GUIDE

CISA Exam Study Guide

The five domains, condensed for exam day

How to use this guide

This guide condenses the CISA exam, ISACA's Certified Information Systems Auditor certification, into what you need on exam day: how the exam works, a study plan, the key ideas of each domain, the traps that catch people, and 18 original practice questions with explanations.

It is not ISACA material and contains no real exam questions. Use it next to ISACA's official exam content outline, and practice the way of thinking more than the facts.

> **Tip:** Don't memorize lists. Picture a restaurant inspector with a clipboard: they plan the visit around the riskiest dishes, ask for proof, and write a fair report. The owner fixes the problems, not the inspector. That picture answers a lot of exam questions.

How the exam works

At the time of writing, the exam looks like this. Confirm every detail, including fees, duration, scheduling and experience waivers, on isaca.org before you book.

Item	What to expect
Format	150 multiple choice questions, taken online or at a test center
Time	Four hours
Scoring	Scaled score from 200 to 800; 450 or higher passes
Job practice	Five domains, current outline in effect since August 1, 2024
After passing	Apply within five years, show five years of relevant work experience (some can be waived), agree to ISACA's Code of Professional Ethics, earn yearly continuing education (CPE)

Domain	Weight	Restaurant picture
1 Information System Auditing Process	18%	How the inspector works

Domain	Weight	Restaurant picture
2 Governance and Management of IT	18%	How the owner runs the place
3 Information Systems Acquisition, Development and Implementation	12%	Building a new kitchen
4 Information Systems Operations and Business Resilience	26%	The daily service, and the night the power goes out
5 Protection of Information Assets	26%	Locks, keys, safe and cameras

Domains 4 and 5 make up more than half the exam. Domains 1 and 2 build the auditor mindset that every other question depends on.

How questions are written

Most questions describe a short scenario and ask for the **best**, **first**, **most important** or **greatest risk** answer. Often two or three options are technically true. The right one is the one an IT auditor would choose in that role.

Read every question in four steps:

1. **Who am I?** An IS auditor, unless the question says otherwise.
2. **What is asked?** First step, best control, biggest concern, best evidence.
3. **Spot the keyword:** first, best, most, primary, greatest.
4. **Pick the answer that fits the auditor's role,** not the one a system administrator would pick.

An 8 week study plan

Plan by domain weight and start with your weakest area. Use practice questions as reasoning drills: for every wrong option, write one line on why it is wrong.

Week	Focus	Goal
1	Domain 1: standards, ethics, independence, risk based planning	Know the audit process end to end
2	Domain 1: evidence, sampling, analytics, reporting, follow up	Explain each type of evidence and sampling
3	Domain 2: governance, strategy, policies, roles, segregation of duties	Separate governance from management
4	Domain 2: risk management, performance, vendors. Domain 3 part one	Supplier lifecycle, project and SDLC controls

Week	Focus	Goal
5	Domain 3 part two, Domain 4: operations, change, incidents	Go live, migration, application controls, change management
6	Domain 4: business resilience	BIA, RTO, RPO, backups, recovery sites, plan tests
7	Domain 5: access, identity, network, encryption, monitoring, incidents	The access lifecycle and how to audit it
8	Mixed practice exams, review of weak spots, rest	Timed practice, then a calm last two days

> **Tip:** Map your own work to each domain. If you have run access reviews, faced a SOC 2 audit or managed backups, use those memories as your examples. They stick far better than definitions.

Domain 1: Information System Auditing Process (18%)

Key concepts

- **Standards and ethics:** ISACA's IT Audit Framework (ITAF) sets standards (what you must do) and guidelines (how). Every CISA agrees to a code of ethics: honest, confidential, competent, keep learning. Due professional care means acting like a careful professional, not being perfect.
- **Independence:** in fact (your judgment is free) and in appearance (an outsider would agree). Never audit something you designed or run.
- **Audit charter:** the signed mandate for internal audit: purpose, authority, responsibility, access to people and records. Approved by the board or audit committee.
- **Reporting line:** internal audit reports functionally to the audit committee, never to the people it audits.
- **Audit universe and risk based planning:** list everything auditable, rank it by risk, audit high risk areas more often.
- **Three risks:** inherent risk (before any control), control risk (a control fails to catch a problem), detection risk (the auditor misses it). Detection risk is the only one the auditor controls.
- **Materiality:** would the issue change someone's decision?
- **Evidence:** must be sufficient, reliable and relevant. Gathered by inquiry, observation, inspection, reperformance and data analytics.
- **Sampling:** statistical (random, measurable confidence) or non statistical (judgment). Attribute sampling tests controls (yes or no); variable sampling estimates amounts.
- **CAATs:** computer assisted audit techniques test whole populations with SQL, scripts or audit tools.
- **Findings:** condition, criteria, cause, effect, recommendation.

