

CISA Exam Prep

200+ High-Yield Terms & Concepts for the Certified
Information Systems Auditor Exam

TemplateForge

Copyright (c) 2026 TemplateForge. All rights reserved.

This material is for personal study use. No part of this book may be reproduced or distributed without written permission from the publisher.

This guide is an independent study aid and is not affiliated with or endorsed by any certifying board or licensing authority. Always verify current exam requirements with your official source.

Contents

CISA Exam Prep -- High-Yield Terms & Concepts

How to Use This Guide

PART 1 -- THE CISA EXAM & AUDITING FOUNDATIONS (10 Concepts)

PART 2 -- DOMAIN 1: INFORMATION SYSTEM AUDITING PROCESS

Section 1.1: Audit Planning & Approach (16 Concepts)

Section 1.2: Performing the Audit & Reporting (14 Concepts)

PART 3 -- DOMAIN 2: GOVERNANCE AND MANAGEMENT OF IT

Section 2.1: IT Governance & Strategy (15 Concepts)

Section 2.2: IT Resource & Portfolio Management (15 Concepts)

PART 4 -- DOMAIN 3: INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT & IMPLEMENTATION

Section 3.1: Acquisition & Development (14 Concepts)

Section 3.2: Testing, Implementation & Post-Implementation (14 Concepts)

PART 5 -- DOMAIN 4: INFORMATION SYSTEMS OPERATIONS & BUSINESS RESILIENCE

Section 4.1: IT Operations & Service Management (18 Concepts)

Section 4.2: Backups, Recovery & Disaster Recovery (20 Concepts)

PART 6 -- DOMAIN 5: PROTECTION OF INFORMATION ASSETS

Section 5.1: Information Security Management & Controls (24 Concepts)

Section 5.2: Access Control & Identity Management (16 Concepts)

Section 5.3: Cryptography & Network Security (14 Concepts)

PART 7 -- FINAL REVIEW & TEST-DAY STRATEGY (10 Concepts)

CISA Exam Prep -- High-Yield Terms & Concepts

&Category: IT Audit / Cybersecurity Certification

&Design: Deep teal (#0E7490) + gold accent

Important Disclaimer: An independent study companion. This publication is not affiliated with, endorsed by, or sponsored by ISACA (formerly the Information Systems Audit and Control Association), the owner and administrator of the CISA certification, nor by any of ISACA's affiliated bodies. CISA (Certified Information Systems Auditor) is a registered trademark of ISACA. The CISA exam content, passing standards, and eligibility requirements change over time -- for complete and authoritative preparation, consult the official ISACA CISA Review Manual, the CISA Candidate Guide, and the current CISA Job Practice published by ISACA, and verify current requirements on isaca.org. This workbook is a general study aid, not a substitute for official ISACA materials.

How to Use This Guide

The Certified Information Systems Auditor (CISA) credential is a globally recognized certification for information systems auditing, control, and security professionals. The exam is computer-based and consists of 150 multiple-choice questions covering the five task domains of the CISA Job Practice (information system auditing process; governance and management of IT; information systems acquisition, development, and implementation; information systems operations and business resilience; and protection of information assets). This workbook distills the highest-yield terms and concepts from all five domains into plain, original language you can drill and recall quickly. Work through the tables to test yourself on definitions, key facts, and the kind of judgment ISACA expects from a practicing IT auditor. This is a study aid -- pair it with the official ISACA CISA Review Manual and practice questions for full preparation.

PART 1 -- THE CISA EXAM & AUDITING FOUNDATIONS (10 Concepts)

Know the credential, the exam, and the core mindset of IT auditing before you memorize content.

#	Term	Key Facts	Strategy Tip	Example
1	CISA (Certified Information Systems Auditor)	A professional certification for IS/IT auditors, control professionals, and information security professionals, administered by ISACA.	Emphasize that CISA certifies an auditor's skill in auditing information systems and IT governance/control.	A candidate who passes the CISA exam and meets requirements earns the CISA credential.
2	ISACA	The global professional association that develops and administers the CISA (and other) certifications and publishes frameworks such as COBIT.	Refer candidates to ISACA's official materials for current exam content.	ISACA publishes the CISA Review Manual and sets the exam.

3	CISA Exam Format	A computer-based exam of 150 multiple-choice questions.	Budget your time carefully across all 150 items.	A candidate answers 150 questions in the allotted exam window.
4	Certification Requirements	CISA certification requires passing the exam AND meeting ISACA's work-experience requirements (related IS/IT audit, control, or security experience) and code-of-conduct/ethics requirements.	Passing the exam alone does not confer the credential -- experience also counts.	A candidate passes the exam and later documents the required audit work experience to be certified.
5	Continuing Education	Certified professionals must maintain the credential with continuing professional education and fees (CPE).	Plan for ongoing CPE to keep the certification current.	A CISA holder completes CPE activities each year to maintain certification.
6	The Auditor's Mindset	The IT auditor provides independent, objective assurance and advisory services on controls, risk, and governance.	Adopt an objective, risk-based, evidence-driven perspective on every question.	An auditor evaluates whether controls adequately mitigate identified risks rather than assuming they do.
7	Risk-Based Auditing	Auditing that focuses effort on the highest-risk areas and significant controls.	Allocate audit time proportionally to risk and materiality.	An auditor plans more testing on a high-risk financial system than on a low-risk support system.
8	Assurance vs. Advisory	Assurance engagements provide independent evaluation of controls/processes; advisory engagements provide guidance and recommendation		

S.

