



Cert Guide

Advance your IT career with hands-on learning

CC Certified in Cybersecurity



MARI GALLOWAY
AMENA JAMALI



Practice
Tests



Flash
Cards



Review
Exercises



Study
Planner

CC Certified in Cybersecurity Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, the Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.pearsonITcertification.com/register.
2. Enter the **print book ISBN**: 9780138200381.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.ehelp.org**.

CC Certified in Cybersecurity Cert Guide

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Contents

Introduction

Chapter 1 Cybersecurity Principles

Do I Know This Already? Quiz

Foundation Topics

Information Assurance

The CIA Triad

Confidentiality

Integrity

Availability

Privacy

ISC2 Code of Ethics

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

References

Chapter 2 Risk Management

Table of Contents

Do I Know This Already Quiz

Foundation Topics

Risk Management

Risks, Threats, and Vulnerabilities

The Scope of Risk Management

The Risk Management Process

- Risk Identification

- Risk Assessment

- Risk Treatment

Security Controls and Governance

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

References

Chapter 3 Threats to Security

Do I Know This Already? Quiz

Foundation Topics

Threats to Security

Common Threat Categories

- Malware

- Viruses

- Worms

- Trojans

- Ransomware

- Advanced Persistent Threats

Network Attacks

- Distributed Denial-of-Service Attack

Table of Contents

Man-in-the-Middle Attack

Side-Channel Attack

Detection and Mitigation Techniques

Detection Tools

Scanning and Penetration Testing

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

References

Chapter 4 Physical Access Controls

Do I Know This Already? Quiz

Foundation Topics

Physical Security Controls

Badge Systems

Gates for Physical Protection

Types of Gate Entry Systems

Access Control

Environmental Design

Monitoring for Physical Security

Security Guards

Closed-Circuit Television

Alarm Systems

Logs and Documentation

Authorized Versus Unauthorized Personnel

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Table of Contents

Q&A

References

Chapter 5 Logical Access Controls

Do I Know This Already? Quiz

Foundation Topics

Need to Know and Least Privilege

Segregation of Duties

Security Models

- Discretionary Access Control

- Mandatory Access Control

- Role-Based Access Control

IAM and Automation

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

References

Chapter 6 Computer Networking Fundamentals

Do I Know This Already Quiz

Foundation Topics

Understanding Computer Networking

Ports and Protocols

OSI Model

- Application Layer (Layer 7)

- Presentation Layer (Layer 6)

- Session Layer (Layer 5)

- Transport Layer (Layer 4)

Table of Contents

Network Layer (Layer 3)

Internet Protocol

Data Link Layer (Layer 2)

Protocols

Wireless

Physical Layer (Layer 1)

TCP/IP Model

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

References

Chapter 7 Network Security Infrastructure

Do I Know This Already Quiz

Foundation Topics

On-Premises Network Security Infrastructure

Environmental Controls

Fire Suppression Systems

Redundancy and High Availability

Memorandum of Understanding and Memorandum of Agreement

Designing Secure Networks

Demilitarized Zones

Virtual Local Area Networks

Virtual Private Networks

Network Access Control

Embedded Systems

Cloud Network Security Infrastructure

Cloud Deployment Models

Table of Contents

Public

Private

Community

Hybrid

Cloud Service Models

Infrastructure as a Service

Platform as a Service

Software as a Service

Service-Level Agreement

Managed Service Provider

Cloud Challenges

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

References

Chapter 8 Data and the System

Do I Know This Already? Quiz

Foundation Topics

Data Security

Encryption

Hashing

Non-Repudiation

Authentication

One-Time Passwords

Password Policy

Data Handling

Data Classification

Table of Contents

Data Labeling

Data Retention

Data Destruction

Data Handling Policy

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

References

Chapter 9 Security in the Life

Do I Know This Already? Quiz

Foundation Topics

System Hardening

Baselines

Patch Management

Vulnerability Management

System Updates and Upgrades

Logging and Monitoring

Security Policies

Acceptable Use Policy

Bring Your Own Device Policy

Change Management Policy

Privacy Policy

Security Awareness Training

Social Engineering

Password Protection

Exam Preparation Tasks

Review All Key Topics

Table of Contents

Define Key Terms

Q&A

Reference

Chapter 10 Security in Emergencies

Do I Know This Already? Quiz

Foundation Topics

Incident Response

- Detection

- Classification

- Containment

- Response

- Recovery

- Reflection

- Testing

Business Continuity

- Business Impact Analysis

- Testing

- Backup and Recovery

Disaster Recovery

- Recovery Time Objective

- Recovery Point Objective

- Maximum Tolerable Downtime

- Replication, Hot Sites, Warm Sites, and Cold Sites

- Failover Testing

Governance Processes

- Policies

- Standards

- Procedures

Table of Contents

Guidelines

Regulations and Laws

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

References

Chapter 11 Tying It All Together

Security as a Whole

Defense-in-Depth

The Castle Analogy

The Whole of Information Assurance

Summary

Chapter 12 After the Certification

Take a Breather and Reflect

Update Your Professional Profiles

Showcase Your Passion and Knowledge

Seek Mentorship and Sponsorship

Stay Informed About Emerging Threats and Technologies

Contribute to the Community Through Thought Leadership

Explore Further Education Opportunities

Evaluate Career Progress and Set New Goals

Summary

Chapter 13 Final Preparation

Suggested Plan for Final Review and Study

Summary

Appendix A: Answers to the Do I Know This Already?

Table of Contents

Quizzes and Q&A

Appendix B: CC Certified in Cybersecurity Cert Guide Exam
Updates

Glossary of Key Terms

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Z

Index

Table of Contents

Online Elements

Appendix C: Study Planner