfaction, control effectiveness, and residual risk.
- Validate data integrity after migration.
- Deliver PIR report with improvement recommendations.

Domain 5 — Protection of Information Assets

Core Objective

To evaluate, implement, and manage logical, physical, and environmental security controls designed to protect information assets, ensuring confidentiality, integrity, and availability (CIA).

Chapter 1 — Information Asset Security and Control Frameworks

1.1 Purpose of Information Security

- Ensure that data and systems are protected against unauthorized access, disclosure, alteration, destruction, and unavailability.
- Aligns with organizational mission, business goals, and compliance obligations.
- Foundational principle: *CIA + Accountability + Non-repudiation + Privacy.*

1.2 Information Security Management Systems (ISMS)

- **Frameworks:** ISO/IEC 27001, NIST SP 800-53, COBIT 2019 Security Objective, ITIL Security Management.
- **Key components:**
    - Security policies, standards, and procedures
    - Risk management
    - Asset classification and ownership
    - Security organization (roles and responsibilities)
    - Continuous improvement (PDCA cycle)

1.3 Roles and Responsibilities

Role	Responsibility
Board / Executives	Approve security strategy and allocate resources
CISO / ISO	Implement and monitor the ISMS
System Owner	Define access requirements, data classification
Data Owner	Define and approve data protection levels
Custodian	Maintain and back up data
User	Comply with security policies

1.4 Security Policies and Standards

- **Policy hierarchy:** Policy → Standards → Procedures → Guidelines.
- **Characteristics of good policy:** Clear, enforceable, aligned with compliance, regularly reviewed.
- **Control mapping:** Each control objective mapped to policy clause.

1.5 Security Governance and Risk Alignment

- Security must align with enterprise risk management (ERM).
- Auditor should verify that security objectives are linked to business risk appetite, KPIs, and KRI dashboards.

Chapter 2 — Logical Access and Authentication Controls

2.1 Access Control Objectives

- Ensure access is authorized, authenticated, and audited.
- **Core principles:** Need-to-know, least privilege, separation of duties.

2.2 Access Control Models

- **DAC (Discretionary Access Control):** Owner defines access (e.g., file permissions).
- **MAC (Mandatory Access Control):** Central authority assigns labels; often military.
- **RBAC (Role-Based Access Control):** Access based on organizational role.
- **ABAC (Attribute-Based Access Control):** Based on attributes like location, device, time.
- **Rule-Based Access:** Conditional access via firewalls or systems policies.

2.3 Identification, Authentication, and Authorization

- **Identification:** Unique user ID.
- **Authentication:** Proof of identity (factors – something you know/have/are).
- **Authorization:** Mapping to permitted resources.
- **Accountability:** Audit trails, monitoring, logging.

2.4 Authentication Mechanisms

Type	Examples
Knowledge factor	Passwords, PINs
Possession factor	Smart cards, tokens, mobile OTP
Inherence factor	Biometrics – fingerprint, iris, voice
Location/time factor	Geo-fencing, time-of-day access

2.5 Password and Credential Management

- Complexity, expiration, reuse restrictions, MFA integration.
- Use password vaults or federated identity (SSO / SAML / OIDC).
- Auditors verify that credential management follows NIST SP 800-63B guidance.