		Know which activities require independence and which are advisory.	Auditing a control is assurance; recommending a control improvement is advisory.
9	Independence	The state of being free from bias, self-interest, or undue influence	

so audit
conclusions are
objective.

Identify
relationships that
threaten
objectivity.

An auditor does
not audit a
system they
personally
developed.

10	Evidence	Information gathered and evaluated to support audit conclusions, rated by reliability (original, corroborated, competent, sufficient).	Prefer original, independently generated, corroborated evidence.	A signed system authorization form is stronger evidence than a user's verbal statement.
----	----------	--	--	---

PART 2 -- DOMAIN 1: INFORMATION SYSTEM AUDITING PROCESS

This domain covers how the IS auditor plans, performs, and reports the audit itself.

Section 1.1: Audit Planning & Approach (16 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	Audit Charter	The formal document defining the internal audit function's authority, scope, responsibilities, and reporting lines.	A proper charter gives the auditor authority and independence.	The board approves an audit charter granting access to all systems and records.
2	Audit Objectives	The specific goals of an audit engagement, defining what the audit will evaluate and report.	Clear objectives drive the scope and testing approach.	The objective is to assess the effectiveness of change-management controls.
3	Audit Scope	The boundaries of the audit -- which systems, processes, locations, and time periods are covered.	Align scope to objectives and risk; document exclusions.	The audit scope covers the accounting system but not the HR system this year.
4	Audit Program	The detailed plan of audit tests, procedures, and steps to achieve the audit objectives.	Design steps that produce reliable evidence for each objective.	The audit program lists specific walkthroughs and sample-testing steps.
5	Materiality	The significance of an error, omission, or control weakness that could influence decisions of those relying on the information.	Focus audit effort on items that are material to outcomes.	A small posting error is immaterial, while a system-wide control failure is material.
6	Risk Assessment	The process of identifying and evaluating risks to determine which controls and areas require audit attention.	Drive the audit plan from a documented risk assessment.	The auditor rates the risk of a financial misstatement to schedule audit coverage.

7	Inherent Risk	The risk of an error or loss existing before considering controls.	Distinguish inherent risk from control risk and detection risk.	A highly complex system has high inherent risk before any controls are applied.
8	Control Risk	The risk that a material error will not be prevented or detected by the system of internal controls.	Weak controls raise control risk; strong controls lower it.	Because the reconciliation control is weak, control risk is assessed as high.
9	Detection Risk	The risk that audit procedures will not detect a material error that exists.	More effective audit tests reduce detection risk.	The auditor increases substantive testing to lower detection risk.
10	Audit Risk	The risk that the auditor issues an incorrect conclusion; a function of inherent, control, and detection risk.	Remember: audit risk = inherent x control x detection risk.	High inherent and control risk require more audit work to keep audit risk acceptable.
11	Audit Universe	The complete set of auditable entities in the organization (systems, units, processes) from which audits are selected.	Use the universe to plan cyclical coverage of all areas.	The audit universe lists every major application and business process.
12	Risk-Based Audit Plan	The prioritized plan of audit engagements developed from the overall risk assessment.	Schedule highest-risk areas first and most frequently.	The plan schedules an annual financial-systems audit and a biennial low-risk process review.
13	Audit Sampling	Selecting a subset of items to test and drawing conclusions about the population.	Select samples randomly/scientifically to represent the population.	The auditor samples 50 of 5,000 invoices to test authorization.
14	Walkthrough	Tracing a transaction from initiation through processing to completion to		

understand the process and controls.

Walkthroughs confirm the auditor's understanding of the process.	The auditor follows a purchase from requisition through payment
--	---

and posting.

15	Data Analytics in Auditing	Using tools to analyze large data sets for anomalies, trends, and exceptions that direct audit attention.	Leverage analytics for complete-population testing.	The auditor runs analytics to flag unusual vendor payments.
16	Audit Committee	A board-level committee (often independent directors) responsible for oversight of internal and external audit.	The chief audit executive typically reports functionally to the audit committee.	The audit committee reviews and approves the internal audit plan and findings.

Section 1.2: Performing the Audit & Reporting (14 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	Audit Execution	The performance of planned audit procedures, gathering and analyzing evidence.	Follow the audit program and document work as you go.	The auditor executes the planned tests and notes the evidence obtained.
2	Workpapers		Complete, organized workpapers support and defend findings.	Workpapers record the samples tested and the results for each procedure.
3	Audit Finding	A conclusion that a control weakness, noncompliance, or other issue exists, with supporting evidence.	Tie every finding to evidence and to the associated risk.	The finding identifies that password changes are not enforced.
4	Root Cause Analysis		Address the root cause to prevent recurrence.	The root cause of duplicate payments is a missing invoice-matching control.
5	Audit Recommendation	The proposed remediation or improvement to address an audit finding.	Make recommendations specific, practical, and risk-aligned.	The recommendation is to implement automated three-way invoice matching.
6	Management Action Plan		Track agreed actions to closure.	Management commits to deploy the control fix by quarter end.
7	Audit Report	The final communication of audit scope, objectives, findings, recommendations, and		

conclusion.

