ISACA CISM – Certified Information Security Manager 2025

This ISACA Certified Information Security Manager (CISM) training prepares professionals for modern challenges in governance, risk, and incident response. Designed for roles like Information Security Manager or GRC Lead, this course covers high-impact skills like threat modeling, risk treatment, and post-incident review. It's perfect prep for the CISM exam or recertification.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Creating An Information Security Program

Organizational Culture

Security Governance

The Importance of Strategy

Information Security Frameworks

Strategic Objectives

Business Model for Information Security (BMIS)

Validation

IS Program Resources

Introduction

The P3

Standards, Guidelines and Architecture

Controls, Metrics and Assets

Risk Ledgers, Vulnerability Assessments and Insurance

Critical Data, BIA's and BC/DR Planning

Incident Logs and Audits

Information Security Training, 3rd Party Risk and LCR Requirements

Validation

Creating A Successful IS Program

Introduction

Creating A Business Case

Communications and Reporting

How To Communicate Technical Information

WEEK 2

Commitment From Management

End User Information Security Training

Causes Of Failure To Avoid

Validation

Organizational Roles and Using Metrics

Introduction

Organization Level Roles

Roles Pertaining To Our Data

The World of Metrics

Metrics Scenario 1

Metrics Scenario 2

Have We Achieved Success

DAD Triad

Validation

Introduction To Risk Management

Introduction

The Role of Risk Managent

Risk Management Frameworks

Risk Management Strategy

Analyzing Risk

Risk Analysis Techniques

Dealing With Risk

WEEK 3

Validation

Risk Management Frameworks and Processes

Introduction

Risk Management Activities

NIST SP 800-39

NIST SP 800-30

ISO/IEC 27005

Factor Analysis of Information Risk (FAIR)

Risk Management Walk-Through

Validation

Managing Assets and Threats

Introduction

Hardware, Software and Information Assets

Cloud and Virtual Assets

Asset Information and Classification

Identifying Threats To Assets

Identifying Asset Vulnerabilities

Bonus Nugget

Validation

Information Security Risk Management

Introduction

Risk Management Objectives Pt.1

Risk Management Objectives Pt.2

Third Party Risk Management Pt.1

WEEK 4

Third Party Risk Management Pt.2

The Risk Register

Integrating Risk Management Into Other Processes

Risk Monitoring and Reporting

Validation

Introduction

Building Blocks Of An Information Security Program

Information Security Program Details

Information Security Architecture

Security Program Management

Security Policies

Working With Resources

Validation

Information Security Operations

Introduction

Security Operations Centers (SOCs)

Vulnerability and Patch Management

Protecting Networks Pt.1

Protecting Networks Pt.2

Content Filtering Solutions

Endpoint Protection and Management

Validation

Managing An Information Security Program

Introduction

Secure Software Development

WEEK 5

Identity & Access Management (IAM)

Security Awareness Training and MSSPs

Data Backup and Recovery

Financial and Capacity Management

Validation

Implementing and Managing Security Controls

Introduction

Security Controls

Categories Of Security Controls

Security Control Functions

Testing Security Controls

Security Control Objectives and Frameworks

Designing Security Controls

Key Performance Indicators (KPIs)

Validation

The Incident Response Process

Introduction

Phases Of Incident Response

Incident Response Preparation

Incident Response Planning

Detection, Initiation and Evaluation Of Incidents

Containment, Eradication and Recovery

Post Incident Activities

Incident Response Resources

Validation

BC/DR Planning and Standards

Introduction

BC and DR Planning (BCDR)

The BCDR Planning Process

Creating a BC Plan

WEEK 6

DR Planning

Resiliency Technologies

BCDR Testing

BCDR Resources

Validation

Last updated 6.26.2025