What the exam likes to test

- Understanding the business and its risks comes before any testing.
- Evidence strength: system generated and independent evidence beats verbal answers and documents prepared by the auditee. Evidence the auditor obtains directly is strongest.
- The population must be complete before you sample.
- The auditor recommends; management decides and fixes. Accepting risk is management's call.

Traps

> **Warning:** Inherent versus control risk: if the question mentions no control, it is about inherent risk. Sample versus population: a perfect sample from an incomplete list proves nothing, so validate the population first.

Domain 2: Governance and Management of IT (18%)

Key concepts

- **Governance versus management:** the board evaluates, directs and monitors; management plans, builds and runs.
- **IT strategy follows business strategy.** An IT steering committee of business and IT leaders sets priorities and approves major spending.
- **Frameworks:** COBIT (ISACA's governance framework), ITIL (service management), ISO 27001 (security management system).
- **Policy layers:** policy (what and who), standard (specific requirements), procedure (step by step how), guideline (advice, not mandatory).
- **Roles:** data owners in the business decide who gets access; IT is the custodian. Segregation of duties stops one person from doing and hiding a risky task.
- **Three lines model:** first line runs controls, second line oversees risk and compliance, third line is internal audit giving independent assurance.
- **Risk management:** identify, assess, treat (avoid, reduce, transfer, accept), monitor. A risk register with inherent and residual risk, owners and review dates. Risk appetite is set by the board.
- **Performance:** KPIs show how well you perform; KRIs warn that risk is rising. Balanced scorecard and maturity or capability levels.
- **Vendors:** due diligence, contract terms (security duties, breach notice, right to audit, exit), SLA monitoring, review of SOC reports, exit plan.

What the exam likes to test

- The first thing to check is that an approved strategy or policy exists.
- Approval at the right level: top policies by senior management or the board.
- Segregation of duties conflicts, and compensating controls in small teams.
- Outsourcing work never outsources accountability.

Traps

- **SOC 1 versus SOC 2:** SOC 1 covers controls relevant to financial reporting; SOC 2 covers security, availability and related criteria. Type 2 tests operation over a period.
- **Complementary user entity controls:** the vendor report assumes you do your part, such as MFA and removing leavers. Check that you do.
- **Policy versus procedure:** clicks and screens mean procedure.

Domain 3: Information Systems Acquisition, Development and Implementation (12%)

Key concepts

- **Business case and feasibility:** why, cost, benefit, risk, approved by real authority. Benefits realization checks later whether it paid off.
- **Project governance:** project manager, steering committee, scope, budget and timeline control.
- **Build versus buy:** requirements first, including security and privacy. Contracts with SLAs, right to audit, data return, and source code escrow where the vendor might disappear.
- **SDLC:** requirements, design, build, test, release. Waterfall in phases; agile in short sprints; DevOps with automated build, test and deploy.
- **Testing:** unit, integration, system, user acceptance testing (UAT) signed by the business.
- **Go live:** readiness review, known defects accepted, go or no go decision. Changeover methods: parallel, phased, pilot, big bang. A tested rollback plan.
- **Data migration:** completeness and accuracy proven with record counts and control totals, signed off by the data owner.
- **Post implementation review:** compare results with the business case.
- **Application controls:** input (edit checks, range, format, duplicates), processing (run to run totals), output (right reports to the right people), interfaces (counts, totals, error queues with owners).

What the exam likes to test

- The auditor's involvement early in a project, to check that controls are designed in, without designing them.