Report objectively; include strengths as well as weaknesses.	The audit report summarizes findings and the overall control conclusion.
--	--

8	Audit Opinion / Conclusion	The overall evaluation of whether controls are adequate to mitigate key risks.	Frame conclusions against the audit objectives and scope.	The opinion states that controls are not fully adequate due to a key weakness.
9	Quality Assurance in Auditing	Ongoing programs to ensure the audit function itself meets professional standards (e.g., internal/external assessments).	Apply continuous quality improvement to audit processes.	An external peer review evaluates the audit function against standards.
10	Generally Accepted Standards / Professional Frameworks	Professional guidance and standards (e.g., ISACA's IT Audit Framework standards) that govern IS auditing practice.	Align audit practice to recognized professional standards.	The audit team follows its professional audit standards for independence and evidence.
11	Audit Universe & Coverage Ratio	The portion of the auditable universe actually covered by audit in a period.	Monitor coverage to ensure high-risk areas are not neglected.	The audit function reviews coverage to confirm all critical systems were audited.
12	Confidentiality of Audit Results	Keeping audit findings and evidence secure and shared only with those who need them.	Protect sensitive audit information from disclosure.	Audit reports are distributed only to the audit committee and relevant management.
13	Follow-Up Audit	A subsequent review to confirm that agreed management actions were implemented effectively.	Verify remediation, not just agreement to act.	A follow-up audit checks that password controls are now enforced.
14	Continuous Auditing	The use of automated tools and monitoring to evaluate controls and data on an ongoing basis.	Continuous auditing enables faster detection of control issues.	Automated monitoring flags control exceptions as they occur rather than at year end.

PART 3 -- DOMAIN 2: GOVERNANCE

AND MANAGEMENT OF IT

This domain covers how IT is governed, strategically aligned, and managed through its resources and performance.

Section 2.1: IT Governance & Strategy (15 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	IT Governance	The framework and processes that ensure IT investments and resources support and extend the organization's strategy and objectives.	Governance is about directing and controlling IT for value and risk.	The board sets IT strategy and oversees IT risk within the governance structure.
2	IT Strategy	The long-term plan aligning IT capabilities with business goals and objectives.	IT strategy must align directly with business strategy.	IT builds a cloud-migration roadmap that supports a business growth goal.
3	Strategic Alignment	The degree to which IT plans and activities are consistent with and support business objectives.	Test each IT initiative for its business value and alignment.	A new customer portal is aligned with the goal to improve customer experience.
4	COBIT	An ISACA-published framework for the governance and management of enterprise IT, organizing objectives into domains and processes.	Use COBIT concepts (goals cascade, enablers) when discussing IT governance.	The organization adopts COBIT to structure its IT governance practices.
5	Enterprise IT Governance Board	A governing body (often including board/executive representation) that sets IT direction and oversees IT risk.	Effective governance needs top-level sponsorship.	An IT steering committee approves major IT investments and priorities.
6	IT Steering Committee	A cross-functional committee that prioritizes, directs, and		

reviews IT projects and portfolios.

Steering committees align IT work to business priorities.	The steering committee reviews the project portfolio and reprioritizes
---	--

resources.

7	Stakeholder	An individual or group with an interest in or affected by the organization and its IT (users, executives, customers, regulators).	Engage stakeholders to understand requirements and risks.	The auditor interviews system owners and users to understand expectations.
8	Value Delivery	Ensuring IT delivers business value through benefits realization, cost optimization, and effective resource use.	Evaluate whether IT investments produce intended benefits.	A post-implementation review confirms the new system delivered the planned savings.
9	Performance Management	Measuring and reporting on whether IT objectives and service levels are being met.	Use KPIs and KRIs to monitor IT performance and risk.	Dashboards track system availability against target service levels.
10	Key Performance Indicator (KPI)	A metric used to evaluate the success of a process or activity against objectives.	KPIs measure whether desired outcomes are achieved.	The percentage of projects delivered on time is a project-management KPI.
11	Key Risk Indicator (KRI)	A metric used to provide early warning of increasing risk exposure.	KRIs help detect risk rising before a loss occurs.	A rising number of failed access attempts is a KRI for a security exposure.
12	IT Policy	A high-level statement of management intent, rules, and principles governing IT use and behavior.	Policies set the tone; standards and procedures implement them.	An acceptable-use policy governs how employees may use company systems.
13	IT Standard	A mandatory, specific requirement or benchmark that implements policy.	Standards operationalize policy into measurable rules.	A password standard requires 12+ characters with complexity.
14	IT Procedure	A detailed, step-by-step method for performing a task in compliance		

with policy and standards.

Procedures
provide the
how-to that
enables
consistent

execution.

A
change-impleme
ntation
procedure lists
the steps to

deploy a patch.

15	Roles and Responsibilities	The defined duties, authority, and accountability of
----	----------------------------	--

individuals and functions (segregated to avoid conflicts).

Clear roles with segregation of duties reduce risk.

The administrator who grants access is

different from the person who approves access.

Section 2.2: IT Resource & Portfolio Management (15 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	IT Portfolio Management	Managing the organization's IT projects and assets as a portfolio to optimize value, risk, and alignment.	Manage projects and assets together, not in isolation.	The portfolio balances high-value new projects with compliance-driven maintenance.
2	Project Management	The application of knowledge, skills, and processes to complete a project within scope, time, and budget.	Monitor scope, schedule, cost, and quality throughout.	A project manager tracks milestones and budget to keep the deployment on track.
3	Project Phase / Lifecycle	The distinct stages of a project (initiation, planning, execution, monitoring, closure).	Review quality and governance at each phase gate.	A project is reviewed before moving from planning into execution.
4	Program Management	Coordinating a group of related projects managed together to achieve benefits not available individually.	Programs group related projects for combined benefits.	A digital-transformation program coordinates several related IT projects.
5	Business Case	The documented justification for an IT investment, including costs, benefits, risks, and options.	A sound business case precedes major IT spend.	A business case quantifies ROI before approving a new CRM purchase.
6	Benefits Realization	The process of identifying, managing, and measuring the benefits expected from an IT investment.	Plan for how benefits will be realized and measured.	A program tracks whether the system actually cut processing time as promised.
7	Resource Plan	The plan for acquiring and assigning the		

people, funding,
and technology
needed for IT
work.

