ISACA CRISC – Certified in Risk and Information Systems Control

This Certified in Risk and Information Systems Control (CRISC) training is used to prepare for the CRISC certification exam. Learn how to identify and manage enterprise IT risk by identifying, implementing and maintaining information systems controls that effectively deter and prevent intrusions.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Organizational Governance

Security Governance

Information Security Strategy

Identifying and Managing Strategic Objectives

Organizational Roles and Structure

Risk Culture

Security Program Resources

Overview

Policies, Processes, and Procedures

Standards, Guidelines, and Architecture

Controls, Metrics, and Assets

Risk Ledgers, Vulnerability Assessments, and Insurance oh my!

Critical Data, BIA's, and BC/DR Planning

Incident Logs, Audits, & Culture

Security Training, Third Party Risk, & LCR Requirements

Risk Governance

Overview

Risk Management Standards and Frameworks

Three Lines of Defense

Risk Profile

Risk Appetite, Tolerance and Capacity

Legal Concerns and Ethics

WEEK 2

Risk and Threat Identification

Overview

Risk Events

Risk Analysis

Risk Identification

Risk Management Workflow

Threat Landscape

Threat Modeling

Vulnerability Analysis and Risk Scenario Development

Overview

Vulnerability Analysis

Cloud Computing Vulnerabilities

Big Data

Vulnerability Assessment and Penetration Testing

Risk Scenario Development

Risk Scenario Tools

IT Risk Analysis and Evaluation

Overview

IT Risk

Risk Assessment Techniques and Reporting

Risk Register

Risk Analysis Methodologies

WEEK 3

Business Impact Analysis

Continuity Objectives

Types of Risk

Risk Response

Overview

Key Points To Risk Response

Risk and Control Ownership

Risk Response

3rd Party Risk Management

Managing Issues and Exceptions

Managing Emerging Risk

Control Design and Implementation

Overview

Security Controls

Security Control Categories

Security Control Functions

Control Objectives and Frameworks

Control Implementation

Control Testing

Risk Monitoring and Reporting

Don't show this next time.

Risk Treatment Plans

Working With Risk Data

WEEK 4

Data Sources

Risk and Control Monitoring Techniques

Risk and Control Reporting Techniques

Key Performance Indicators (KPIs)

Key Risk Indicators (KRIs)

Key Control Indicators (KCIs)

Network and Endpoint Security

Overview

Discovering Networking Basics

Exploring the OSI Model

Digging into LANs

Discussing LAN Cabling

Reviewing LAN Considerations

Exploring WANs

Discussing Network Management

Examining Network Infrastructure Security

Exploring Firewalls

Business Application Security

Overview

Touring Telephony Applications

Reviewing Network-Based Applications

Exploring Cloud Computing Basics

Discussing Cloud Computing Risks

Examining Virtualization Basics

Managing Mobile Device Security

WEEK 5

Reviewing Wireless Networks

Identifying Internet of Things (IoT)

Information Systems Operations

Overview

Common Technology Components

IT Asset Management

Job Scheduling and Process Automation

System Interfaces

End-User Computing

Data Governance

Operating Systems

Software Licensing

Source Code Management

Capacity Management

Data Classification and Encryption

Overview

Exploring Data Classification

Covering Encryption Basics

Reviewing Encryption Systems

Diving into Digital Signatures

Touring Cryptographic Applications

Examining Public Key Infrastructure (PKI)

Information Technology Principles

Overview

Enterprise Architecture

IT Operations Management

Project Management

Enterprise Resilience

System Development Lifecycle (SDLC)

Emerging Trends in Technology

WEEK 6

Information Security Principles

Overview

Information Security Principles

Information Security Concepts

The CIA Triad

Administrative Security Controls

Control Assessment Types

Data Lifecycle Management

Data Privacy

Last updated 12.23.2025