

MICHAEL GREGG  
ROB JOHNSON

## Cert Guide

Learn, prepare, and practice for exam success



# CISA<sup>®</sup>

Certified Information  
Systems Auditor<sup>®</sup>(CISA)

PEARSON IT  
CERTIFICATION

Exclusive Offer – 40% OFF

## Pearson IT Certification Video Training

livelessons®

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

Use coupon code **PITCVIDEO40** during checkout.



## Video Instruction from Technology Experts



### Advance Your Skills

Get started with fundamentals, become an expert, or get certified.



### Train Anywhere

Train anywhere, at your own pace, on any device.



### Learn

Learn from trusted author trainers published by Pearson IT Certification.

## Try Our Popular Video Training for FREE!

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

Explore hundreds of **FREE** video lessons from our growing library of Complete Video Courses, LiveLessons, networking talks, and workshops.

PEARSON  
IT CERTIFICATION

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

ALWAYS LEARNING

PEARSON

# **Certified Information Systems Auditor (CISA) Cert Guide**

## **Table of Contents**

Cover

Title Page

Copyright Page

About the Authors

Acknowledgments

About the Technical Reviewer

Table of Contents

Introduction

Chapter 1 The CISA Certification

Exam Intent

Why the CISA Certification Is So Important

CISA: The Gold Standard

Exam Requirements

CISA Exam Windows

Scheduling to Take the Exam

Deadline to Apply for the CISA Certification

ISACA Agreements

CISA Exam Domains

Question Format and Grading

Exam Grading

Exam Questions

# **Table of Contents**

Getting Exam Results and Retests

Maintaining CISA Certification

Reporting CPE Hours Earned

Earning CPE Hours

Top 10 Tips and Tricks

Chapter Summary

Define Key Terms

Suggested Readings and Resources

## **Chapter 2 The Information Systems Audit**

Do I Know This Already? Quiz

Foundation Topics

Skills and Knowledge Required to Be an IS Auditor

Work-Related Skills

Knowledge of Ethical Standards

ISACA Standards, Procedures, Guidelines, and Baselines

Knowledge of Regulatory Standards

Guidance Documents

Auditing Compliance with Regulatory Standards

Knowledge of Business Processes

Types of Audits

Risk Assessment Concepts

Risk Management

Auditing and the Use of Internal Controls

The Auditing Life Cycle

Audit Methodology

The Auditing Life Cycle Steps

Chain of Custody and Evidence Handling

# Table of Contents

Automated Work Papers

CAATs

Audit Closing

Report Writing

The Control Self-Assessment Process

Continuous Monitoring

Quality Assurance

The Challenges of Audits

Communicating Results

Negotiation and the Art of Handling Conflicts

Chapter Summary

Exam Preparation Tasks

Review All the Key Topics

Complete Tables from Memory

Define Key Terms

Exercises

2.1 Network Inventory

Review Questions

Suggested Readings and Resources

## Chapter 3 The Role of IT Governance

Do I Know This Already? Quiz

Foundation Topics

The IT Steering Committee

Corporate Structure

IT Governance Frameworks

COBIT

ITIL

# **Table of Contents**

COBIT Versus ITIL

## **Enterprise Risk Management**

The Risk Management Team

Asset Identification

Threat Identification

Quantitative Risk Assessment

Qualitative Risk Assessment

The Three Lines of Defense Model

## **Policy Development**

Policy

Policy, Standards, Procedures, and Baselines

Auditing Policies, Standards, Procedures, and Baselines

Data Classification

Security Policy

## **Management Practices of Employees**

Forced Vacations, Rotation of Assignments, and Dual Control

Separation Events

Roles and Responsibilities

Segregation of Duties (SoD)

