

AWS Certified Security - Specialty Certification Guide (SCS-C01)

AWS security concepts and best practices

Nikhil Agarwal



www.bpbonline.com

First Edition 2024

Copyright © BPB Publications, India

ISBN: 978-93-55516-640

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

To View Complete
BPB Publications Catalogue
Scan the QR Code:



www.bpbonline.com

Kup książkę

Dedicated to

*My parents, the original programmers of my life; my wife, the ultimate
debugger of my dreams and my friends, the trusted network*

About the Author

Nikhil is an innovator in the field of cyber security, recognized by his remarkable knowledge and innovative approach. When it comes to data and cloud security, he is the go-to guy. He leads large-scale projects, helping clients solve their most pressing data security and cloud security challenges.

Nikhil's reputation as a noted technology expert is well-deserved, as he is passionate about sharing his knowledge and building communities. He has also co-founded an open-source emerging tech community in India called FutureGPT.

In recognition of his outstanding contributions to the field, Nikhil was ranked 18th globally in Cyber Security, 10th in Emerging Technologies, and 3rd in Cloud Security Leaders by Onalytica in 2021. His accomplishments were further celebrated in 2022 when he was named a Cloud Security Champion by the Cloud Security Alliance and recently awarded Cyber Security Champion in 2024 by Bsides.

He has a proven ability to work across cultures and serve clients globally, having previously held senior leadership roles with Fortanix Inc, Deloitte Singapore, PwC Thailand, Quick Heal, and Atos.

About the Reviewer

Ritesh Gohil is a dedicated Information Security Engineer with over five years of professional experience in Cyber Security and Penetration Testing. His expertise spans across Web applications, APIs, Mobile (Android and iOS) applications, and Cloud Security / Penetration Testing. He has made significant contributions to the field by publishing eight CVEs in Mitre and is recognized as one of the top 25 researchers on the Yogosha platform. Ritesh has also received multiple honorable mentions from Google and Apple.

Ritesh specializes in advanced AWS security solutions, ensuring robust protection for cloud environments, and maintaining compliance standards. His passion for cybersecurity is evident through his participation in bug bounties and his active involvement in security research, where he has reported numerous vulnerabilities and received commendations from the Indian Government for his responsible vulnerability disclosure.

He is currently working at Ryanair, Europe's Favourite Airline, where he is part of the Red Team, responsible for penetration testing, security audits, and fortifying digital infrastructure. Ritesh holds multiple industry certifications, including AWS Certified Security – Specialty, eWPTXv2, eCPPTv2, CRTP, eJPT, and CEH. He completed his MSc in Cyber Security from the National College of Ireland. His dedication to the field is further demonstrated through his active participation in security conferences and contributions to various security platforms.

Acknowledgement

Creating this book has been an incredible journey, and I could not have done it without the amazing support of so many wonderful people.

First, to my parents: thank you for your endless love and support. Your constant encouragement and belief in me have been my foundation.

To my wonderful wife: thank you for your patience, understanding, and constant support. Your love and encouragement have been my greatest source of motivation.

To my friends: thank you for your kindness, laughter, and always being there when I needed a break. Your support has made every challenge seem manageable.

Finally, to everyone who has been a part of this journey, whether directly or indirectly: your contributions, no matter how small, have made a significant impact. Thank you for being a part of this adventure.

This book is a testament to the power of support, collaboration, and the collective effort of many wonderful people. Thank you all for being a part of my life and this journey.

Preface

Welcome to the **AWS Certified Security - Specialty Certification Guide (SCS-C01)**, an exhaustive guide that is specifically designed to assist you in managing the complexities of AWS security and achieving this highly valued certification. This book has been designed to ensure that you have a comprehensive understanding of the essential concepts, practices, and technologies necessary to secure AWS environments.

Chapter 1: Getting Started with Foundations of Cloud Security- This chapter covers the foundation for your learning experience by addressing the fundamental principles of cloud security. You will gain an understanding of the different security challenges and benefits that cloud computing offers.

