

THREATNEXIS

CYBERSECURITY CERTIFICATION ACADEMY

CompTIA Security+

SY0-701 Certification Track

ISACA CISM

Certified Information Security
Manager Track

FREE TRACK GUIDE

Domain Overviews • Core Concepts • Memory Tricks • Exam Tips • Study Strategy

Welcome to Your Certification Journey

This guide covers two of the most impactful certifications in cybersecurity today:

CompTIA Security+

Your entry point into professional cybersecurity. The most widely-recognized baseline security certification worldwide, trusted by the DoD, major enterprises, and government agencies.

Best For: IT pros, help desk, admins moving into security

ISACA CISM

Your leadership credential in information security management. The CISM signals you can manage, design, and oversee an enterprise information security program — not just execute tasks.

Best For: Security managers, CISOs, GRC professionals

PART 1: CompTIA Security+

SY0-701 | The Foundation of Your Security Career

Overview

Think of Security+ as your security driver's license. You wouldn't hand someone the keys to a race car without first confirming they know the rules of the road. Security+ confirms you know the rules of the cybersecurity road.

Exam Code	SY0-701
-----------	---------

Questions	Up to 90 (multiple choice + performance-based)
Duration	90 minutes
Passing Score	750 out of 900
Experience Rec.	Network+ and 2 years IT with security focus (recommended, not required)
Validity	3 years (renew via CE credits or re-exam)
Cost	~\$392 USD

Why Security+ Matters

Real-World Impact

Security+ is DoD 8570/8140 compliant, meaning it is required for thousands of U.S. government and defense contractor roles. It is also one of the most commonly requested certifications in entry-to-mid-level security job postings globally.

From a hiring manager's perspective, Security+ is shorthand for: 'This person understands security fundamentals and speaks the language.'

The Five Exam Domains

The SY0-701 exam is built around five domains. Think of them as five rooms in a house — you need to know every room, but some rooms are bigger than others.

Domain	Topic	Weight
1.0	General Security Concepts	12%
2.0	Threats, Vulnerabilities & Mitigations	22%
3.0	Security Architecture	18%
4.0	Security Operations	28%
5.0	Security Program Management & Oversight	20%

Domain 1.0 — General Security Concepts (12%)

The Lay of the Land

This domain is your foundation. Before you can defend anything, you need to know what you're defending against and the language everyone uses to talk about it.

Key Concepts You Must Know

- Security Controls — Preventive, Detective, Corrective, Compensating, Directive

- The CIA Triad — Confidentiality, Integrity, Availability
- Non-repudiation — proving someone did what they said they did
- Authentication, Authorization, and Accounting (AAA)
- Public Key Infrastructure (PKI) fundamentals
- Cryptography basics — symmetric vs asymmetric
- Zero Trust Architecture principles

Memory Anchor

THE CIA TRIAD ANALOGY: Think of a bank vault. Confidentiality = only authorized people see what's inside. Integrity = the money hasn't been tampered with. Availability = you can access it when you need it. Every security control you'll ever learn maps back to one or more of these three.

Mnemonic: Security Control Categories

Remember "PPT-DCC" for control types:

- P — Preventive (stops the attack)
- P — Physical (locks, guards, cameras)
- T — Technical (firewalls, AV, encryption)
- D — Detective (IDS, logs, audits)
- C — Corrective (patches, backups, restore)
- C — Compensating (alternative when primary can't be used)

Domain 2.0 — Threats, Vulnerabilities & Mitigations (22%)

Know Your Enemy

This is the largest attack-focused domain. The exam will throw threat actor scenarios at you and expect you to identify the attack type, the vector, and the best mitigation.

