Learning with TK

CISA Domain Overview Guide

A concise breakdown of all five CISA domains — key concepts, common exam traps, and recommended resources for each.

Domain 1 | Domain 2 | Domain 3 | Domain 4 | Domain 5

By Tharun Krishna · learningwithtk.com

HOW TO USE THIS GUIDE

This guide is designed as your quick-reference companion — not a replacement for the ISACA CISA Review Manual, but a way to orient yourself in each domain, identify what to focus on, and know where to go deeper.

Each domain section includes: an overview of what the domain covers and why it matters; key concepts distilled to what the exam actually tests; common exam traps — the reasoning errors that cost candidates points; and recommended resources for each domain.

Use this guide at the start of each study phase to preview what's coming, and return to it in your final consolidation weeks to rapidly review where you're strong and where you need to reinforce.

EXAM DOMAIN WEIGHTS AT A GLANCE

Domain	Title	Weight	~Questions
1	IS Auditing Process	**21%**	~32
2	Governance & Mgmt of IT	**17%**	~25
3	Acquisition, Dev & Impl	**12%**	~18
4	Operations & Resilience	**23%**	~34
5	Protection of Info Assets	**27%**	~40

1

Information System Auditing Process

Exam Weight: ~21% · ~32 Questions

DOMAIN OVERVIEW

Domain 1 sets the foundation for everything else on the CISA exam. It defines what IS auditing means, how audit work is planned and executed, and how results are communicated. ISACA expects you to understand the entire audit lifecycle — from scoping and risk-based planning through fieldwork, evidence collection, and final reporting. The audit standards that govern this process come from ISACA's IT Audit and Assurance Standards, which carry significant weight on the exam.

KEY CONCEPTS

Audit Planning & Scope	Risk-based audit planning, defining objectives, audit charter, and scope boundaries.
Audit Standards	ISACA IT Audit Standards, professional ethics, independence, and due professional care.
Types of Audits	Compliance, operational, integrated, and IS audits — know the differences and when each applies.
Evidence & Sampling	Types of audit evidence, reliability hierarchy, and statistical vs. judgmental sampling.
Control Testing	Tests of controls (design effectiveness vs. operating effectiveness), substantive testing.
Audit Reporting	Findings, conclusions, recommendations, management responses, and follow-up procedures.
CAAT / Data Analytics	Computer-Assisted Audit Techniques, audit software tools, data analysis methods.
Risk Assessment	Inherent risk, control risk, detection risk, and overall audit risk model.

COMMON EXAM TRAPS

! ISACA always wants the auditor to assess risk FIRST before planning any audit procedure.

! Independence is non-negotiable — if an auditor has a conflict of interest, the correct action is to disclose or withdraw.

! 'Materiality' in IS auditing is about risk significance, not just financial dollar amounts.

! Audit findings should always be discussed with management BEFORE the final report is issued.

! When asked what to do 'first' on a new audit, the answer is almost always: understand the environment and assess risk.

! Don't confuse 'tests of controls' with 'substantive tests' — ISACA treats these as distinct steps.

RECOMMENDED RESOURCES

- ISACA CISA Review Manual — Chapter 1 (most authoritative source)
- ISACA IT Audit and Assurance Standards Framework (free on ISACA.org)
- Mike Chapple's CISA Study Guide — Domain 1 walkthrough
- ISACA QAE Database — filter by Domain 1 for targeted practice
- Coursera / Udemy CISA courses — Domain 1 video modules (20–30 min overview recommended)

2

Governance and Management of IT

Exam Weight: ~17% · ~25 Questions

DOMAIN OVERVIEW

Domain 2 is where strategy meets accountability. It covers how organizations structure IT governance, align IT strategy with business goals, and ensure that management oversight mechanisms are in place. You need to understand frameworks like COBIT, ITIL, and ISO/IEC 27001, but more importantly, you need to understand why they matter and how an auditor evaluates their effectiveness. Enterprise architecture, IT policies, and investment management also fall under this domain.

KEY CONCEPTS

IT Governance Frameworks	COBIT 2019, ITIL 4, ISO/IEC 38500, TOGAF — know the purpose of each, not implementation details.
IT Strategy & Alignment	Linking IT strategy to business objectives, IT steering committees, and governance structures.
Policies & Procedures	Policy hierarchy (policy → standard → guideline → procedure) and ownership.
IT Investment & Portfolio Mgmt	Business cases, cost-benefit analysis, portfolio rationalization, and value delivery.
Risk Management Frameworks	NIST RMF, ISO 31000 — how risk governance integrates into overall IT management.
Organizational Structures	IT organizational charts, RACI models, segregation of duties at the governance level.
Maturity Models	CMMI, COBIT maturity levels — how auditors assess organizational process maturity.
Performance Monitoring	KPIs, KRIs, IT balanced scorecard, and how governance effectiveness is measured.