Chapter 2: The AWS Certified Security-specialty Exam Domains - This chapter covers the specific domains that are covered by the certification exam. In order to ensure that you have sufficient preparation for every section of the exam, this chapter outlines the key areas of interest that you need to focus on.

Chapter 3: Identity and Access Management: Laying a Solid Foundation - This chapter covers the fundamentals of IAM. To ensure that access to your AWS resources is both secure and effective, you will learn how to manage users, groups, roles, and permissions.

Chapter 4: Securing Infrastructure Design in AWS - This chapter covers the best practices for designing secure AWS infrastructure. It also covers methods for securing your digital assets and network from a variety of threats.

Chapter 5: Securing Network Design in AWS - This chapter covers the specifics of securing your network architecture. You will learn about VPCs, subnets, security groups, and other network elements that are essential to the security of AWS.

Chapter 6: Application and Host-based Security - This chapter covers the applications and host environments. Best practices for protecting your code, applications, and operating systems are also discussed in this chapter.

Chapter 7: Data-at-rest, Data-in-transit and Data-in-use Protection - This chapter covers data security in Cloud. To ensure the security of your sensitive information, you will learn about a variety of data security measures, such as encryption, access controls, and data obfuscation.

Chapter 8: Encryption and Key Management - This chapter covers the field of encryption and Key Management. This chapter provides a comprehensive explanation of the methods and services necessary to effectively implement and perform encryption and key management within AWS.

Chapter 9: AWS Multi-account Architecture and Access Control - This chapter covers the benefits and complexities of managing multiple AWS accounts. You'll learn how to establish a secure multi-account strategy that ensures proper access control and governance.

Chapter 10: Infrastructure-as-Code and CI/CD - This chapter covers the modern practices for automating infrastructure deployment and management. You will learn how to use Infrastructure-as-Code (IaC) tools and continuous integration/continuous deployment (CI/CD) pipelines to maintain secure and compliant environments.

Chapter 11: Application and Network Logging Strategies - This chapter covers how to promptly detect and respond to security incidents by implementing effective logging strategies.

Chapter 12: Troubleshooting Security and Monitoring Alerts - This chapter covers the practical approaches to troubleshooting security issues and responding to monitoring alerts. The tools necessary to maintain a secure and resilient AWS environment are discussed in this chapter.

Chapter 13: Incident Detection, Response, and Remediation - This chapter covers the critical aspects of incident management. To reduce the impact of security incidents on your organization, you will learn how to detect, respond to, and resolve them.

Chapter 14: Compliance, Governance, and Data Security Standards - This chapter covers the essential requirements for maintaining compliance with various standards and regulations. You will gain knowledge about establishing governance frameworks and adhering to data security standards in this course.

Chapter 15: Assessment, Audit, and Evidence Collection - This chapter covers the guidance on conducting security assessments and audits. In order to effectively gather and present evidence of your security practices, this chapter ensures that you are prepared.

Chapter 16: Automated Security Investigation and Remediation - This chapter covers the implementation of automation in security operations. You will learn how to use AWS services to automate security investigations and remediation duties, which will improve your capacity to respond to threats promptly.

Chapter 17: Exam Preparation Tips - This chapter covers the conclusion of the book by summarizing the primary topics and offering concluding insights on your progress to the role of AWS Security Specialist.

Whether you are new to AWS or seeking to expand your knowledge, this book is designed for developers and security professionals. This guide will help you gain the skills and confidence to excel in the field of AWS security and achieve your certification objectives. This book will be both informative and beneficial.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

<https://rebrand.ly/mdp9klg>

We have code bundles from our rich catalogue of books and videos available at <https://github.com/bpbpublications>. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At www.bpbonline.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