Match resources to priorities and capabilities.	A project resource plan allocates
---	---

developers and
budget to the
build phase.

8	IT Budget	The financial plan for IT spending across operations, projects, and resources.	Monitor actual spend against the approved budget.	The IT budget allocates funds to infrastructure, applications, and support.
9	Capability Management	Ensuring the organization has the people, skills, and technology needed to deliver IT services now and in the future.	Assess skills and competencies to close gaps.	The organization trains staff in cloud skills to support its strategy.
10	Asset Management	Tracking and managing IT assets over their lifecycle (acquisition, use, maintenance, disposal).	Know what assets exist and where they are.	A CMDB records all hardware and software assets and their owners.
11	Software Asset Licensing	Managing software licenses to ensure compliance and cost efficiency.	Prevent license noncompliance and uncontrolled spend.	An audit reveals more software installed than licenses purchased.
12	Outsourcing / Managed Services	Engaging external providers to deliver IT functions or services under contract.	Evaluate and monitor outsourced providers' controls and performance.	The organization outsources payroll hosting and reviews the provider's reports.
13	Service Level Agreement (SLA)	A contract defining the expected level of service (availability, response, performance).	Base service monitoring on SLA targets.	An SLA requires 99.9% availability and 4-hour issue response.
14	Due Diligence	The process of investigating and validating a third party's capability, controls, and reliability before engaging them.	Assess third-party risk before signing contracts.	Before outsourcing, the organization reviews the vendor's security certifications.
15	Vendor / Third-Party Risk Management	The ongoing process of identifying and managing risks posed by external		

providers and partners.

Monitor third parties throughout the relationship, not just at onset.	The organization periodically reviews the cloud vendor's compliance reports.
---	--

PART 4 -- DOMAIN 3: INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT & IMPLEMENTATION

This domain covers how systems are acquired, built, and brought into production -- and how the auditor evaluates that process.

Section 3.1: Acquisition & Development (14 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	System Development Lifecycle (SDLC)	The structured process of planning, analyzing, designing, building, testing, and deploying an information system.	Systems built with a disciplined SDLC have more reliable outcomes.	A new billing system follows the SDLC from requirements through deployment.
2	Requirements Definition	The identification and documentation of what a system must do to meet business needs.	Complete, clear requirements reduce rework and defects.	The team documents functional and technical requirements for a new order system.
3	Feasibility Study	An analysis of whether a proposed system is technically, operationally, and financially viable.	Assess alternatives and costs before committing.	A feasibility study compares build vs. buy options for a CRM.
4	Buy vs. Build Decision	Choosing between purchasing commercial software and developing a custom solution.	Evaluate total cost, fit, and long-term support for each option.	The organization buys an off-the-shelf ERP because customization is limited.
5	Prototyping	Building a working model of the system early to clarify requirements and design.	Prototypes help users validate needs before full build.	Users review a clickable prototype of a new dashboard.
6	Agile Development	An iterative development approach that delivers functionality in small increments with continuous feedback.	In agile, requirements evolve and testing is continuous.	The team delivers a feature every two-week sprint and adjusts priorities.
7	Waterfall Development	A sequential, phase-by-phase development		

model with
defined stages.

Waterfall suits
projects with
stable,

well-defined
requirements.

A regulatory
reporting system
uses a waterfall

approach with
fixed phases.

8	Design Review	A formal evaluation of system design for correctness, security, and consistency with requirements.	Review design before coding to catch issues early.	A design review confirms the database schema meets data-integrity needs.
9	Change Control / Change Management	The formal process of evaluating, approving, and implementing changes to systems to minimize disruption and risk.	All changes should be approved, tested, and documented.	A change-control board approves each production code change with testing evidence.
10	System Architecture	The high-level structure of a system's components, data, interfaces, and technology.	Architecture should support requirements, security, and scalability.	A three-tier architecture separates presentation, logic, and data.
11	Software Configuration Management	Controlling changes to software code and configuration (versioning, baselines, builds).	Track all code changes and versions reliably.	Each code change is versioned and linked to its build in the repository.
12	Segregation of Duties in Development	Separating development, testing, and production roles so no one person controls an entire change independently.	Prevent developers from moving their own code to production directly.	Developers cannot deploy to production; a release team performs deployments.
13	Data Integrity	Ensuring data is accurate, complete, and consistent, and is processed correctly.	Design controls to guard data accuracy and consistency.	Input validation and referential integrity protect data quality.
14	Application Controls	Controls built into an application (input, processing, output) to ensure valid and complete data.	Contrast application controls with general IT controls.	An application rejects an order with invalid account numbers (input control).

