No. 146

CERTIFICATION GUIDE

ISACA CISM Study Guide

A plain-language guide to the 2026 CISM exam content outline

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 146

ISACA CISM Study Guide

A plain-language guide to the 2026 CISM exam content outline

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

ISACA CISM Study Guide

A plain-language guide to the 2026 CISM exam content outline

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. ISACA and CISM are trademarks of ISACA. This guide is independent and is not affiliated with, sponsored by or endorsed by ISACA. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this guide 1

PART I · THE CERTIFICATION

1 What CISM is 4
2 The 2026 update 5
3 Requirements 6
4 Exam format 7
5 The CISM mindset 8
6 Ethics 9
7 Maintaining CISM 10
8 A study plan 11

PART II · GOVERNANCE AND RISK

9 Domain 1: governance 13
10 Culture and structure 14
11 Roles and responsibilities 15
12 Security strategy 16
13 Policies, standards and frameworks 17
14 Legal and regulatory requirements 18
15 Domain 2: risk management 19
16 Risk assessment 20
17 Risk treatment 21
18 Risk ownership 22
19 Monitoring and reporting 23
20 Third-party and emerging risks 25

PART III · PROGRAM AND INCIDENTS

21 Domain 3: the security program 27
22 Enterprise and security architecture 28
23 Resources 29

FREE SAMPLE · ojayo.com

24 Controls 30
25 Awareness and training 31
26 Managing external services 32
27 Metrics and reporting 33
28 Domain 4: incident management 34
29 The incident response plan 35
30 Continuity and recovery 36
31 Testing plans 37
32 Managing an incident 38
33 Post-incident review 39

PART IV · EXAM SUCCESS

34 Practice questions 41
35 Answers 43
36 Exam strategy 44
37 Exam day 45
38 After you pass 46
39 Common mistakes 47
40 Next steps 48
Checklists 49
Glossary 50
Further reading 51

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this guide

What this guide covers, who it is for, and how to use it.

CISM (Certified Information Security Manager) from ISACA is a leading certification for people who manage, design and oversee enterprise information security programmes. It focuses on governance, risk, programme management and incident management rather than hands-on technology.

This guide explains CISM in plain language. It covers the experience requirements and exam format, then each of the four domains with diagrams, the management mindset the exam rewards, a study plan, original practice questions and exam-day advice. It reflects ISACA's updated exam content outline, which took effect on **November 3, 2026**.

What this guide is, and is not

- An independent study companion written in its own words.
- **Not** official ISACA material; it does not reproduce exam questions or the official outline.
- Use ISACA's exam content outline and official review materials as your checklist.

Who this guide is for

- **Security managers** and aspiring CISOs.
- **Security professionals** moving into leadership.
- **GRC professionals** wanting a management credential.

FREE SAMPLE · ojayo.com

How the guide is organized

- **Part I — The certification** (Chapters 1–8): what CISM is, the 2026 update, requirements, exam format, the mindset, ethics, maintenance and a study plan.
- **Part II — Governance and risk** (Chapters 9–20): Domains 1 and 2.
- **Part III — Program and incidents** (Chapters 21–33): Domains 3 and 4.
- **Part IV — Exam success** (Chapters 34–40): practice questions, exam strategy and next steps.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical study and exam advice.

IN PRACTICE
How a concept looks in a real job.

WATCH OUT
Common traps and misunderstandings.

KEY IDEA
The one thing to remember from a section.

A note on screens

Screens are **illustrations**, not real ISACA exam screens or product screens.

FREE SAMPLE · ojayo.com

PART I

The certification

These chapters explain what CISM is, what changed in 2026 and how to prepare.

FREE SAMPLE · ojayo.com

CHAPTER 1

What CISM is

A management certification.

A definition

CISM validates the ability to govern, build and manage an information security programme that supports business objectives, manages risk and responds to incidents.

Not a technical exam

CISM rarely asks how a technology works. It asks what a security manager should do, in what order, and why.

KEY IDEA

CISM is about aligning security with the business.

FREE SAMPLE · ojayo.com

CHAPTER 2

The 2026 update

The November 2026 update.

Domain	Before Nov 3, 2026	From Nov 3, 2026
1 Information Security Governance	17%	18%
2 Information Security Risk Management	20%	20%
3 Information Security Program	33%	33%
4 Incident Management	30%	29%

Figure 2.1 CISM domains and weights

What changed

ISACA kept the four domains, placed greater emphasis on security strategy and programme development, and added two content areas: **enterprise architecture** and **information security architecture**. Updated preparation materials were released on September 1, 2026.

FREE SAMPLE · ojayo.com

CHAPTER 3

Requirements

Experience is required.



Figure 3.1 The path to CISM

Experience

ISACA requires five years of information security work experience, including three years in information security management across several of the domains. Some waivers exist. You can pass the exam first and apply once you meet the requirement, within ISACA's time limits. Check the current rules on ISACA's website.

FREE SAMPLE · ojayo.com

CHAPTER 4

Exam format

The exam.

- **Questions**: 150 multiple choice.
- **Time**: 4 hours.
- **Scoring**: scaled from 200 to 800; 450 or higher passes.
- **Delivery**: test centre or remote proctoring.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide (you are reading this)
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

ISACA CISM Study Guide

Enjoyed it? The full book has 56 pages and 40 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.