



Microsoft Security, Compliance, and Identity Fundamentals

Exam Ref SC-900

Yuri Diogenes
Nicholas DiCola
Kevin McKinnerney
Mark Morowczynski

Exam Ref SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Yuri Diogenes
Nicholas DiCola
Kevin McKinnerney
Mark Morowczynski

Exam Ref SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Table of Contents

Cover

Title Page

Copyright Page

Contents at a glance

Contents

Introduction

- Organization of this book

- Preparing for the exam

- Microsoft certification

- Errata, updates & book support

- Stay in touch

Chapter 1 Describe the concepts of security, compliance, and identity

- Skill 1-1: Security and compliance concepts and methodologies

 - Zero-trust methodology

 - Shared responsibility model

 - Defense-in-depth

 - Common threats

 - Encryption

 - Cloud Adoption Framework

- Skill 1-2: Identity concepts

 - Identity as the primary security perimeter

Table of Contents

What is authentication?

What is authorization

What is Active Directory?

What are federation services and identity providers?

Common identity attacks

Thought experiment

Thought experiment answers

Chapter summary

Chapter 2 Microsoft Identity and Access Management Solutions

Skill 2-1: Define the basic identity services and identity types of Azure AD

Describe what Azure Active Directory is

Describe what hybrid identity is

Describe Azure AD identities (users, devices, groups, and service principals/applications)

Describe the different external identity types (guest users)

Skill 2-2: Describe the authentication capabilities of Azure AD

Describe the different authentication methods

Describe password protection and management capabilities

Describe self-service password reset

Describe multifactor authentication

Describe Windows Hello for Business and passwordless credentials

Skill 2-3: Describe the access management capabilities of Azure AD

Describe what conditional access is

Describe uses and benefits of conditional access

Describe the benefits of Azure AD roles

Skill 2-4: Describe the identity protection and governance capabilities of Azure AD

Describe what identity governance is

Table of Contents

Describe what entitlement management and access reviews are

Describe the capabilities of PIM

Describe Azure AD Identity Protection

Thought experiment

Thought experiment answers

Chapter summary

Chapter 3 Capabilities of Microsoft security solutions

Skill 3-1: Basic security capabilities in Azure

Azure network security groups

Azure DDoS protection

Azure Firewall

Azure Bastion

Web Application Firewall

Data encryption in Azure

Skill 3-2: Security Management capabilities in Azure

Azure Security Center

Azure Secure Score

Cloud workload protection with Azure Defender

Cloud security posture management capabilities

Security baselines for Azure

Skill 3-3: Security capabilities in Azure Sentinel

What is Security Information and Event Management (SIEM)?

What is security orchestration, automation, and response (SOAR)?

What is extended detection and response (XDR)?

Azure Sentinel

Skill 3-4: Threat protection with Microsoft 365 Defender

Describe Microsoft 365 Defender services

Describe Microsoft Defender for Identity

Describe Microsoft Defender for Office 365

Table of Contents

Describe Microsoft Defender for Endpoint

Describe Microsoft Cloud App Security

Skill 3-5: Security management capabilities of Microsoft 365

Describe the Microsoft 365 Security Center

Describe how to use Microsoft Secure Score

Explore security reports and dashboards

Describe incidents and incident management capabilities

Skill 3-6: Endpoint security with Microsoft Intune

What is Intune?

Endpoint security with Intune and Microsoft Endpoint Manager admin center

Thought experiment

Thought experiment answers

Chapter summary

Chapter 4 Describe the capabilities of Microsoft compliance solutions

Skill 4-1: Common compliance needs

Microsoft Compliance Center

Microsoft Compliance Manager

Compliance Score

Skill 4-2: Information protection and governance

Data classification capabilities

Content Explorer and Activity Explorer

Sensitivity labels

Retention policies and labels

Records management

Data loss prevention

Skill 4-3: Insider risk

Insider risk management

Table of Contents

- Communication compliance
- Information barriers
- Privileged access management
- Customer Lockbox

Skill 4-4: eDiscovery

- Microsoft 365 eDiscovery
- Content Search
- Core eDiscovery Workflow
- Advanced eDiscovery workflow

Skill 4-5: Auditing

- Microsoft 365 audit capabilities
- Advanced Audit

Skill 4-6: Resource governance

- Azure resource locks
- Azure Blueprints
- Azure Policy
- Cloud Adoption Framework

Thought experiment

Thought experiment answers

Chapter summary

Index