Section 3.2: Testing, Implementation & Post-Implementation (14 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	Unit Testing	Testing individual components or modules in isolation to verify they work correctly.	Test the smallest units before integration.	The developer tests a single login function in isolation.
2	Integration Testing	Testing that combined modules and interfaces work together correctly.	Verify that modules cooperate as a whole.	The team tests that the order module correctly passes data to the inventory module.
3	System Testing	Testing the complete, integrated system against its requirements.	Confirm the whole system meets specifications.	End-to-end system testing verifies a full order-to-payment flow.
4	User Acceptance Testing (UAT)	Formal testing by end users to confirm the system meets their needs before go-live.	Obtain explicit user sign-off before deployment.	Business users execute real scenarios and approve the system for release.
5	Regression Testing	Re-testing previously working functionality to ensure new changes did not break it.	Run regression tests after every change.	After a bug fix, the team re-runs the test that previously verified the feature.
6	Test Data	Controlled data used for testing that does not risk production data and is properly controlled.	Use sanitized or masked data and protect it.	The team tests with masked customer data rather than live production data.
7	Test Environment	A separate environment for executing tests, isolated from production.	Keep test separate from production to avoid disruption.	Staging mirrors production so testing does not affect live systems.
8	Implementation / Go-Live	The controlled transition of the new system into production use.	Plan and communicate the cutover carefully.	The new system goes live over a weekend after final checks.

9	Parallel Run	Running the old and new systems together and comparing results during transition.	Parallel running reduces cutover risk.	Payroll is run on both old and new systems for two periods and results compared.
10	Cutover Planning	The detailed plan for switching to the new system, including conversion, rollback, and timing.	Anticipate rollback and contingency in the cutover plan.	The cutover plan includes a rollback step if the new system fails.
11	Data Conversion / Migration	The process of moving data from old formats/systems to the new system, with validation.	Validate completeness and accuracy after migration.	The team reconciles record counts after converting legacy data.
12	Post-Implementation Review	An evaluation after go-live of whether the system meets requirements, benefits, and controls.	Verify intended benefits and identify lessons learned.	A review confirms the new system achieved its targets and notes improvements.
13	Backout / Rollback Plan	The predefined procedure to revert to the prior state if an implementation fails.	Always have a tested rollback ready.	A failed deployment activates the rollback to the prior stable release.
14	Release Management	The process of planning, scheduling, and controlling the movement of builds to production.	Coordinate releases to avoid conflicts and downtime.	Releases are batched and scheduled to minimize production disruption.

PART 5 -- DOMAIN 4: INFORMATION SYSTEMS OPERATIONS & BUSINESS RESILIENCE

This domain covers the day-to-day reliable operation of systems and the ability to recover from disruptions.

Section 4.1: IT Operations & Service Management (18 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	IT Operations	The day-to-day activities that keep IT systems and services running reliably.	Effective operations require monitoring, controls, and procedures.	The operations team manages backups, scheduling, and system monitoring.
2	Problem Management	The process of identifying and resolving the root causes of incidents to prevent recurrence.	Fix root causes, not just symptoms.	A recurring outage is investigated to find and fix its underlying cause.
3	Incident Management	The process of responding to and restoring service after an unexpected interruption.	Respond quickly to restore service and limit impact.	Help desk tickets are triaged and resolved to restore a downed system.
4	Change Management	The controlled process for approving and implementing changes to avoid disruptions.	Review, test, approve, and document every change.	An emergency change is reviewed after-hours and logged immediately.
5	Service Desk	The single point of contact for users to report issues and request services.	Track and resolve user requests efficiently.	Users call the service desk to report a login problem.
6	Capacity Management	Ensuring IT resources (CPU, storage, network) are sufficient to meet current and future demand.	Monitor utilization and plan for growth.	An upward trend in storage use triggers a capacity upgrade.
7	Performance Monitoring	Continuously measuring system and network performance against targets.	Use monitoring to detect and prevent degradations.	Alerts notify staff when a server's CPU stays above a threshold.
8	Job / Batch Scheduling	Automating the execution of routine processing tasks (e.g., nightly		

batch jobs) on
schedule.

Ensure
scheduled jobs
run successfully
and on time.

A nightly backup
job runs
automatically
and is checked
each morning.

9	System Software Controls	Controls over operating systems, utilities, and system software to ensure reliable and secure operation.	Control access and changes to system software.	System administrator access to the OS is tightly restricted and monitored.
10	ITIL	A widely used framework of best practices for IT service management (service strategy, design, transition, operation, continual improvement).	Use ITIL concepts for structured service management.	The organization adopts ITIL processes for incident, problem, and change management.
11	Service Catalog	A documented listing of the IT services offered, with descriptions and service levels.	A clear catalog sets expectations for users.	Employees browse the service catalog to request a new software install.
12	Business Continuity Management	The holistic management of processes to ensure critical business functions continue during and after a disruption.	BCM protects the organization's ability to operate.	Business continuity planning covers the resumption of critical processes.
13	Business Impact Analysis (BIA)	An analysis that identifies critical functions and the impact of their disruption to determine recovery priorities.	The BIA drives recovery time and recovery point targets.	The BIA identifies that order processing cannot be down more than 4 hours.
14	Recovery Time Objective (RTO)	The maximum acceptable time to restore a system or process after a disruption.	Lower RTO requires faster, often costlier recovery.	The order system has an RTO of 4 hours.
15	Recovery Point Objective (RPO)	The maximum acceptable data loss (measured in time) after a		

disruption.

Lower RPO requires more frequent backups.	The system has an RPO of 15 minutes, requiring
---	--

near-continuous
backups.

