



Free guide · October 2026

CISA Exam Guide

Certified Information Systems Auditor, set by ISACA. What's tested, how the questions are worded, a study timeline and how to book.

CISA is ISACA's credential for professionals who audit, control, monitor and assess information systems. The exam doesn't reward memorising frameworks. It rewards thinking like a senior, independent IS auditor: risk first, evidence before conclusions, and recommendations rather than fixes.

Questions

150 multiple choice

Time

4 hours (about 96 seconds a question)

Scoring

Scaled 200–800; pass mark 450

Where

PSI test centre or online, remotely proctored

Exam fee

US\$575 ISACA members, US\$760 non-members

Booking window

Book any time; six months to sit it after registering

1 · What's tested

5 domains, their weights and what the examiner looks for

2 · Question wording

The keywords, the traps and a worked example

3 · Study timeline

A 12-week plan, plus a short-on-time version

4 · How to book

Step by step, with fees and exam-day checklist



1 What's tested

ISACA publishes the weight of each domain. Spend your study time in roughly the same proportions.

Domain	Topic	Weight	Questions
1	Information Systems Auditing Process	18%	≈ 27
2	Governance and Management of IT	18%	≈ 27
3	IS Acquisition, Development and Implementation	12%	≈ 18
4	IS Operations and Business Resilience	26%	≈ 39
5	Protection of Information Assets	26%	≈ 39

- 1**
18%

Information Systems Auditing Process

IS audit standards and ethics, risk-based audit planning, types of controls, audit project management, sampling, evidence, data analytics, reporting and follow-up.

What the examiner is really testing: Whether you plan and run an audit the ISACA way: risk-based, evidence-led, independent.
- 2**
18%

Governance and Management of IT

IT governance and strategy, policies and standards, organisational structure, enterprise architecture, risk management, IT resource and vendor management, performance monitoring.

What the examiner is really testing: Whether you see IT as serving business objectives, with the board and senior management accountable.
- 3**
12%

IS Acquisition, Development and Implementation

Business cases and feasibility, project governance, system development methods, control design, testing, configuration and release management, migration, post-implementation review.

What the examiner is really testing: Where the auditor adds value in a project, and which controls must exist before go-live.
- 4**
26%

IS Operations and Business Resilience

IT operations, asset and job management, change, configuration and patch management, problem and incident management, backups, business impact analysis, continuity and disaster recovery (RPO, RTO).

What the examiner is really testing: Whether operations are controlled day to day, and whether the business can recover what matters, as fast as it needs to.
- 5**
26%

Protection of Information Assets

Information security frameworks, privacy, physical and environmental controls, identity and access management, network and endpoint security, encryption and PKI, security monitoring and incident response, evidence collection.

What the examiner is really testing: Whether the right people can reach the right data, and nobody else, and whether breaches are spotted and handled.



2 How the questions are worded

Every question has one best answer, and usually one close distractor that is technically true but wrong for the auditor in the room. The keyword in capitals tells you which kind of “right” the examiner wants.

Keyword	What it's asking
BEST / MOST appropriate	Several options may be true. Pick the one that deals with the biggest risk, fixes the cause rather than the symptom, or is the most complete.
FIRST	A question about order. The auditor understands and evaluates before acting: find out what controls exist, then judge them, then recommend.
PRIMARY / MAIN	Asks why something exists. Choose the core purpose, not a side benefit (a backup exists to recover data, not to save storage).
GREATEST concern / risk	Think business impact. The option that could hurt the organisation's objectives most wins, not the most technical flaw.
MOST LIKELY	The usual, everyday cause or result. Avoid exotic edge cases.
LEAST / NOT / EXCEPT	The question is reversed. Slow down: three options are true and you are hunting the odd one.

Distractors that cost easy marks

- ✗ **The auditor fixes it.** Auditors recommend; management implements. An option where the auditor revokes access, changes a setting or designs the control is usually wrong.
- ✗ **Skipping a step.** Jumping straight to a recommendation or a report before checking compensating controls or confirming the finding.
- ✗ **Too technical.** A deep configuration detail beats a governance-level answer only when the question is clearly technical.
- ✗ **Fixing the symptom.** Correcting one bad transaction instead of the control that let it through.
- ✗ **Absolute words.** Options with “always”, “all” or “never” are rarely the auditor's answer.