Threat Actor Types — Know These Cold

Threat Actor	Motivation	Sophistication
Nation-State	Espionage, sabotage	Very High (APT)
Organized Crime	Financial gain	High
Hacktivist	Political/social cause	Moderate
Insider Threat	Revenge, money, accident	Varies
Script Kiddie	Fun, notoriety	Low
Shadow IT	Convenience	Low (but risky)

Attack Types You Must Recognize

- Social Engineering: Phishing, Vishing, Smishing, Whaling, BEC
- Malware: Ransomware, RAT, Trojan, Worm, Virus, Spyware, Rootkit

- Network Attacks: DoS/DDoS, Man-in-the-Middle, DNS Poisoning, ARP Spoofing
- Password Attacks: Brute Force, Dictionary, Rainbow Table, Credential Stuffing
- Application Attacks: SQL Injection, XSS, CSRF, Directory Traversal
- Cryptographic Attacks: Birthday, Downgrade, Side-Channel

Exam Warning

EXAM TRAP: The exam loves to mix up attack types. A phishing email that uses urgency and authority is social engineering. The same email delivering a malicious attachment is also a malware delivery vector. Know the overlap.

Domain 3.0 — Security Architecture (18%)

How Secure Systems Are Built

Architecture is about the big picture. This domain asks: how do you design systems, networks, and environments so security is baked in — not bolted on?

Core Architecture Concepts

- Cloud Models: IaaS, PaaS, SaaS — and what YOU are responsible for in each
- Network Segmentation: VLANs, DMZ, Microsegmentation
- Zero Trust: Never trust, always verify — even inside the network
- Secure by Design: Defense in Depth, Least Privilege, Fail Secure
- Infrastructure as Code (IaC) and automation risks
- Virtualization and Container Security

Shared Responsibility Model — Cloud Must-Know

One of the most tested Security+ topics is understanding who is responsible for what in cloud environments.

Model	Provider Responsible For	You Responsible For
IaaS	Physical, network, hypervisor	OS, middleware, apps, data
PaaS	Physical, network, OS, middleware	Apps, data
SaaS	Everything except config & data	Data, access management, config

Domain 4.0 — Security Operations (28%) — THE HEAVYWEIGHT

Where Security Gets Done

With 28% of the exam, this is your highest-value domain. It covers the day-to-day operational security work: monitoring, incident response, identity management, and tooling.

Incident Response Phases — PICERL

PICERL Mnemonic

P — Preparation | I — Identification | C — Containment | E — Eradication | R — Recovery | L — Lessons Learned
Memory phrase: 'Professionals In Cybersecurity Eradicate, Recover, and Learn'

Identity and Access Management (IAM) Essentials

- MFA: Something you know + have + are
- SSO: One login for many systems
- PAM: Privileged Access Management — protect admin accounts
- Federation: Trust between organizations (SAML, OAuth, OIDC)
- RBAC vs ABAC vs DAC vs MAC — know the differences

Security Tooling You Must Know

Tool/Technology	Primary Purpose
SIEM	Aggregate and correlate security logs and events
SOAR	Automate response playbooks
EDR	Endpoint detection, investigation, and response
IDS/IPS	Detect and/or prevent intrusions on the network
DLP	Prevent sensitive data from leaving the organization
CASB	Security policy enforcement for cloud applications
WAF	Protect web applications from Layer 7 attacks

Domain 5.0 — Security Program Management & Oversight (20%)**The Manager's Lens**

This domain shifts from technical to managerial. It's about governance, risk, compliance, and how security programs are built and measured. Even as a technical candidate, you need to think like a manager here.

Key Governance Concepts

- Policies, Standards, Procedures, Guidelines — hierarchy matters
- Risk Management: Identify → Assess → Treat → Monitor
- Risk Treatment Options: Accept, Avoid, Transfer, Mitigate
- Compliance Frameworks: NIST CSF, ISO 27001, PCI DSS, HIPAA, SOX
- Data Classification: Public, Internal, Confidential, Restricted
- Privacy regulations: GDPR, CCPA — know the concepts, not every clause

Mnemonic: Risk Treatment — MATT

MATT Mnemonic

M — Mitigate (reduce the risk) A — Accept (live with it) T — Transfer (insurance, contracts) T — Terminate/Avoid (stop doing the risky thing) Or think: 'Managers Always Take Time' to manage risk properly.

Security+ Exam Strategy

The Manager Mindset Trap

Security+ is primarily a technical exam, but Domain 5 questions require you to think at the management level. When a Domain 5 question asks what to do after a breach, the answer is rarely 'call the FBI first.' It's 'contain the incident, then notify according to your IR plan.'