<https://discord.bpbonline.com>



Table of Contents

1. Getting Started with Foundations of Cloud Security	1
Introduction	1
Structure	1
Objectives	2
Understanding the fundamentals of cloud security	2
Overview of the shared responsibility model.....	2
Risk assessment and threat modeling.....	3
<i>How cloud security works with shared responsibility.....</i>	<i>4</i>
<i>A quick look at cloud computing model</i>	<i>4</i>
Cloud security recommended practices	6
Conclusion	7
2. The AWS Certified Security-specialty Exam Domains	9
Introduction	9
Structure	9
Objectives	10
Exam format and preparation recommendations	10
<i>About the exam.....</i>	<i>10</i>
<i>Exam format</i>	<i>10</i>
<i>Unscored content</i>	<i>11</i>
<i>Domains covered</i>	<i>11</i>
Exam preparation recommendations.....	13
Conclusion	14
3. Identity and Access Management: Laying a Solid Foundation.....	15
Introduction	15
Structure	15
Objectives	16
Defining IAM.....	16

<i>Key concepts of IAM policies and permissions</i>	17
<i>Use cases for IAM policies and permissions</i>	18
<i>IAM integration with other AWS services</i>	21
<i>Authorization and authentication of AWS resources</i>	24
<i>IAM users security</i>	25
IAM groups.....	29
IAM roles.....	30
<i>AWS security token service</i>	31
<i>Cross-account access roles</i>	31
Access management with policies and permissions.....	34
Access management in Amazon S3	36
Conclusion	38
4. Securing Infrastructure Design in AWS	41
Introduction	41
Structure	41
Objectives	41
Physical security.....	42
Storage security	42
Compute security	43
<i>Security of the AWS infrastructure</i>	43
<i>Physical security</i>	44
<i>AWS data center physical security</i>	44
<i>AWS region and availability zone design</i>	45
Storage security.....	45
Amazon S3 security	45
Amazon EBS security	47
Compute security	48
Amazon EC2 security	48
Amazon ECS security	50
Conclusion	51

5. Securing Network Design in AWS	53
Introduction	53
Structure	53
Objectives	54
Understanding the basics of network security	54
Best practices for network design and architecture	55
<i>AWS global infrastructure</i>	<i>55</i>
<i>Regions</i>	<i>55</i>
<i>Availability zones</i>	<i>57</i>
Virtual private cloud.....	58
Subnet	60
Route tables.....	61
<i>Internet gateway.....</i>	<i>62</i>
<i>NAT gateway.....</i>	<i>63</i>
<i>VPC peering</i>	<i>65</i>
<i>Shared VPCs</i>	<i>66</i>
<i>Elastic network interface</i>	<i>66</i>
<i>Elastic IP addresses</i>	<i>67</i>
Network access management.....	68
<i>Stateful vs. stateless.....</i>	<i>69</i>
<i>Security groups</i>	<i>69</i>
<i>Best practices for the security group</i>	<i>71</i>
<i>Network ACLs.....</i>	<i>71</i>
<i>Custom network ACLs and other AWS services.....</i>	<i>71</i>
<i>VPC Endpoints</i>	<i>72</i>
<i>Connecting a VPC to on-premises networks</i>	<i>72</i>
<i>AWS direct connect.....</i>	<i>72</i>
<i>VPC flow logs</i>	<i>72</i>
<i>Amazon Route 53.....</i>	<i>72</i>
<i>Amazon CloudFront</i>	<i>73</i>
<i>Amazon API gateway.....</i>	<i>73</i>

Elastic load balancer	74
AWS web application firewall	74
AWS shield	75
Scenario-based examples	75
Exam tips.....	76
Conclusion	77
References.....	78
6. Application and Host-based Security	79
Introduction	79
Structure	79
Objectives	80
Overview	80
Best practices for application security.....	81
Secure coding and development techniques.....	82
Implement code review in AWS	83
Host-based security	84
AWS system manager	85
Systems manager.....	85
Patch manager.....	86
HIDS and HIPS	87
Amazon CloudWatch	87
Amazon GuardDuty	89
Use cases for Amazon GuardDuty	90
Enabling Amazon GuardDuty	90
Exporting GuardDuty findings to an Amazon S3 bucket.....	91
Setting up GuardDuty finding alerts through SNS	92
AWS Elastic Beanstalk.....	93
Security best practices for Elastic Beanstalk.....	94
Implement least privilege access	94
Keep your platforms up to date	94
Make sure that environment instances use IMDSv2	95