- UAT is signed by the business, not IT.
- Migration needs reconciliation evidence, not a promise.
- An automated control can be tested once if IT general controls are effective.

Traps

> **Warning:** IT general controls (access, change, operations) protect the whole environment. Application controls check each transaction. If ITGCs are weak, testing one automated control once proves little.

Domain 4: Information Systems Operations and Business Resilience (26%)

Key concepts

- **Operations:** job scheduling with alerts on failure, monitoring and operational logs, end user computing (critical spreadsheets and scripts outside IT).
- **Asset and configuration management:** inventory, licenses, CMDB, approved baselines.
- **Incident versus problem management:** incidents restore service now; problem management finds and removes the cause. A known error has a known cause and a pending fix.
- **Change management:** request, test, independent approval, deploy, record. Developers do not push to production alone. Emergency changes still get documented and approved afterwards.
- **Patch management:** deadlines by severity.
- **Capacity and service levels:** plan for peaks, measure SLAs, act on misses.
- **Databases and system software:** few privileged users, direct data changes logged, no shared admin accounts.
- **Business impact analysis (BIA):** identifies critical processes, impact over time, and the maximum tolerable downtime.
- **RTO and RPO:** recovery time objective (how fast you must be running again) and recovery point objective (how much data you can lose). Both come from the BIA.
- **Plans:** business continuity plan (keep serving customers, owned by the business) and disaster recovery plan (restore technology, owned by IT).
- **Backups:** full, incremental (changes since the last backup), differential (changes since the last full). Offsite and immutable copies. A backup counts only when a restore has been tested.
- **Recovery sites:** hot (hours), warm (days), cold (weeks), reciprocal agreements (risky). In the cloud: multiple zones and regions.
- **Plan tests:** checklist review, tabletop, simulation, parallel test, full interruption.

What the exam likes to test

- The BIA comes first, always.
- RPO drives backup frequency; RTO drives the recovery option.
- An untested plan is only an assumption.
- Unauthorized production changes are a top risk.

Traps

- **RTO versus RPO:** RTO looks forward in time, RPO looks back at data loss. Nightly backups mean an RPO of roughly 24 hours.
- **Incremental versus differential:** incremental is fast to back up and slow to restore; differential is the opposite.

> **Restaurant view:** The owner's notebook says how long the restaurant can stay closed before regulars go elsewhere. That is the BIA. Starting the generator every month is the restore test.

Domain 5: Protection of Information Assets (26%)

Key concepts

- **Classification and ownership:** label data by sensitivity, every data set has a business owner.
- **Physical and environmental controls:** badges, visitor logs, power, cooling, fire suppression. In the cloud, the provider runs the building; review its audit report.
- **Identification, authentication, authorization:** claim who you are, prove it, get what you are allowed. Logs tie actions to one person.
- **MFA, SSO, password managers.** Least privilege and need to know, built with roles.
- **Access lifecycle:** joiner, mover, leaver, periodic access reviews. HR is the source of truth for leavers.
- **Privileged access:** few named admins, separate accounts, sealed break glass account, sessions logged, reviewed more often.
- **Network security:** firewalls, segmentation, VPN, zero trust, separate guest wifi, cloud configuration monitoring.
- **Encryption:** symmetric (one shared key) and asymmetric (a key pair). PKI and certificates. At rest and in transit. Key management is where the risk lives.
- **Endpoints:** MDM, disk encryption, EDR, patching.
- **Logging and monitoring:** SIEM with owned alerts, protected logs, enough retention.
- **Incident response:** prepare, detect, contain, eradicate, recover, learn. Chain of custody for evidence; forensics on copies.

- **Testing:** vulnerability scans (automated, frequent) and penetration tests (a person tries to exploit, yearly or after big changes). Awareness training.
- **Privacy:** collect only what you need, use it for the stated purpose, keep it only as long as needed.

What the exam likes to test

- Leavers who keep access and unreviewed admin accounts are top findings.
- The data owner decides access, not IT.
- Logs that nobody reviews are a finding.
- Encryption is only as strong as key management.

Traps

- **Authentication versus authorization:** the passport proves who you are; the boarding pass says which plane you can board.
- **Scan versus penetration test:** a scan lists known weaknesses; a pen test tries to exploit them.