Compensating Controls

Key Employee Controls

## **Performance Management**

Key Performance Terms

## **Management and Control Frameworks**

Enterprise Architecture

Change Management

Quality Management

## **Maturity Models**

# **Table of Contents**

Implementing a Maturity Model

Managements Role in Compliance

Process Optimization Techniques

Taguchi

PDCA

Taguchi Versus PDCA

Management of IT Suppliers

Third-Party Outsourcing

Third-Party Audits

Contract Management

Performance Monitoring

Relationship Management

Chapter Summary

Exam Preparation Tasks

Review All the Key Topics

Complete Tables from Memory

Key Terms

Exercises

3.1 Determining the steps for quantitative risk assessment

Review Questions

Suggested Readings and Resources

**Chapter 4 Maintaining Critical Services**

Do I Know This Already? Quiz

Foundation Topics

Threats to Business Operations

The Business Continuity Planning (BCP) Process

Project Management and Initiation

# **Table of Contents**

Business Impact Analysis  
Criticality Analysis  
Development and Recovery Strategy  
Final Plan Design and Implementation  
Training and Awareness  
Implementation and Testing  
Paper Tests  
Preparedness Tests  
Full Operation Tests  
Monitoring and Maintenance  
Understanding BCP Metrics

## **Recovery Strategies**

Alternate Processing Sites  
Alternate Processing Options  
Hardware Recovery  
Redundant Array of Independent Disks  
Software and Data Recovery  
Backup and Restoration  
Telecommunications Recovery  
Verification of Disaster Recovery and Business Continuity Process Tasks  
The Disaster Life Cycle

## **Chapter Summary**

### **Exam Preparation Tasks**

### **Review All the Key Topics**

### **Define Key Terms**

### **Exercises**

#### **4.1 Business Impact and Risk**

### **Review Questions**



# **Table of Contents**

Suggested Readings and Resources

## **Chapter 5 Information Systems Acquisition and Development**

Do I Know This Already? Quiz

Foundation Topics

### **IT Acquisition and Project Management**

IT Acquisition

Software Escrow Agreements

Software Licensing

Project Management

Roles, Responsibility, and Structure of Project Management

Project Culture and Objectives

Making the Business Case for Investment

Return on Investment

Project Management Activities and Practices

Project Initiation

Project Planning

Project Control and Execution

Project Closing

### **Business Application Development**

Systems-Development Methodology

Phase 1: Initiation phase

Phase 2: Development

Phase 3: Implementation

Phase 4: Operation and Maintenance

Phase 5: Disposal

Tools and Methods for Software Development

### **Information Systems Maintenance**

### **Outsourcing and Alternative System Development**

# Table of Contents

- Cloud Computing
- Cloud Threats
- Application-Development Approaches
- N-tier
- Virtualization