<i>Set up monitoring</i>	95
<i>AWS Lambda</i>	95
<i>Lambda use cases</i>	96
<i>Exam tips</i>	98
Conclusion	98
References.....	99
7. Data-at-rest, Data-in-transit and Data-in-use Protection.....	101
Introduction	101
Structure	101
Objectives	102
Overview	102
Data encryption techniques and best practices	102
<i>Encryption of data in transit</i>	103
<i>Encryption of data at rest</i>	104
<i>Securing Amazon Virtual Private Cloud</i>	105
<i>Encryption for AWS CloudTrail</i>	106
<i>Encrypting Amazon elastic container registry</i>	108
<i>Encrypting Amazon Elastic Container Service</i>	109
<i>Encrypting Amazon elastic Kubernetes service</i>	110
<i>Use of AWS Nitro for data in use security</i>	112
<i>Benefits of using AWS Nitro</i>	112
<i>Storage security controls and best practices</i>	113
<i>AWS Encryption SDK</i>	113
<i>Encryption for DynamoDB</i>	116
<i>Encrypting Amazon EC2 and EBS</i>	118
<i>Securing AWS Lambda</i>	118
Encrypting Amazon relational database service	119
<i>Encrypting Amazon S3</i>	121
<i>Encrypting Amazon elastic file system</i>	122
<i>Exam tips</i>	123
Conclusion	125

8. Encryption and Key Management	127
Introduction	127
Structure	127
Objectives	128
Overview	128
Key management concepts and best practices.....	128
AWS key management service.....	131
<i>CloudHSM</i>	139
<i>CloudHSM use-cases</i>	141
<i>APIs for CloudHSM</i>	142
AWS certificate manager	143
<i>AWS secrets manager</i>	144
<i>Exam tips</i>	146
Conclusion	147
9. AWS Multi-account Architecture and Access Control	149
Introduction	149
Structure	149
Objectives	150
Overview	150
Understand AWS organizations and account management.....	150
<i>Best practices for using AWS organizations</i>	151
<i>Managing AWS accounts</i>	152
IAM roles and cross-account access	152
<i>How IAM roles work</i>	154
<i>The process of creating and managing IAM roles</i>	154
Security best practices for multi-account environments	158
<i>Least privilege principle</i>	158
<i>Keeping your duties separate</i>	159
<i>Continuous monitoring and auditing</i>	159
<i>Example 1: Enforce the least privilege for IAM users</i>	160
<i>Example 2: Separation of duties for cross-account access</i>	160

<i>Example 3: Enable continuous monitoring with CloudTrail</i>	161
AWS service control policies	161
<i>Benefits of deploying SCPs</i>	162
<i>Example 1: Permissions SCP to deny access</i>	163
<i>Example 2: Tagging SCP to enforce S3 tagging requirement</i>	164
<i>Example 3: Permissions SCP to allow access to specific EC2</i>	164
<i>Exam tips</i>	165
<i>IAM roles and cross-account access</i>	166
Conclusion	167
References.....	167
10. Infrastructure-as-Code and CI/CD	169
Introduction	169
Structure	169
Objectives	170
Overview	170
Infrastructure-as-Code ideas and best practices.....	170
<i>Example 1: CloudFormation stack operations</i>	172
<i>Example 2: S3 bucket creation for CloudFormation templates</i>	173
<i>Example 3: Lambda function deployment</i>	173
AWS CloudFormation and AWS CodePipeline.....	175
AWS CloudFormation.....	175
<i>How to define and structure CloudFormation templates</i>	176
<i>Best practices for writing CloudFormation templates</i>	177
AWS CodePipeline	178
<i>Setting up AWS CodePipeline: Best practices for security</i>	179
Security best practices for CI/CD pipelines.....	184
AWS Config and AWS service catalog	187
AWS Config.....	188
<i>Best security practices of AWS config</i>	190
AWS service catalog	190