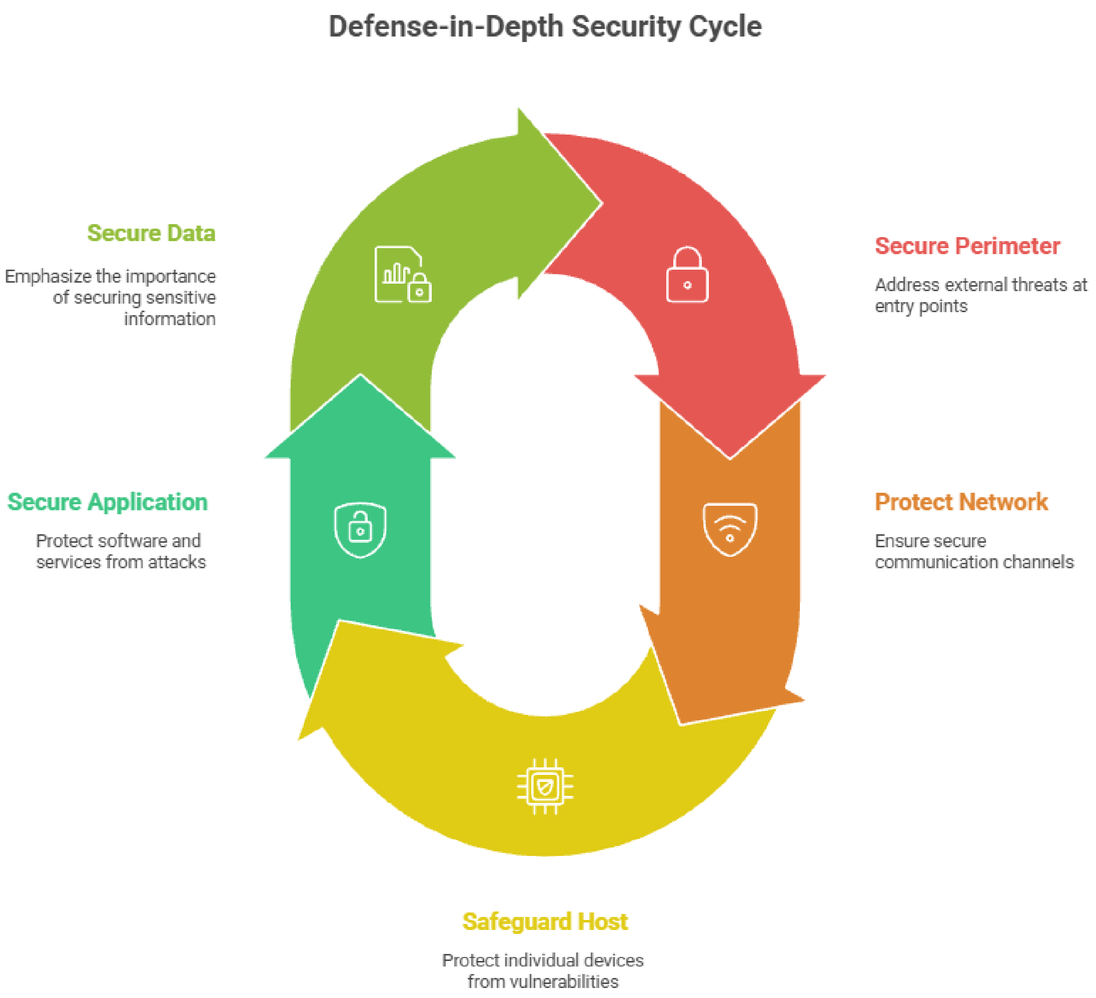
2.6 Remote and Network Access Controls

- VPNs, SSH, RADIUS/TACACS+, NAC (Network Access Control).

- Audit: Verify encryption, endpoint health checks, and revocation procedures.

2.7 Logging and Monitoring

- Centralized SIEM systems; log correlation, anomaly detection.
- Auditor checks for completeness, retention, time synchronization (NTP).



Defense-in-Depth Security Cycle
Secure Data
Emphasize the importance of securing sensitive information
Secure Perimeter
Address external threats at entry points
Secure Application
Protect software and services from attacks
Protect Network
Ensure secure communication channels
Safeguard Host
Protect individual devices from vulnerabilities

Chapter 3 — Network Infrastructure Security

3.1 Network Architecture

- **Defense-in-depth layers:** Perimeter → DMZ → Internal → Host → Application → Data.
- Segmentation via VLANs, firewalls, zero-trust network access (ZTNA).

3.2 Network Security Devices

- **Firewalls:** Packet filtering, stateful inspection, next-gen firewalls.

- **IDS/IPS:** Signature-based, anomaly-based.
- **Proxy Servers:** Content filtering, caching.
- **DLP Systems:** Monitor e-mail, endpoints, network traffic for data exfiltration.
- **Network Access Control (NAC):** Posture assessment before connection.

3.3 Encryption and Network Protection

- **Protocols:** TLS 1.3, IPSec, SSH, HTTPS, S/MIME, DNSSEC.
- **VPN types:** Site-to-site vs remote-access.
- **Auditor’s review:** Verify key lengths, certificate validity, and cipher strength.