The auditor mindset

Most hard questions are solved by thinking like an auditor, not a technician.

Principle	What it means on the exam
Risk based	Understand the business and the risk before you test anything. Focus effort where risk is highest.
Independence	Never audit what you designed or run. Disclose any conflict. Advise, but never own a control.
Evidence	Trust what you can verify. System generated, independent and auditor obtained evidence beats verbal answers.
Roles	The auditor reports and recommends. Management decides, fixes and accepts risk.
Root cause	Prefer the answer that fixes the cause over one that fixes a single instance.
Design, then operation	Test that a control could work before testing that it worked all period.

> **Example:** An auditor finds that three leavers still have active accounts in the payroll app. The tempting answer is to disable them yourself. The auditor's answer is to check whether the accounts were used after the leaving date, size the impact, find the cause and report it so management fixes the process.

Practice questions

These 18 questions are original and written for this guide. Answers and explanations follow at the end of the section.

1. An IS auditor is planning the yearly audit plan for internal audit. What should the auditor do FIRST?

- A. Select the systems with the most users
- B. Perform a risk assessment of the audit universe
- C. Repeat last year's plan to keep coverage consistent
- D. Ask IT management which areas they want audited

2. While testing offboarding, the auditor receives a list of 60 leavers from the IT team. What should the auditor do before selecting a sample?

- A. Pick 25 names at random
- B. Increase the sample to the full list
- C. Ask IT to confirm all accounts were removed
- D. Confirm the list is complete by comparing it with HR and payroll records

3. Which evidence is MOST reliable for confirming that MFA is enforced in the identity provider?

- A. The IT manager's written statement
- B. A screenshot attached to a ticket last quarter
- C. The configuration observed by the auditor directly in the admin console
- D. The security policy that requires MFA

4. An internal auditor helped design the new access review process last year. This year, the auditor is assigned to audit it. What is the BEST action?

- A. Disclose the conflict and have another auditor perform the review
- B. Audit it, since the auditor knows the process well
- C. Audit it but mention the involvement in the report appendix
- D. Ask the process owner to approve the assignment

5. Which risk is the auditor able to directly control?

- A. Inherent risk
- B. Control risk
- C. Detection risk
- D. Business risk

6. A company's information security policy has not been reviewed in three years and was approved by the IT manager only. What is the auditor's GREATEST concern?

- A. The policy may be too technical

- B. The policy is not stored in a document management system
- C. Employees may not have acknowledged it
- D. The policy may not reflect current risks and lacks senior management backing

7. A critical SaaS vendor processes customer data. Which is the BEST evidence that the company is managing this vendor?

- A. A signed contract from four years ago
- B. The vendor's marketing page about security
- C. A yearly review of the vendor's SOC 2 Type 2 report, with exceptions and user entity controls followed up
- D. A questionnaire the vendor completed during onboarding

8. Which measure is a key risk indicator rather than a key performance indicator?

- A. Number of critical vulnerabilities open past their deadline, rising for three months
- B. Percentage of tickets closed within SLA
- C. Projects delivered on budget
- D. Help desk customer satisfaction score

9. A team of four engineers deploys to production. Each engineer can merge their own changes. What is the BEST recommendation if adding staff is not possible?

- A. Remove production access from all engineers
- B. Require a second engineer's review on every pull request, enforced by branch protection, and review deploy logs monthly
- C. Accept the risk without documentation
- D. Ask the auditor to approve each change

10. During a data migration to a new billing system, which evidence BEST shows that the migration was complete and accurate?

- A. The project manager's email saying the migration succeeded
- B. The vendor's migration tool documentation
- C. A successful login to the new system
- D. Reconciled record counts and control totals between old and new systems, signed off by the data owner

11. Who should sign off user acceptance testing for a new finance application?

- A. The development lead
- B. The IS auditor
- C. The business users and process owner
- D. The database administrator

12. An automated input control rejects invoices above a set limit. IT general controls over change management are weak. What is the auditor's main concern?

- A. The control's logic could be changed without approval, so a single test does not prove it worked all period
- B. The control may reject valid invoices
- C. Users may find the control annoying
- D. The limit may be too high

13. The policy sets an RPO of 15 minutes for the customer database. Backups run once every night. What is the BEST conclusion?