<i>Best practices of AWS service catalog</i>	192
<i>Exam tips</i>	192
<i>AWS Config and AWS service catalog</i>	193
Conclusion	194
References.....	194
11. Application and Network Logging Strategies	195
Introduction	195
Structure	195
Objectives	196
Overview	196
Understanding AWS CloudTrail and AWS CloudWatch	197
<i>AWS CloudTrail</i>	197
<i>CloudTrail recorded event fields</i>	199
<i>AWS CloudWatch</i>	203
<i>AWS logging sources categories and supporting services</i>	206
<i>Setting up AWS CloudWatch</i>	207
Best practices for application and network logging	211
<i>Understanding application and network logging</i>	211
Log analysis and monitoring techniques.....	213
<i>Amazon inspector</i>	213
<i>Amazon GuardDuty</i>	215
<i>AWS Security Hub</i>	216
<i>AWS systems manager</i>	217
<i>AWS Trusted Advisor</i>	218
<i>Log analysis and monitoring techniques</i>	219
Security information and event management	221
<i>SIEM importance</i>	221
<i>Implementing SIEM in AWS</i>	221
<i>Log collection and ingestion</i>	222
<i>Event correlation</i>	222
<i>Continuous improvement</i>	223

<i>Exam tips</i>	223
Conclusion	224
References.....	224
12. Troubleshooting Security and Monitoring Alerts	225
Introduction	225
Structure	225
Objectives	226
Overview	226
Understanding how to fix problems	226
<i>Case study: Resolving a misconfigured S3 bucket access</i>	227
<i>Case study: Mitigating unauthorized access with incident response</i>	228
Best practices for security monitoring and alerting	229
AWS X-Ray.....	231
<i>Use cases and examples</i>	234
AWS system manager	236
<i>Examples and use cases</i>	237
AWS troubleshooting best practices.....	238
<i>Exam tips</i>	239
Conclusion	240
13. Incident Detection, Response, and Remediation	241
Introduction	241
Structure	241
Objectives	242
Overview	242
AWS security incident response framework.....	242
<i>Key phases of the incident response framework</i>	242
<i>Importance in the incident response framework</i>	243
Useful case studies for the examination	244
<i>Case study 1: Unauthorized access and response</i>	244
<i>Case Study 2: Cyberattack using ransomware</i>	244
<i>Case Study 3: DDoS attack mitigation</i>	245

Best practices for responding to and fixing problems	245
AWS Security Hub	247
Amazon GuardDuty	250
<i>Case Study: Using AWS GuardDuty and Security Hub</i>	253
<i>Scenario: Finding and responding to suspicious activity</i>	253
<i>Exam tips</i>	254
Conclusion	255
14. Compliance, Governance, and Data Security Standards	257
Introduction	257
Structure	257
Objectives	258
Overview	258
Understanding compliance and governance requirements	258
<i>Compliance and governance in AWS</i>	258
<i>AWS Identity and Access Management</i>	259
<i>AWS Key Management Service</i>	259
<i>AWS Config</i>	259
<i>AWS CloudTrail</i>	260
<i>AWS Artifact</i>	260
<i>AWS Config rules</i>	260
AWS compliance and governance programs	260
<i>AWS compliance programs</i>	261
<i>AWS governance programs</i>	261
Best practices for data privacy and protection	264
<i>AWS Artifact</i>	266
<i>How the AWS artifact works</i>	267
AWS config rules	269
<i>Case study: Ensuring public S3 buckets compliance</i>	272
<i>Exam tips</i>	273
Conclusion	273