16	High Availability	Designing systems to be continuously available using redundancy and failover.	Eliminate single points of failure.	A database cluster fails over automatically if the primary node fails.
17	Redundancy	Providing duplicate components so a failure does not cause downtime.	Redundant components increase availability.	Dual power supplies and mirrored disks provide redundancy.
18	Load Balancing	Distributing workloads across multiple servers to improve performance and availability.	Balance traffic to avoid overloading single servers.	A load balancer spreads web traffic across several application servers.

Section 4.2: Backups, Recovery & Disaster Recovery (20 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	Backup	A copy of data taken to enable restoration after loss or corruption.	Back up data regularly and verify restorability.	A nightly backup copies the database to secure storage.
2	Full Backup	A complete copy of all selected data.	Full backups restore quickly but take time and space.	A full backup of the database is taken every Sunday.
3	Incremental Backup	A backup of only the data changed since the last backup (full or incremental).	Incremental backups are fast but require a full chain to restore.	Daily incremental backups capture only changes since the last backup.
4	Differential Backup	A backup of all data changed since the last full backup.	Restores faster than incremental but uses more space.	Differential backups grow between full backups but simplify restore.
5	Offsite Backup / Cold Storage	Storing backups at a separate physical location to survive a site disaster.	Store recovery copies away from the primary site.	Backup tapes are stored in a secure offsite facility.
6	Cloud Backup	Backing up data to remote cloud storage with redundancy.	Cloud backups provide geographic resilience.	The database is continuously replicated to a cloud region.
7	Backup Verification	Testing that backups can actually be restored when needed.	An untested backup is no protection.	The team periodically performs a test restore of the backup.
8	Restore / Recovery	The process of recovering data and systems from backups after a loss.	Practice restores so they work under pressure.	After an outage, the team restores the database from the last valid backup.
9	Disaster Recovery Plan (DRP)	The documented plan for recovering IT systems and operations after a major disaster.	Test the DRP with exercises and drills.	A DR exercise simulates a data-center outage and validates recovery.

10	Disaster Recovery Site	An alternate facility used to recover operations after a disaster.	Choose the site type based on RTO/RPO needs.	An alternate site hosts recovery after the primary center is lost.
11	Hot Site	A fully equipped alternate site that can take over operations quickly after a disaster.	Hot sites provide the fastest recovery.	A hot site has the hardware ready to resume processing immediately.
12	Warm Site	An alternate site with some equipment/readiness but not fully mirrored.	Warm sites balance cost and recovery speed.	A warm site can restore systems within a day after activation.
13	Cold Site	A basic alternate location with power and space but no ready equipment.	Cold sites are cheapest but slowest to recover.	Equipment must be brought in and set up at a cold site.
14	RTO/RPO Targets	Agreed metrics (recovery time and data loss) that drive recovery design and testing.	Base recovery design on defined targets.	Because RTO is short, the organization maintains a hot site.
15	Resilience Testing / DR Drill	Periodic exercises to validate recovery plans and readiness.	Test regularly; fix gaps found in exercises.	A simulated failover drill reveals a network dependency that must be fixed.
16	Crisis Management / Incident Response Plan	The plan for coordinating the organization's response to a major disruption or security incident.	Have clear roles, escalation, and communication.	A crisis team activates predefined procedures during a major outage.
17	The 3-2-1 Backup Rule	Keep at least 3 copies of data, on 2 different media, with 1 copy offsite.	The 3-2-1 rule improves resilience to loss.	A company keeps the primary copy, a local backup, and an offsite copy.
18	Immutable / WORM Backups	Backups that cannot be altered or deleted for a set period, protecting against		

ransomware and
tampering.

Immutable copies resist deletion by attackers.	An immutable backup cannot be overwritten or encrypted by ransomware.
---	---

19	Journaling	Recording changes to data so a system can be restored to a specific point in time.	Journaling supports point-in-time recovery.	A journaled file system replays changes to recover to a recent state.
20	Site Replication	Continuously replicating data or systems to an alternate site for rapid recovery.	Replication enables near-zero data loss.	The database is synchronously replicated to a second site.

PART 6 -- DOMAIN 5: PROTECTION OF INFORMATION ASSETS

This domain covers the confidentiality, integrity, and availability of information assets -- security management, access, and cryptography.

Section 5.1: Information Security Management & Controls (24 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	Information Security (InfoSec)	Protecting the confidentiality, integrity, and availability (CIA) of information.	Anchor every security discussion in the CIA triad.	Access controls protect confidentiality; backups protect availability.
2	Confidentiality	Ensuring information is accessed only by those authorized.	Use access controls and encryption for confidentiality.	Only authorized managers can view salary data.
3	Integrity	Ensuring information is accurate and has not been altered by unauthorized parties.	Use hashes, validation, and change controls for integrity.	A digital signature detects tampering with a report.
4	Availability	Ensuring information and systems are accessible when needed.	Use redundancy, backups, and monitoring for availability.	A financial system remains accessible during peak hours via load balancing.
5	Security Policy	The high-level statement of management intent and rules for protecting information assets.	Policies are the foundation; standards/procedures implement them.	A security policy defines the acceptable use of company systems.
6	Security Awareness Training	Ongoing education to help employees understand and follow security practices.	People are a key control; train them regularly.	New employees complete security-awareness training on phishing and passwords.
7	Risk Management	The process of identifying, assessing, and responding to risks to information assets.	Choose responses: mitigate, transfer, accept, or avoid.	A high-risk vulnerability is mitigated by applying a patch.
8	Threat	A potential cause of an unwanted event that could damage information assets.	Identify threats to understand what controls must address.	Malware, phishing, and insider misuse are common threats.