Performance-Based Questions (PBQs)

PBQs appear at the start of the exam. They ask you to drag, drop, configure, or analyze. Best strategy: flag them, skip to the multiple-choice questions, then return. PBQs take longer and your confidence from the MC questions will help.

Keyword Recognition

When You See...	Think...
MOST important / BEST action	Risk-based priority thinking
FIRST step	IR phases — Preparation or Identification
Prevent vs. Detect	IPS = prevent IDS = detect
Data at rest	Encryption (AES, BitLocker, FileVault)
Data in transit	TLS, IPsec, HTTPS
Non-repudiation	Digital signatures
Least privilege	Minimum access needed to do the job

Security+ Quick Review Checklist

Use this checklist to gauge your readiness. If you can't answer a category confidently, prioritize it in your studies.

Topic Area	Can I explain this?	Priority
CIA Triad and security control types	Yes / No	HIGH
All major threat actor types	Yes / No	HIGH
Phishing, vishing, smishing differences	Yes / No	HIGH
Malware types and behaviors	Yes / No	HIGH
Cloud shared responsibility model	Yes / No	HIGH

Incident Response phases (PICERL)	Yes / No	HIGH
MFA, SSO, RBAC, ABAC explained	Yes / No	HIGH
SIEM vs SOAR vs EDR vs IDS/IPS	Yes / No	MEDIUM
Risk treatment options (MATT)	Yes / No	MEDIUM
Governance hierarchy (policy → procedure)	Yes / No	MEDIUM

PART 2: ISACA CISM

Certified Information Security Manager | The Leadership Credential

Overview

If Security+ is the driver's license, CISM is your commercial pilot certificate. It says you don't just know how to drive — you can plan the route, manage the crew, and handle emergencies at 30,000 feet. CISM is specifically designed for information security managers and those who manage, design, and assess enterprise information security programs. It is one of the most respected credentials globally for security leadership.

Exam Questions	150 multiple choice questions
Duration	4 hours
Passing Score	450 out of 800
Experience Req.	5 years InfoSec work experience (with substitutions allowed)
Validity	3 years (120 CPE credits over 3 years)
Cost	~\$575 (member) / \$760 (non-member)
Offered By	ISACA

Career Impact

CISM is consistently ranked among the top 5 highest-paying IT certifications in the world. Holders average \$120,000–\$160,000+ USD annually in the U.S. It is the gold standard for security management roles.

The Four CISM Domains

CISM has four domains, each representing a pillar of information security management. Notice that Domain 1 carries the most weight — this signals what ISACA considers most important.

Domain	Topic	Weight
1	Information Security Governance	17%
2	Information Security Risk Management	20%
3	Information Security Program	33%
4	Incident Management	30%

Domain 1 — Information Security Governance (17%)

Security Starts at the Top

Governance is about establishing and maintaining the framework that ensures information security strategies align with organizational goals. This is the 'why are we doing this' domain.

If you've been heads-down in technical work, this domain requires a mental shift. Governance asks: Is security aligned to the business? Are we accountable? Are we consistent?

Core Governance Concepts

- Security strategy must align to business strategy — not the other way around
- The CISO's role: advise, design, oversee — not just implement
- Governance frameworks: COBIT, ISO 27001, NIST CSF
- Policies flow down: Policy → Standard → Procedure → Guideline
- Roles: Board, C-Suite, CISO, Security Team, End Users
- Metrics and KPIs: measure what matters

The CISM Mindset

CISM PHILOSOPHY: Security is a business enabler, not just a cost center. Every answer that aligns security to business objectives scores points on the CISM. When in doubt, pick the answer that supports the business mission.

Domain 2 — Information Security Risk Management (20%)

Managing Risk, Not Eliminating It

Here's the truth that every CISM candidate must internalize: you cannot eliminate all risk. Your job as a security manager is to ensure risk is understood, measured, and managed to an acceptable level.