15. Assessment, Audit, and Evidence Collection	275
Introduction	275
Structure	275
Objectives	276
Overview	276
<i>Understanding audit and assessment requirements</i>	<i>276</i>
<i>Identify audit scope and standards</i>	<i>276</i>
<i>Understand the AWS shared responsibility model</i>	<i>277</i>
<i>Implementing AWS best practices</i>	<i>277</i>
<i>AWS audit and assessment programs</i>	<i>278</i>
Secure your evidence: Collect Smart and Store Safe	278
<i>Amazon inspector</i>	<i>281</i>
<i>Configuring Amazon Inspector</i>	<i>282</i>
<i>AWS certificate manager</i>	<i>286</i>
<i>How to configure AWS Certificate Manager in AWS</i>	<i>288</i>
<i>Exam tips</i>	<i>290</i>
Conclusion	292
16. Automated Security Investigation and Remediation	293
Introduction	293
Structure	293
Objectives	293
Overview	294
Understanding security automation and orchestration	294
<i>Integration of AWS services</i>	<i>296</i>
Security playbooks and incident response automation	297
AWS security incident response automation	299
<i>Exam tips</i>	<i>302</i>
Conclusion	302
17. Exam Preparation Tips	303
Introduction	303
Structure	303
Objectives	304

Getting ready for the AWS security certification.....	304
An overview of certification.....	305
Exam format and topics	306
AWS security specialty mock exam 1.....	307
<i>Answers for AWS security speciality mock exam 1</i>	310
AWS security specialty mock exam 2.....	311
<i>Answers for AWS security speciality mock exam 2</i>	314
Conclusion	315
Glossary	315
Index	317-322

CHAPTER 1

Getting Started with Foundations of Cloud Security

Introduction

Computing in the cloud has evolved as a crucial technological advancement that has significantly altered the method in which we manage, process, and store data. The traditional approach to computing has been fundamentally altered as a result of the provision of an infrastructure that is both scalable and adaptable and that can be accessed at any time and from any location. On the other hand, with tremendous power comes great responsibility, and the obligation of safeguarding the cloud infrastructure falls on both the **Cloud Service Providers (CSPs)** and the clients who use their services. The principles of cloud security, the shared responsibility paradigm, risk assessment, threat modeling, and best practices are going to be covered in this chapter.

Structure

This chapter will cover the following topics:

- Understanding the fundamentals of cloud security
- Overview of the shared responsibility model
- Risk assessment and threat modeling
- Cloud security recommended practices

Objectives

This introduction chapter will offer readers with a basic grasp of the fundamentals of cloud security and will build the basis for the rest of the book, which will delve into particular tools and approaches for securing cloud environments. The goal of this chapter is to provide readers with a solid understanding of the fundamentals of cloud security. The reader will obtain a clear grasp of the significance of cloud security as well as how to approach it methodically after going through an overview of the shared responsibility model, risk assessment, and threat modeling. In addition to that, this chapter will present readers with a set of best practices that they should follow to keep their cloud environments safe.

Understanding the fundamentals of cloud security

Data, apps, and the underlying infrastructure in a cloud computing environment all need to be protected for cloud security to be effective. Access control, encryption, network security, **Identity and Access Management (IAM)**, and disaster recovery are some of the different security methods that are included in this. It is essential to have a solid understanding of the principles of cloud security to guarantee the safety of cloud-based infrastructure. The following are some of the central ideas:

- **Confidentiality:** The protection of sensitive information from being accessed or disclosed in an unapproved manner is what is meant by the term confidentiality.
- **Integrity:** It refers to the protection of data from unintended changes or deletions made by unauthorized parties.
- **Availability:** This refers to the guarantee that the data and services will be accessible whenever they are needed.
- **Authentication:** This refers to the process of determining if a user or a computer system is who they claim to be.
- **Authorization:** This refers to the process of allowing access to resources according to user roles and permissions. This procedure is referred to as "authorization."
- **Non-repudiation:** This is the assurance that a user cannot deny doing an action; it is also known as the non-repudiation guarantee.