9	Vulnerability	A weakness in a system or control that a threat could exploit.	Scan for and remediate vulnerabilities.	An unpatched server has a known vulnerability an attacker could exploit.
10	Attack Vector	The path or means by which an attacker gains access or causes harm.	Understand attack vectors to design defenses.	Email phishing is a common attack vector for initial access.
11	Defense in Depth	Using multiple layers of security controls so a failure in one layer is caught by another.	Layer controls (network, host, application, data).	A web app is protected by a firewall, a WAF, application controls, and monitoring.
12	Least Privilege	Granting users only the minimum access needed to perform their duties.	Apply least privilege to limit exposure.	A data-entry clerk has no administrator rights.
13	Segregation of Duties	Dividing duties so no single person can both perpetrate and conceal an error or fraud.	Separate incompatible duties across people.	The person who requests a purchase cannot also approve and receive it alone.
14	Security Baseline	A predefined minimum standard of security configuration applied to systems.	Harden systems to a consistent baseline.	All servers are configured to the approved security baseline before deployment.
15	Vulnerability Management	The ongoing process of identifying, prioritizing, and remediating vulnerabilities.	Patch and remediate based on risk.	A monthly scan identifies critical vulnerabilities that are patched urgently.
16	Patch Management	The process of identifying, testing, and applying software updates to fix vulnerabilities.	Test patches before deploying to production.	Security patches are tested in staging and then deployed.

17	Security Incident	An event that violates or threatens the organization's security policy or information assets.	Detect, respond, and learn from incidents.	A phishing attempt that compromises a user account is a security incident.
18	Incident Response	The structured process of detecting, containing, eradicating, and recovering from security incidents.	Have a documented, tested incident response plan.	The response team contains a breach, eradicates the threat, and recovers systems.
19	Security Information and Event Management (SIEM)	A solution that collects and analyzes security logs for correlation and alerting.	Use SIEM to detect threats from log data.	A SIEM correlates failed logins across systems to flag an attack.
20	Logging and Monitoring	Recording security-relevant events and reviewing them for anomalies.	Retain and review logs for suspicious activity.	The audit team reviews system logs for unauthorized access attempts.
21	Zero Trust	A security model that assumes no user or device is trusted by default and verifies every access request.	Apply least-privilege and continuous verification.	A zero-trust network requires verification for each access, not just at login.
22	Data Loss Prevention (DLP)	Controls that detect and prevent the unauthorized transmission or exfiltration of sensitive data.	Protect sensitive data from leaving the environment.	A DLP tool blocks an employee from emailing files containing card numbers.
23	Endpoint Protection	Security software and controls protecting end-user devices (antivirus, EDR, policy).	Protect every endpoint as a potential entry point.	An endpoint detection and response tool isolates a compromised laptop.
24	Security Operations Center (SOC)	A centralized team/facility that monitors, detects, and responds to security events.	A SOC provides 24/7 monitoring and response.	A SOC analyst triages alerts and escalates confirmed threats.

Section 5.2: Access Control & Identity Management (16 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	Access Control	Mechanisms that regulate who can access resources and what they can do.	Control access based on identity, need, and risk.	A user is granted read-only access to a shared folder.
2	Authentication	Verifying the identity of a user or system.	Use strong authentication factors.	A user proves identity with a password and a one-time code.
3	Authorization	Granting an authenticated user the rights to perform specific actions.	Authentication confirms identity; authorization grants access.	After logging in, the user is authorized to edit only their own records.
4	Multi-Factor Authentication (MFA)	Authentication using two or more independent factors (something you know, have, are).	Enable MFA to reduce credential-compromise risk.	Login requires a password and a code from an authenticator app.
5	Password Policy	Rules governing password creation, complexity, and reuse.	Enforce strong, unique passwords.	Passwords must be at least 12 characters and unique per system.
6	Identity and Access Management (IAM)	The framework of policies and tools for managing digital identities and their access.	IAM centralizes identity, authentication, and authorization.	An IAM system provisions and de-provisions user accounts across systems.
7	Role-Based Access Control (RBAC)	Granting access based on a user's role or job function.	RBAC simplifies administration by role.	All accountants are granted the same role-based access to the ledger.
8	Access Review / Recertification	Periodic review of user access to confirm it remains appropriate and remove stale access.	Regularly recertify access to prevent excessive privileges.	A quarterly review removes a departed employee's system access.

9	User Provisioning / De-provisioning	Creating, modifying, and removing user accounts and access.	De-provision promptly when access is no longer needed.	An employee's access is removed on their last day.
10	Segregation of Duties in Access	Preventing one user from holding incompatible access rights that enable fraud.	Conflicting access must be split or compensated.	A person who can initiate a payment cannot also approve and reconcile it alone.
11	Privileged Access Management (PAM)	Special controls for highly privileged (administrator) accounts.	Protect and monitor privileged accounts closely.	Admin credentials are vaulted, rotated, and their use is logged.
12	Single Sign-On (SSO)	Allowing a user to authenticate once and access multiple systems.	SSO improves usability but concentrates risk on one credential.	A user logs in once and is authenticated across several applications.
13	Federation	Trust relationships that let identities be shared across organizations.	Federate identity across trusted partners.	An organization trusts another's identity provider for partner access.
14	Biometric Authentication	Authenticating using physical characteristics (fingerprint, face, iris).	Biometrics are a possession/inherence factor.	A phone unlocks using a fingerprint scan.
15	Session Management	Controlling the lifecycle of an authenticated session (creation, timeout, termination).	Enforce sessions to prevent unauthorized continued access.	A session times out after inactivity and requires re-authentication.
16	Access Control Lists (ACL)	A list of permissions attached to a resource specifying who can access it.	Use ACLs to enforce precise permissions on objects.	A file's ACL grants read access to the finance group only.