Try one

During a review of a new payroll system, an IS auditor finds that two programmers can update programs directly in production. What should the auditor do **FIRST**?

- A. Recommend that the programmers' production access be removed
- B. Find out whether compensating controls exist, such as logging and independent review of changes**
- C. Report the issue to the audit committee
- D. Ask the system administrator to revoke the access

Answer: B. “FIRST” asks about order. Before recommending anything, the auditor must judge the real risk, and that depends on compensating controls. A comes later, C skips management and the facts, and D has the auditor running the fix.



3 A 12-week study timeline

Built for working professionals at about 8–10 hours a week. Domains are ordered so the auditor’s mindset comes first, and the heaviest-weighted areas get the most time.

Week	Focus	What to do
1	Orientation	Read the exam outline. Sit a 50-question diagnostic untimed and note your weakest domains.
2–3	Domain 1	Standards, risk-based planning, sampling, evidence and reporting. This is the lens for every other domain.
4	Domain 2	Governance, strategy, policies, risk and vendor management.
5	Domain 3	Project governance, development methods, testing and implementation controls.
6–7	Domain 4	Operations, change and incident management, backups, BIA, continuity and recovery.
8–9	Domain 5	Access, network, encryption, physical security and incident response.
10	Mixed practice	Mixed sets of 50–100 questions. Keep an error log: why the right answer beat yours.
11	Full mock	At least one full 150-question, 4-hour mock. Review every wrong answer and every guess.
12	Final review	High-yield notes and the error log only. Rest the day before.

Short on time?

Six weeks or less? Spend the first week on Domain 1 and the question keywords, two weeks on Domains 4 and 5 (over half the exam), one on Domains 2 and 3, and the last two on timed mocks and your error log.

Habits that move the score

- ✓ Practise questions from week one, not only at the end.
- ✓ Study little and often: five 90-minute sessions beat one long weekend.
- ✓ Re-read the question’s last line before choosing.
- ✓ Keep an error log: for each miss, write why the right answer beat yours.
- ✓ Time yourself: about 96 seconds a question. Flag and move on.
- ✓ Take your mocks under exam conditions, start to finish.



4 How to book

1

Set up your ISACA account

Create a free account at isaca.org. Membership is optional, but it lowers the exam fee.

2

Register and pay

Register for the CISA exam and pay in full: US\$575 for members, US\$760 for non-members. Registration is open all year.

3

Mind the six-month window

Your eligibility to sit the exam lasts six months from the day you register. Register when you are about 8–10 weeks from ready.

4

Schedule with PSI

In your ISACA account, go to Certification & CPE Management, then Schedule Your Exam, and continue to PSI. Pick a test centre or remote proctoring. You can book from 48 hours after paying, up to 90 days ahead.

5

Check your ID

The name on your ISACA account must match your government-issued ID exactly.

6

Rescheduling

You can reschedule without penalty if you do it at least 48 hours before your appointment, within your eligibility period.

7

After you pass

Apply for certification within five years of passing: a US\$50 processing fee, verified work experience (five years in IS audit, control, assurance or security, with some substitutions allowed), and agreement to ISACA's Code of Professional Ethics and CPE policy.

Exam-day checklist

- ☐ Government ID with the exact name on your account
- ☐ Arrive 30 minutes early, or start remote check-in early
- ☐ For remote exams: a quiet room, clear desk, webcam and a tested connection
- ☐ Know your pace: about 96 seconds a question
- ☐ Flag hard questions and come back; never leave one blank
- ☐ Sleep well the night before. No new topics on exam day.

Free official resources

ISACA CISA exam content outline:

isaca.org/credentialing/cisa/cisa-exam-content-outline

ISACA exam candidate guide:

isaca.org/credentialing/exam-candidate-guides

Go deeper

Free notes, puzzles and practice for CISA at

auditcertdesk.com/cisa, with study packs, flashcards and timed mock exams when you want to go further.

Chidambaram Narayanan, CISA Coach

CISA trainer and mentor, and recipient of the Richard Chambers Internal Audit Beacon Award (2024, 2025). He has coached audit professionals through CISA, CIA and AAIA with one idea: learn how the examiner thinks, then learn the content.

Facts checked October 2026. Fees, formats and rules change, so confirm them with ISACA before you book. CISA and AAIA are trademarks of ISACA. CIA is a registered trademark of The Institute of Internal Auditors. This guide is independent and isn't endorsed by either body. Free to share, unchanged.