3.4 Wireless Network Security

- Standards – 802.11i (WPA3).
- Risks: Rogue APs, evil twin attacks, weak pre-shared keys.
- Controls: 802.1X authentication, wireless intrusion detection, MAC filtering.

3.5 Network Monitoring and Incident Detection

- SNMP, NetFlow, Syslog, and SIEM correlation.
- Use of baselines, thresholds, and alerts.
- Audit: Confirm log integrity, completeness, and escalation processes.

Chapter 4 — Encryption and Cryptography Management

4.1 Purpose and Objectives of Cryptography

- Protects confidentiality, integrity, authentication, and non-repudiation of information.
- Supports secure communications, data storage, digital signatures, and transaction integrity.
- Auditors must ensure encryption aligns with enterprise data-classification and regulatory requirements (e.g., GDPR, PCI DSS).

4.2 Types of Cryptographic Systems

Symmetric Encryption

- Uses a single shared key for encryption/decryption.
- Fast and suitable for large data volumes.

- Examples: AES, DES, 3DES, Blowfish.
- **Risks:** Key distribution and management challenges.

Asymmetric Encryption (Public-Key Cryptography)

- Uses paired keys (public + private).
- Enables digital signatures and secure key exchange.
- Examples: RSA, ECC, Diffie-Hellman, ElGamal.
- **Auditor focus:** Key length adequacy, lifecycle management, certificate trust chains.

Hashing Functions

- One-way mathematical transformations for data integrity.
- Examples: SHA-256, SHA-3, BLAKE2.
- **Applications:** Password hashing, digital signatures, file verification.

Hybrid Encryption

- Combines symmetric (for performance) and asymmetric (for key exchange).
- Example: TLS handshake (RSA/ECC + AES).

4.3 Digital Signatures and Certificates

- **Digital Signatures:** Validate message integrity and origin authenticity.
- **Public Key Infrastructure (PKI):** Manages keys, digital certificates, and revocation.
- **Certificate Authorities (CAs):** Issue and manage certificates (X.509).
- **Certificate Lifecycle:** Issuance → Distribution → Renewal → Revocation.
- **Auditor verification:**
  - Certificate policies and procedures.
  - Proper revocation (CRL, OCSP).
  - Separation of duties within CA operations.

4.4 Cryptographic Key Management

- **Key Lifecycle:** Generation → Distribution → Use → Archival → Destruction.
- **Hardware Security Modules (HSMs):** Enforce key-usage policies, prevent key exposure.