Overview of the shared responsibility model

The shared responsibility model is a framework that defines the responsibilities of both the **Cloud Service Provider (CSP)** and the client about the protection of the cloud's underlying infrastructure. The model shifts based on the deployment model for the cloud, which can be either public, private, or hybrid. Refer to the following *Figure 1.1*, showing the shared responsibility model for a CSP:

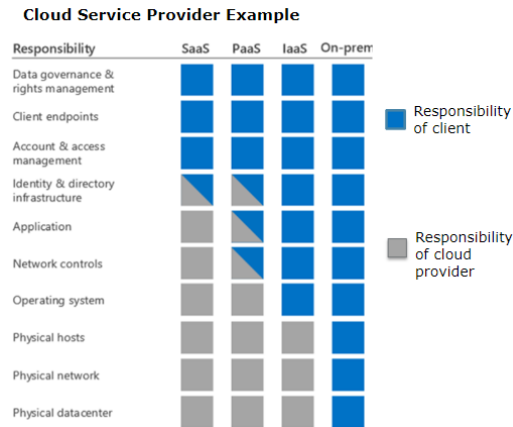


Figure 1.1: Shared Responsibility Model for a CSP

The cloud service provider is responsible for the security of the underlying infrastructure in the public cloud deployment paradigm, whereas the client is responsible for the security of the applications and data. The customer is responsible for the security of the underlying infrastructure when the private cloud deployment model is used, while the cloud service provider is responsible for the security of the applications and data. The customer and the CSP both bear equal responsibility for the safety of the infrastructure, apps, and data when it comes to hybrid cloud deployment models. Because it guarantees that all parties involved are aware of their obligations and take appropriate actions to safeguard the cloud infrastructure, the shared responsibility model is an essential component of cloud security.

Note: Ownership of risks, controls, and outcomes are underpinned by a shared responsibility matrix. Risk management responsibilities can vary sharply depending on the selected cloud deployment and service models. Hence it is critical to understand the areas of responsibility within this model, which allows us to define the scope of the assessment.

Risk assessment and threat modeling

The two most important parts of cloud security are risk assessment and threat modeling. Risk assessment is the process of finding possible risks and weaknesses in the cloud system and figuring out how likely it is that a threat will use them. Threat modeling is the process of looking at possible risks and how they might affect the cloud system. By doing a risk assessment and threat modeling, enterprises can find possible security holes and fix them by putting in place the right security controls.

When looking at the security of a cloud service provider from a technical point of view, risk assessment and threat modeling are very important steps. These practices help find possible risks, weaknesses, and threats to the infrastructure, data, and services of the provider.

Here is what you need to know about risk assessment and threat modeling for CSP:

- **Risk assessment:** Risk assessment is the process of finding, analyzing, and rating possible risks related to the technical infrastructure and activities of the cloud service provider. Its goal is to figure out how likely and bad different risks are so that prevention efforts can be prioritized. Usually, the following steps make up the process:
- **Asset identification:** Determine which servers, databases, apps, and sensitive data are part of the cloud service's asset pool.
- **Risk identification:** Look for possible risks and threats that could hurt the cloud service's privacy, security, or ability to be used. This can include risks like unauthorized entry, data leaks, system failures, and threats from inside the organization.
- **Risk analysis:** Analyse the risks you've found to find out what they might mean, how likely they are to happen, and what might happen as a result. This research helps prioritize risks so that more steps can be taken to reduce them.
- **Risk evaluation:** Evaluate the risks you have found based on how bad they are and put them in order of how important they are to fix. This step looks at how the change might affect the cloud service provider, its customers, and the data they store.

How cloud security works with shared responsibility

The shared responsibility model is a system that shows how a CSP and its customer should handle security. It is like renting an apartment, the landlord takes care of the building, but you are responsible for keeping your area tidy and safe.

The security of the underlying cloud infrastructure is the responsibility of the **Cloud Service Provider (CSP)**. The physical security of the data centers is also taken care of by them.

The customer is in charge of securing the data and apps they store or use in the cloud. This includes securing their gadgets used to access the cloud, data encryption, and user access control.

A quick look at cloud computing model

Different models for cloud computing offer different amounts of service and responsibility:

- **Infrastructure as a Service (IaaS):** You rent everything you need to build something, like computers, storage, and networking. In terms of security and configuration, you have the most control but also the most responsibility. It's kind of like renting a simple office.