## Chapter Summary

Exam Preparation Tasks

Review All the Key Topics

Complete Tables from Memory

Define Key Terms

## Exercises

- 5.1 Project Management

- 5.2 Project Management

## Review Questions

Suggested Readings and Resources

## Chapter 6 Auditing and Understanding System Controls

Do I Know This Already? Quiz

Foundation Topics

Audit Universe and Application Auditing

Programmed and Manual Application Controls

- Business Process Controls

- Input Controls

- Processing Controls

- Data File Controls

- Output Controls

Auditing Application Controls

- Understanding the Application

# **Table of Contents**

Observation and Testing

Data Integrity Controls

Application System Testing

Continuous Online Auditing

## **Auditing Systems Development, Acquisition, and Maintenance**

Project Management

## **Business Application Systems**

E-commerce

Electronic Data Interchange

Email

Business Intelligence

Decision Support Systems

Artificial Intelligence and Expert Systems

Customer Relationship Management

Supply Chain Management

Social Media

## **Chapter Summary**

Exam Preparation Tasks

Review All the Key Topics

Define Key Terms

Exercises

6-1 Software Application Audit

Review Questions

Suggested Readings and Resources

## **Chapter 7 Systems Maintenance and Service Management**

Do I Know This Already? Quiz

Foundation Topics

# **Table of Contents**

## **Service Management Frameworks**

COBIT

FitSM

ISO 20000

eTOM

## **Fundamental Technologies**

Operating Systems

Secondary Storage

Utility Software

Database-Management Systems

Database Structure

Software Licensing Issues

Digital Rights Management

## **Network Infrastructure**

Network Types

Network Standards and Protocols

The OSI Reference Model

The Application Layer

The Presentation Layer

The Session Layer

The Transport Layer

The Network Layer

The Data Link Layer

The Physical Layer

Network Services and Applications

Comparing the OSI Model to the TCP/IP Model

The Network Access Layer

The Internet Layer

The Host-to-Host/Transport Layer

# **Table of Contents**

The Application Layer

Network Services

Wireless Technologies

Bluetooth

802.11 Wireless

Smartphones, Tablets, and Hotspots

Network Equipment

Edge Devices

DMZ

Firewalls

Firewall Configuration

IDS/IPS

Wide Area Networks

Packet Switching

Circuit Switching

Capacity Planning and Systems Performance Monitoring

Network Analyzers

System Utilization and Load Balancing

Third Parties and Cloud Providers

Network Design

Network Cabling

Chapter Summary

Exam Preparation Tasks

Review All the Key Topics

Define Key Terms

Exercises

7.1 Organizing Network Components

Review Questions

# **Table of Contents**

Suggested Readings and Resources

## **Chapter 8 Protection of Assets**

Do I Know This Already? Quiz

Foundation Topics

Access Control

Identification and Authentication (I&A)

Authentication by Knowledge

Authentication by Ownership

Authentication by Characteristic

Single Sign-on

Federation

Remote Access

RADIUS

Diameter

TACACS

Additional Remote Access Options

SSH

VPNs

Physical and Environmental Access Controls

Fences, Gates, and Bollards

Other Physical and Environmental Controls

Using Guards to Restrict Access

Locks

Lighting

CCTV

Heating, Ventilation, and Air Conditioning (HVAC)

Security Controls for Hardware and Software

Securing Voice Communications

# **Table of Contents**

Encryptions Role as a Security Control

Private Key Encryption

Data Encryption Standard (DES)

Advanced Encryption Standard (AES)

Public Key Encryption

RSA Encryption

Elliptic Curve Cryptography (ECC)

Quantum Cryptography

Hashing and Digital Signatures

Public Key Infrastructure (PKI)

Using Cryptography to Secure Assets

Internet Security Protocols

## **Protection of Information Assets**

Information Life Cycle

Access Restriction

Laws Related to the Protection of Information

Maintaining Compliance

Protection of Privacy

Using Data Classification to Secure Critical Resources

## **Data Leakage and Attacks**

Attacks Against Encryption

Threats from Unsecured Devices

Threats from Improper Destruction

Threats to the Infrastructure

## **Chapter Summary**

## **Exam Preparation Tasks**

## **Review All the Key Topics**

## **Complete Tables from Memory**

# **Table of Contents**

Define Key Terms

Review Questions

Suggested Reading and Resources

## **Chapter 9 Asset Threats, Response, and Management**

Do I Know This Already? Quiz

Foundation Topics

Security Controls

- Technical Controls

- Cloud Computing

- Operating Systems

- Databases

- Virtualization

- Administrative Controls

Attack Methods and Techniques

- Social Engineering and Nontechnical Attacks

- Sniffing

- Man-in-the-Middle Attacks and Hijacking

- Denial of Service

- Botnets

- Malware

- Wireless and Bluetooth

- SQL Injection

- Buffer Overflow

- XSS and XSRF

- Logic Bombs, Rounding Down, and Asynchronous Attacks

- Integer Overflow

- Password Attacks

Prevention and Detection Tools and Techniques



# **Table of Contents**

Audit and Log Review

Security Testing Techniques

Vulnerability Scanning

Penetration Testing

## **Problem and Incident Management Practices**

Tracking Change

Fraud Risk Factors

Insiders

Outsiders

Incident Response

Emergency Incident Response Team

Incident Response Process

Incident Response and Results

Forensic Investigation

Forensics Steps

Other Forensic Types

Computer Crime Jurisdiction

## **Chapter Summary**

Exam Preparation Tasks

Review All the Key Topics

Complete Tables from Memory

Define Key Terms

Review Questions

Suggested Reading and Resources

## **Chapter 10 Final Preparation**

Tools for Final Preparation

Pearson Test Prep Practice Test Software and Questions on the Website

Accessing the Pearson Test Prep Software Online

# **Table of Contents**

Accessing the Pearson Test Prep Software Offline

Customizing Your Exams

Updating Your Exams

Premium Edition

Memory Tables

Chapter-Ending Review Tools

Suggested Plan for Final Review/Study

Summary

## **Glossary**

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

# **Table of Contents**

S

T

U

V

W

Z

Appendix A: Answers to the Do I Know This Already  
Quizzes and Review Questions

Index

Online Elements

Appendix B: Memory Tables

Appendix C: Memory Tables Answer Key

Where are the companion content files?