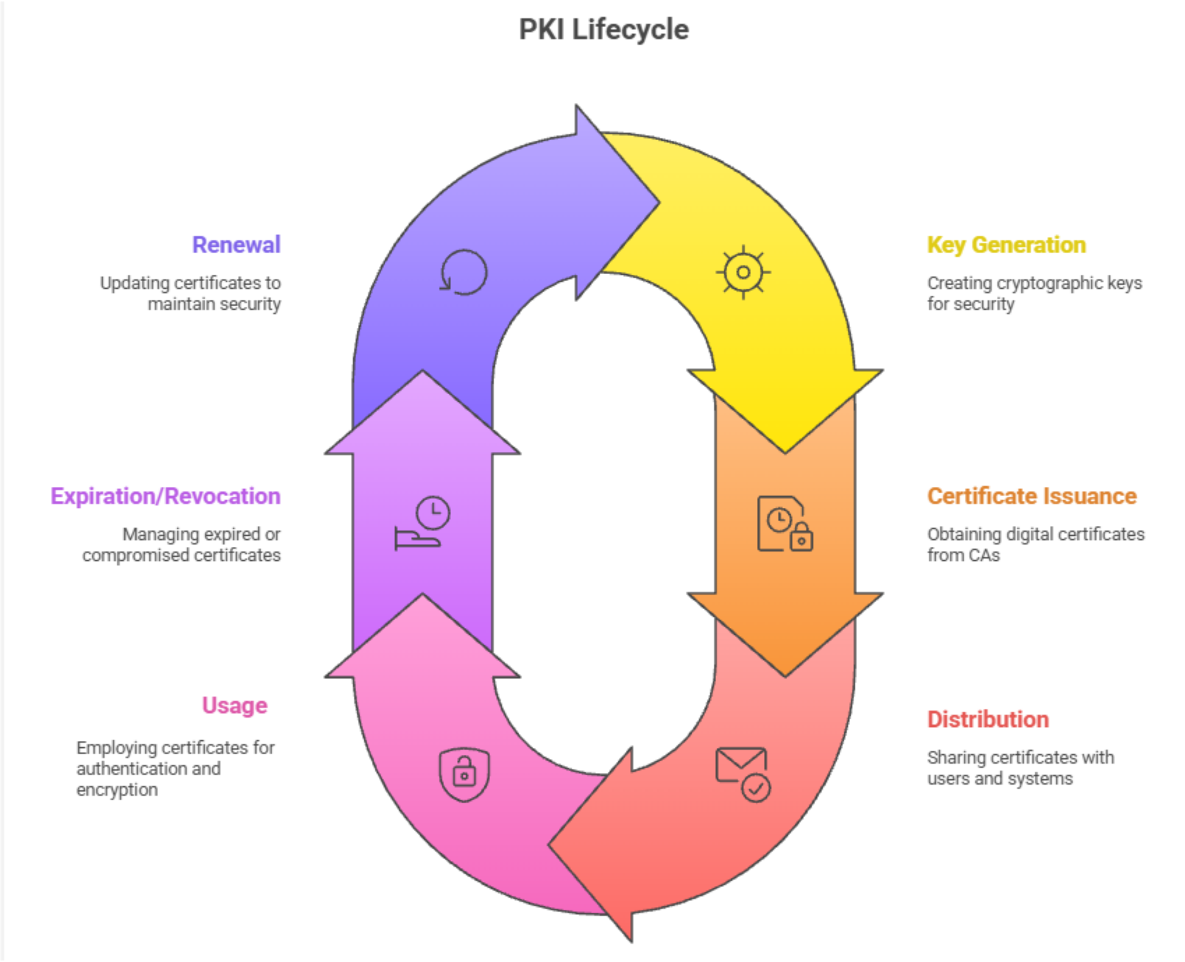
- **Auditor checks:**
    - Key rotation intervals.
    - Dual control and split knowledge.
    - Secure storage and backup of keys.
    - Documented key-management policy (aligns with ISO/IEC 11770-3).

4.5 Cryptographic Protocols

- **Data at Rest:** AES-256, BitLocker, database TDE.
- **Data in Transit:** TLS 1.3, IPSec, SSH.
- **Data in Use:** Trusted Execution Environments (Intel SGX, AMD SEV).
- **Audit consideration:** Ensure deprecated algorithms (MD5, SHA-1, SSL v2/v3) are prohibited.

4.6 Auditing Encryption Controls

- Verify encryption covers sensitive data classifications.
- Evaluate cryptographic key-management systems.
- Review access controls to encryption keys and HSMs.
- Examine compliance with regulations (FIPS 140-3, GDPR Art. 32, HIPAA).



PKI Lifecycle
Renewal
Updating certificates to maintain security
Key Generation
Creating cryptographic keys for security
Expiration/Revocation
Managing expired or compromised certificates
Certificate Issuance
Obtaining digital certificates from CAs
Usage
Employing certificates for authentication and encryption
Distribution
Sharing certificates with users and systems

Chapter 5 — Physical and Environmental Security Controls

5.1 Objectives

To prevent unauthorized physical access, damage, and interference to business premises, data centers, and supporting facilities.

5.2 Physical Security Layers

1. **Perimeter Security:** Fencing, signage, security guards, CCTV, vehicle barriers.
2. **Building Access:** Smart cards, biometric scanners, turnstiles, visitor logging.
3. **Room/Area Controls:** Locking racks, restricted server rooms, mantraps.
4. **Equipment Security:** Cable locks, tamper-evident seals, secure device disposal.
5. **Environmental Controls:** Fire detection/suppression, HVAC, power supply.

5.3 Environmental Controls

- **Fire suppression:** Halon alternatives (FM-200, Inergen).

- **Power management:** UPS, diesel generators, redundant feeds (N+1).
- **HVAC:** Maintain temperature/humidity for hardware stability.
- **Water damage prevention:** Leak detection, raised floors.