- A. The control is effective because backups run daily
- B. The backup design cannot meet the RPO, so the recovery capability is inadequate
- C. The RTO must be increased
- D. More restore tests are needed

14. What should be completed FIRST when building a business continuity program?

- A. Disaster recovery plan
- B. Selection of a hot site
- C. Tabletop exercise
- D. Business impact analysis

15. A production configuration was changed on a Friday night to fix an outage. There is no ticket or approval. What should the auditor recommend?

- A. Ban all emergency changes
- B. Revert the change immediately
- C. Allow emergency changes but require documentation and approval after the fact, with monitoring of how often they occur
- D. Remove the engineer's access permanently

16. Who should decide which employees get access to customer financial data?

- A. The data owner in the business
- B. The IT administrator
- C. The IS auditor
- D. The CISO alone

17. Logs from all critical systems are collected in a SIEM, but thousands of alerts remain open and unassigned. What is the GREATEST risk?

- A. Storage costs will rise
- B. Logs may be in the wrong format

- C. The SIEM license may expire
- D. Real attacks may go undetected because alerts are not reviewed

18. Quarterly access reviews are signed off by managers, but the auditor finds that users marked for removal are still active. What does this MOST likely indicate?

- A. The control design is adequate and operating effectively
- B. The review is performed but the removal step does not operate, so the control is not effective
- C. Managers should review monthly instead
- D. The auditor should remove the users

Answers and explanations

Q	Answer	Why
1	B	Risk based planning comes first. Habit, user counts or management wishes do not set audit priorities.
2	D	Validate the population before sampling. A sample from an incomplete list proves nothing.
3	C	Evidence the auditor obtains directly is strongest. A policy shows intent, not operation.
4	A	Auditing your own work breaks independence. Disclose and reassign.
5	C	Detection risk depends on the auditor's procedures, such as sample size and test quality.
6	D	An outdated policy approved at the wrong level is a governance failure, the root problem behind the others.
7	C	Ongoing monitoring with a current independent report shows the company kept accountability.
8	A	A KRI warns that risk is rising. The others measure performance.
9	B	A compensating control keeps segregation of duties in a small team. The auditor never approves changes.
10	D	Reconciliations and owner sign off are evidence; an email is a promise.
11	C	The business confirms the system meets its needs. IT and the auditor do not own acceptance.
12	A	Testing an automated control once relies on effective change controls. Without them, the result cannot be relied on for the whole period.
13	B	RPO drives backup frequency. Nightly backups give roughly 24 hours of possible data loss.
14	D	The BIA sets priorities, RTO and RPO. Plans and sites come after.

Q	Answer	Why
15	C	Emergency changes are allowed, but never without a record and later approval. Too many emergencies is itself a signal.
16	A	The data owner decides access. IT is the custodian that implements it.
17	D	Collecting logs without review gives no detection. Every alert needs an owner.
18	B	The control fails in operation. The auditor reports it and management fixes the removal step.

Glossary

Term	Meaning
Assurance	Confidence others can rely on, based on an independent check
Audit charter	The approved document that gives internal audit its purpose, authority and access
Audit universe	Everything in the organization that could be audited
CAAT	Computer assisted audit technique: software used to test data directly
Compensating control	A second control that reduces the same risk when the main one is weak
Control risk	The chance a control fails to prevent or detect a problem
Detection risk	The chance the auditor's procedures miss a problem
Inherent risk	Risk before any control is considered
Materiality	Whether an issue is significant enough to change a decision
Population	The full set of items a control should have acted on
Test of design	Checking whether a control, if followed, would address the risk
Test of operating effectiveness	Checking whether the control worked consistently over the period
Workpaper	The auditor's record of what was tested, how, and the conclusion
BIA	Business impact analysis: what matters most and how long you can be without it
RTO and RPO	How fast a system must be restored, and how much data loss is acceptable
ITGC	IT general controls: access, change management and operations controls

Next steps

Watch the free CISA Deep Dive full course on YouTube, and find the other free compliance courses on the Taistek channel. If this guide helped you, you can support the channel on Ko-fi.