Section 5.3: Cryptography & Network Security (14 Concepts)

#	Term	Key Facts	Strategy Tip	Example
1	Cryptography	The use of mathematical techniques to protect information (confidentiality, integrity, authentication).	Use cryptography appropriate to the data and risk.	Encryption protects stored customer data and transmitted data.
2	Encryption		Encrypt data at rest and in transit.	A database encrypts customer records so they are unreadable without the key.
3	Symmetric Encryption	Encryption using the same key for encryption and decryption.	Symmetric is fast but requires secure key sharing.	AES is used with a shared secret to encrypt a file.
4	Asymmetric (Public-Key) Encryption	Encryption using a public/private key pair; what one key encrypts the other decrypts.	Use public-key for key exchange and digital signatures.	A sender encrypts with the recipient's public key; only the private key decrypts.
5	Hashing	A one-way function producing a fixed-size digest that verifies data integrity.	Hashes detect changes but cannot be reversed.	A SHA-256 hash confirms a download was not altered.
6	Digital Signature	A cryptographic mechanism providing integrity, authentication, and non-repudiation, created with a private key.	Digital signatures prove origin and integrity.	A signed contract confirms the signer and that it was not altered.
7	Certificate Authority (CA)		Certificates establish trust in public-key operations.	A CA issues an SSL certificate for a website.
8	Public Key Infrastructure (PKI)	The framework of policies, systems, and CAs for		

managing public
keys and
certificates.

PKI supports
trust for
encryption and
signatures.

The organization
runs an internal
PKI for employee
certificates.

9	Key Management	The policies and practices for generating, storing, distributing, and rotating cryptographic keys.	Protect keys as the most sensitive assets.	Encryption keys are stored in a hardware security module (HSM).
10	Transport Layer Security (TLS)	The protocol that encrypts data in transit over networks.	Use TLS for secure communications.	Website traffic is protected in transit with TLS.
11	Firewall	A security device/filter that controls traffic entering and leaving a network based on rules.	Segment and filter network traffic.	A firewall blocks inbound traffic to non-essential ports.
12	Network Segmentation	Dividing the network into zones to contain threats and limit access.	Segment sensitive systems from the general network.	The payment system is on a separate segment from employee workstations.
13	Intrusion Detection / Prevention System (IDS/IPS)	Systems that detect (IDS) and block (IPS) malicious network or host activity.	Use IDS/IPS to detect and stop attacks.	An IPS blocks traffic that matches known attack signatures.
14	Virtual Private Network (VPN)	An encrypted tunnel for secure remote access over the internet.	Use VPNs for secure remote connections.	A remote employee connects via VPN to access internal systems securely.

PART 7 -- FINAL REVIEW & TEST-DAY STRATEGY (10 Concepts)

A concise wrap-up of the auditor's mindset and a practical test-day plan.

#	Term	Key Facts	Strategy Tip	Example
1	Review the Five Domains	The CISA exam assesses five broad domains: audit process; IT governance; acquisition/devel		

opment;
operations/resilie
nce; and
protection of
assets.

Drill every domain; none should be neglected.	A candidate reviews flashcards across all five domains before the exam.
--	--

2	Risk Is Central	Nearly every CISA question is about identifying, evaluating, or responding to risk.	When unsure, choose the answer that best handles risk.	A question asks which control best mitigates a data-breach risk.
3	Independence Matters	The auditor must stay objective and independent of the areas audited.	Flag answers that compromise auditor objectivity.	An answer suggesting an auditor audits work they performed is likely wrong.
4	Controls Protect CIA	Controls exist to protect confidentiality, integrity, and availability.	Map control questions back to the CIA triad.	A hashing question maps to integrity.
5	Evidence Quality	Stronger evidence is original, independent, and corroborated.	Prefer the most reliable evidence in testing questions.	An independent confirmation beat a user's recollection.
6	Time Management	With 150 questions, keep a steady pace and flag hard items to return to.	Move through, mark, and revisit questions you skip.	A candidate tracks time and leaves sufficient time for review.
7	Eliminate Distractors	Many wrong answers are plausible but address the wrong layer or scope.	Eliminate answers that are true but off-topic.	A general security answer is rejected when the question is specifically about access control.
8	Read the Question Fully	CISA scenarios hinge on a specific detail (scope, responsibility, timing).	Identify the exact issue before choosing.	A question differs based on whether the person is management, user, or auditor.
9	Best vs. Correct	Some questions ask for the best or most effective choice among valid options.	Pick the most complete, risk-focused answer.	Among valid controls, choose the one that best reduces the stated risk.
10	Pair with Official Materials	This workbook is a review aid; pair it with the official ISACA CISA Review Manual and practice questions.	Verify current exam content and requirements with ISACA.	A candidate studies this guide and the official ISACA materials for full preparation.

End of workbook. Prepare thoroughly, stay risk-focused, and good luck on the CISA exam.