The Risk Management Lifecycle

1. Identify assets and threats
2. Assess likelihood and impact
3. Analyze risk (qualitative vs quantitative)
4. Determine risk response strategy
5. Implement controls
6. Monitor and report residual risk

Key Risk Concepts

Term	Definition
Risk	Likelihood × Impact — the combination of a threat exploiting a vulnerability
Threat	A potential event that could harm an asset
Vulnerability	A weakness that can be exploited by a threat
Exposure	The degree to which an asset is open to harm

Residual Risk	Risk that remains AFTER controls are applied
Inherent Risk	Risk that exists BEFORE controls are applied
Risk Appetite	How much risk the organization is WILLING to accept
Risk Tolerance	The acceptable variance around the risk appetite

Risk Treatment Options — TAME

TAME Mnemonic

T — Transfer (insurance, contracts, outsourcing) A — Accept (acknowledge and live with the risk) M — Mitigate (implement controls to reduce) E — Eliminate/Avoid (stop the risky activity entirely) Remember: CISM always asks for the MOST appropriate treatment given the scenario.

Domain 3 — Information Security Program (33%) — THE BIG ONE

Building and Running the Program

This is the largest CISM domain and the heart of the certification. If Domains 1 and 2 are the strategy and the risk picture, Domain 3 is how you execute. Building a security program means creating the infrastructure — people, processes, and technology — that delivers security outcomes.

Security Program Components

- Security policies and standards — the rules everyone plays by
- Security architecture — how controls are designed and deployed
- Security awareness training — humans are your biggest vulnerability
- Third-party/vendor risk management — your risk extends to your supply chain
- Technical controls integration — firewalls, IAM, encryption, monitoring
- Program metrics — if you can't measure it, you can't manage it

Controls Framework

Security managers work from frameworks, not intuition. Know these:

- NIST Cybersecurity Framework (CSF): Identify → Protect → Detect → Respond → Recover
- ISO/IEC 27001: ISMS standard — management-driven, internationally recognized
- CIS Controls: Prioritized, practical implementation controls
- COBIT: Governance and management of enterprise IT

NIST CSF Memory Map

NIST CSF ANALOGY: Think of NIST CSF as the security manager's daily planner. • Identify = Know what you have • Protect = Lock it up • Detect = Watch for trouble • Respond = Fight the fire • Recover = Clean up and learn Every security activity you do maps to one of these five functions.

Security Awareness — Never Underestimate People

The CISM exam consistently tests your understanding that people are both the greatest asset and the greatest vulnerability. A world-class technical security program can be undone by one employee clicking a phishing link.

- Training must be role-based — executives get different training than help desk
- Phishing simulations are your early warning system
- Security culture starts at the top — leadership must model behavior
- Measure training effectiveness — not just completion rates

Domain 4 — Incident Management (30%)

When Things Go Wrong

Incident management is not just about technical response. From a CISM perspective, it's about having the plan, the team, the communication strategy, and the lessons-learned process ready before the incident happens.

Incident Management Lifecycle

Phase	Key Activities	CISM Focus
Preparation	Plans, playbooks, team structure, training	Have this BEFORE an incident
Detection	Monitoring, alerting, initial triage	SIEM, SOC, user reports
Classification	Severity rating, impact assessment	Business impact lens
Containment	Isolate affected systems, stop the bleeding	Short-term vs. long-term
Eradication	Remove threat, close vulnerability	Root cause analysis
Recovery	Restore systems, validate, monitor	Business continuity focus
Post-Incident	Lessons learned, reporting, process improvement	MOST important for CISM

Key CISM Incident Concepts

- BCP vs DRP: BCP = keeps the business running | DRP = recovers IT systems
- RTO (Recovery Time Objective): Maximum acceptable downtime
- RPO (Recovery Point Objective): Maximum acceptable data loss (measured in time)
- Communication plan: Who do you tell? When? What do you say?
- Forensics: Preserve evidence, maintain chain of custody
- Post-incident review: always improve the process

Pattern Alert

CISM EXAM PATTERN: On incident questions, the exam almost always rewards preparation and communication over technical heroics. The correct answer is usually 'refer to the incident response plan' or 'notify stakeholders according to the communication plan' — not the most

technically impressive option.

CISM Exam Strategy

Think Like a Manager, Not a Technician

This is the #1 CISM coaching insight. The exam is intentionally written for security managers. If you approach every question with 'what would a CISO say at a board meeting?' you will eliminate many wrong answers immediately.