COMMON EXAM TRAPS

! COBIT is a governance framework, not an operational IT manual — don't confuse it with ITIL.

! The Board of Directors is responsible for IT governance; management is responsible for IT management. This distinction matters on the exam.

- ! A policy without enforcement is just a suggestion — auditors look for evidence of compliance, not just document existence.
- ! When evaluating IT governance, the auditor's role is to provide assurance, not to redesign the structure.
- ! IT steering committees advise and approve — they don't manage day-to-day IT operations.
- ! Questions about 'risk appetite' and 'risk tolerance' are governance questions, not technical ones.

RECOMMENDED RESOURCES

- ISACA CISA Review Manual — Chapter 2
- COBIT 2019 Framework Overview (free download on ISACA.org — focus on the governance objectives)
- IT Governance Institute publications (available via ISACA member access)
- Hemang Doshi's CISA course — Domain 2 is particularly well-explained
- ISO/IEC 38500 summary articles — a 10-minute read covers what you need for the exam

3

Information Systems Acquisition, Development and Implementa

Exam Weight: ~12% · ~18 Questions

DOMAIN OVERVIEW

Domain 3 covers the full lifecycle of how information systems are acquired, built, tested, and deployed. From requirements definition and vendor selection through change management, testing methodologies, and post-implementation review — this domain tests your understanding of where controls must exist in the development process. Auditors in this domain are evaluating whether adequate governance and controls are embedded throughout the SDLC, not just whether the system works.

KEY CONCEPTS

SDLC Methodologies	Waterfall, Agile, Scrum, spiral — know what controls apply differently under each model.
Requirements & Feasibility	Business, functional, and technical requirements; feasibility studies and business cases.
Project Management Controls	Project governance, change control boards, milestone reviews, risk management in projects.
Acquisition & Vendor Mgmt	RFP process, vendor due diligence, contract provisions (SLAs, audit rights, exit clauses).
Testing Methodologies	Unit, integration, system, UAT, regression, penetration testing — roles and responsibilities.
Change & Release Management	ITIL change management, emergency change procedures, version control, rollback.
Data Conversion & Migration	Data quality controls, reconciliation, parallel run testing, cutover controls.
Post-Implementation Review	Benefits realization, lessons learned, performance vs. baseline, sign-off procedures.

COMMON EXAM TRAPS

! In Agile environments, controls must still exist — just applied differently. ISACA doesn't consider Agile a reason to skip controls.

! The auditor should be involved THROUGHOUT the SDLC, not just at the end during UAT.

- ! Change management applies to all changes — emergency changes must be documented and reviewed after implementation.
- ! User Acceptance Testing (UAT) must be performed by USERS, not developers — this segregation is exam-critical.
- ! Vendor contracts must include audit rights — a contract without them is a red flag ISACA expects you to identify.
- ! A post-implementation review is mandatory best practice, not optional — its absence is always a finding.

RECOMMENDED RESOURCES

- ISACA CISA Review Manual — Chapter 3
- PMBOK Guide (basics only — ISACA-level project management knowledge is sufficient)
- ITIL 4 Foundation concepts — Change Management and Release Management modules
- Simplilearn or Udemy CISA Domain 3 video modules
- ISACA QAE Database — Domain 3 practice questions (pay special attention to SDLC scenario questions)

4 Information Systems Operations and Business Resilience

Exam Weight: ~23% · ~34 Questions

DOMAIN OVERVIEW

Domain 4 is one of the highest-weighted domains and one where many candidates underestimate the depth required. It covers IT service management, infrastructure operations, hardware/software management, and critically — business continuity and disaster recovery. The BCP/DRP section alone is worth mastering deeply, as it generates a significant number of exam questions. The auditor's lens here is always: are these operations running reliably, and can the organization survive disruption?

KEY CONCEPTS

IT Service Management (ITIL)	Incident, problem, change, release, and service desk management — ITIL 4 framework.
Hardware & Software Management	Asset lifecycle, patch management, configuration management database (CMDB).
IT Operations Controls	Job scheduling, output controls, tape/media management, capacity planning, monitoring.
Network & Infrastructure	LAN/WAN, VPN, firewall placement, DMZ architecture, cloud infrastructure auditing.
Business Continuity Planning	BCP lifecycle, BIA, RTO/RPO/MTTR/MTPD definitions and their relationships.
Disaster Recovery Planning	DRP testing types (tabletop, simulation, parallel, full cutover), recovery strategies.
Backup & Recovery	Backup types (full, incremental, differential), offsite storage, restoration testing.
Cloud & Virtualization	IaaS/PaaS/SaaS audit considerations, shared responsibility model, hypervisor controls.