5.4 Auditor's Role

- Review facility risk assessments and access logs.
- Verify segregation of critical areas (data centers, network rooms).
- Ensure visitor escort procedures.
- Confirm periodic testing of alarms and UPS systems.

Chapter 6 — Endpoint, Mobile, and Data Protection

6.1 Endpoint Security

- Anti-malware, EDR (Endpoint Detection & Response), host firewalls.
- Patch management via centralized systems (WSUS, SCCM, Intune).
- Application control / allow-listing.
- Disk encryption (BitLocker, FileVault).
- Auditor checks configuration baselines and central policy enforcement.

6.2 Mobile Device Management (MDM)

- Controls: Device enrollment, remote wipe, app restrictions, encryption enforcement.
- BYOD policy considerations: legal consent, data segregation, containerization.
- Audit procedures:
  - Verify MDM profiles push security policies.
  - Ensure corporate data removal upon user termination.

6.3 Data Loss Prevention (DLP)

- Monitors endpoints, e-mails, cloud storage for sensitive data exfiltration.
- Integration with SIEM for alerting and response.
- Audit focus: rule accuracy, incident response handling, retention of DLP logs.

6.4 Backup and Recovery

- Local vs cloud backup, immutable storage, encryption.
- Verification of RPO/RTO alignment.
- Auditor validates testing schedule and restoration logs.

Chapter 7 — Privacy, Data Protection, and Compliance

7.1 Privacy Concepts

- **Definition:** Protecting personal data from unauthorized collection, use, and disclosure.
- **Key privacy principles:** Notice, Choice, Consent, Purpose limitation, Minimization, Accuracy, Retention, Security, Accountability.
- **Applicable frameworks:** GDPR, ISO 27701, CCPA, HIPAA.

7.2 Data Classification and Ownership

- Categories: Public / Internal / Confidential / Restricted.
- Data owners define classification; custodians enforce protection.
- Audit review: policies, labeling consistency, and periodic re-classification.

7.3 Privacy Governance and Roles

Role	Key Responsibility
Data Controller	Determines purpose and means of processing
Data Processor	Processes data on behalf of controller
Data Protection Officer (DPO)	Monitors compliance, handles DSARs
Auditor	Verifies that privacy controls and DPIAs exist

7.4 Privacy Impact Assessments (PIAs) / Data Protection Impact Assessments (DPIAs)

- Identify risks to personal data before new processing activities.
- Contain risk analysis, mitigation steps, and approval records.
- Auditor ensures they're documented and approved before go-live.

7.5 Cross-Border Data Transfer Controls

- Mechanisms: Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), adequacy decisions.
- Audit verification: existence of legal basis for transfer and encryption in transit.

7.6 Compliance Auditing

- Map privacy controls to applicable laws and frameworks.
- Evaluate consent management, user rights (access, erasure, portability).
- Review incident notification timelines (e.g., GDPR Art. 33 – 72 hours).

☑ Domain 5 Summary

By the end of Domain 5, an auditor should be able to:

- Assess logical, physical, and environmental controls.
- Evaluate cryptographic and access-control mechanisms.
- Verify endpoint and data-protection strategies.
- Confirm privacy compliance across jurisdictions.

Conclusion — Turning Concepts into Confidence

If you’ve come this far, you now understand that CISA isn’t just a certification — it’s a *mindset shift*.
It transforms you from someone who looks at systems as “working” or “not working” into someone who asks,

“Is it working securely, efficiently, and compliantly?”

Through these five domains, you’ve learned how organizations are designed, secured, audited, and sustained — from governance to recovery.

Each domain connects to the other, and together they build the foundation of an auditor who not only understands controls but also understands business.

And remember — CISA is not about memorizing ISACA terminology or frameworks word-for-word.
It’s about learning to think like an auditor — questioning, verifying, and continuously improving.

So, when someone says,

"CISA is boring,"
smile and tell them,
"It's only boring until you realize you're learning how to secure the backbone of every business."

THANK YOU

Enroll with MoS – **CISA Training @ ₹4,999**!

WWW.MINISTRYOFSECURITY.CO

MOS