The Business Alignment Rule

When two answers both seem reasonable, pick the one that better aligns security to business objectives. CISM is about enabling the business safely — not locking it down completely.

Common Question Pattern	CISM Answer Bias
What should the CISO do FIRST?	Align with business leadership / assess risk
Best way to get executive buy-in?	Show business impact, not technical details
Most important program component?	Policies that align to business objectives
CISO's primary responsibility?	Protect information assets, enable business
Incident occurred — first step?	Follow the IR plan / contain and communicate

CISM Quick Review Checklist

Topic Area	Confident?	Priority
Security strategy aligns to business strategy	Yes / No	HIGH
Governance frameworks (COBIT, ISO 27001, NIST CSF)	Yes / No	HIGH
Risk: inherent, residual, appetite, tolerance	Yes / No	HIGH
Risk treatment options (TAME)	Yes / No	HIGH
NIST CSF five functions	Yes / No	HIGH
Security program components	Yes / No	HIGH
BCP vs DRP RTO vs RPO	Yes / No	HIGH
Incident management lifecycle phases	Yes / No	MEDIUM
Security awareness program components	Yes / No	MEDIUM
Metrics and KPIs for security programs	Yes / No	MEDIUM

Security+ vs. CISM: Head-to-Head

Many cybersecurity professionals pursue Security+ first to build technical credentials, then CISM as they move into management. Here's how they compare:

Category	CompTIA Security+	ISACA CISM
Focus	Technical security knowledge	Security management & strategy
Audience	Entry/mid-level practitioners	Managers, directors, CISOs
Experience	2 yrs recommended (not required)	5 yrs required
Domains	5 domains	4 domains
Questions	Up to 90	150
Duration	90 minutes	4 hours
Thinking Style	Technical execution	Business risk management
Career Stage	Early to mid career	Mid to senior career
Avg. Salary	\$70k–\$95k	\$120k–\$160k+

Recommended Study Approach

Security+: 60-Day Plan (High Level)

Week	Focus Areas	Daily Time
Weeks 1–2	Domains 1 & 2: Concepts + Threats	1–1.5 hours
Weeks 3–4	Domain 3: Architecture	1–1.5 hours
Weeks 5–6	Domain 4: Operations (heaviest domain)	1.5–2 hours
Week 7	Domain 5: Governance + Risk	1–1.5 hours
Week 8	Full review, practice exams, PBQs	2 hours

CISM: 90-Day Plan (High Level)

Week	Focus Areas	Daily Time
Weeks 1–2	Domain 1: Governance concepts and frameworks	1.5 hours
Weeks 3–4	Domain 2: Risk management lifecycle	1.5 hours
Weeks 5–7	Domain 3: Security program (heaviest domain)	1.5–2 hours
Weeks 8–9	Domain 4: Incident management lifecycle	1.5 hours
Weeks 10–11	Cross-domain practice questions	2 hours
Week 12	Full review + simulated exam	2–2.5 hours

Continue Your Certification Journey

Upgrade to the Premium Threatnexus Toolkit

Want deeper mastery? The free version gave you the foundation. The Premium Threatnexus Toolkit goes all the way:

What's Inside Premium

- Complete domain mastery guides (50–200 pages per cert)
- Full mind maps and visual memory systems
- 500+ scenario-based practice questions
- Flashcard decks for every domain
- Advanced mnemonics and memory palace systems
- Cross-domain relationship maps
- 30/60/90-day study planners
- Rapid review sheets for exam week
- Exam strategy coaching guides
- Framework comparison maps (NIST, ISO, COBIT, CIS)

Coaching Options

- One-on-one tutoring sessions
- Custom study plans built for you
- Domain deep-dive review sessions
- Practice question analysis
- Exam readiness assessments
- Accountability check-ins
- Post-exam debrief if needed

Threatnexus Insider Community — Subscribe Free

JOIN THE COMMUNITY: Subscribe to the Threatnexus Insider Newsletter — free weekly study tips, memory tricks, cheat sheets, practice questions, and exam strategies.
threatnexus.com/newsletter

© Threatnexus Cybersecurity Academy | Teach with Clarity. Teach with Empathy. Teach with Purpose.