COMMON EXAM TRAPS

! RTO (Recovery Time Objective) is how long you can be DOWN. RPO (Recovery Point Objective) is how much DATA you can lose. Confusing these is extremely common.

! The BIA (Business Impact Analysis) always comes BEFORE developing the BCP/DRP — it identifies what is critical.

- ! A DRP that has never been tested is NOT an effective control — testing evidence is required.
- ! In a disaster, the priority is always: protect life first, then data/systems.
- ! Incremental backups restore FASTER than differential? No — differential is faster to restore; incremental is faster to back up. This is a frequent trap.
- ! The auditor does not design the BCP — the auditor evaluates whether an adequate BCP exists and is maintained.
- ! MTTR (Mean Time to Repair) is different from RTO — don't conflate them in scenario questions.

RECOMMENDED RESOURCES

- ■ ISACA CISA Review Manual — Chapter 4 (BCP/DRP section deserves two full reads)
- ■ NIST SP 800-34 Rev 1 — Contingency Planning Guide (free, highly exam-relevant)
- ■ ITIL 4 Foundation — Service Operation and Continual Improvement modules
- ■ YouTube: 'BCP vs DRP explained' — multiple 10-min videos cover the distinctions clearly
- ■ ISACA QAE Database — Domain 4 has the most practice questions; drill BCP/DRP subset extensively

5

Protection of Information Assets

Exam Weight: ~27% · ~40 Questions

DOMAIN OVERVIEW

Domain 5 carries the highest exam weight of all five domains and covers information security in its broadest sense — from classification and access control through cryptography, network security, vulnerability management, and incident response. While it overlaps in places with CISSP or CISM material, the CISA lens is always audit-focused: not 'how do you implement encryption?' but 'how does an auditor evaluate whether encryption controls are adequate?' Understanding controls and their objectives is more important than deep technical implementation knowledge.

KEY CONCEPTS

Information Classification	Data classification schemes, labeling requirements, handling procedures, and ownership.
Access Control	Logical access controls, IAM, RBAC/ABAC, privileged access management (PAM), access reviews.
Cryptography	Symmetric vs. asymmetric, PKI, digital signatures, hashing — know the audit implications of each.
Network Security Controls	Firewalls, IDS/IPS, SIEM, DLP, WAF — audit evaluation, not technical implementation.
Endpoint & Application Security	Patch management, hardening, application security controls, mobile device management.
Vulnerability & Penetration Testing	VA scanning vs. pen testing, remediation tracking, risk-based prioritization.
Incident Response	IR lifecycle (prepare, identify, contain, eradicate, recover, lessons learned), ISACA's role of auditor in IR.
Physical & Environmental Security	Data center controls, access logs, CCTV, environmental sensors, visitor management.

COMMON EXAM TRAPS

! Preventive controls are ALWAYS preferable to detective or corrective controls — if prevention fails, detection is next.

- ! Separation of duties and least privilege are both critical — the exam often tests scenarios where one or both are violated.
- ! Encryption protects confidentiality and integrity. It does NOT by itself guarantee availability.
- ! An IDS detects and alerts. An IPS detects AND blocks. Know the difference — it changes the answer in many scenario questions.
- ! Access reviews must happen PERIODICALLY, not just at hire — exam questions will often ask who is responsible for conducting them (the data owner, not IT).
- ! Multi-factor authentication is stronger than strong passwords alone — but ISACA will test the scenario where MFA is not feasible.
- ! Security incidents must be DOCUMENTED even when resolved quickly — lack of incident logs is always an audit finding.
- ! Physical security is not optional. The exam includes questions where the right answer is a physical control, not a technical one.

RECOMMENDED RESOURCES

- ISACA CISA Review Manual — Chapter 5 (highest priority chapter; reread weak sections twice)
- NIST Cybersecurity Framework (CSF) overview — free on NIST.gov; aligns well with Domain 5 topics
- ISO/IEC 27001 & 27002 control summaries — ISACA expects familiarity with this standard
- SANS Reading Room — free security whitepapers relevant to access control, cryptography, IR
- ISACA QAE Database — Domain 5 largest question pool; aim for 400+ practice questions in this domain alone
- Professor Messer (CompTIA Security+ material) — useful primer on cryptography and network security fundamentals

Ready to go deeper?

This guide is just the beginning. The CISA exam rewards candidates who combine broad domain knowledge with deep understanding of auditor reasoning.

At Learning with TK, you'll find structured courses, domain-specific practice question sets, and guided study plans built for both students and working professionals.

Browse CISA Courses

Book a Free Strategy Call

learningwithtk.com