

ISC2 Certified Cloud Security Professional (CCSP) Exam Guide

*Essential strategies for compliance,
governance, and risk management*

Kim van Lavieren



www.bpbonline.com

First Edition 2024

Copyright © BPB Publications, India

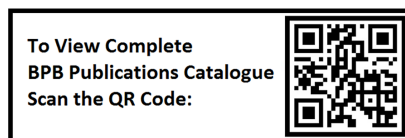
ISBN: 978-93-55517-654

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.



Dedicated to

My loving wife:

Sarah van Lavieren

&

My grandparents:

Fred and Ada

About the Author

Kim van Lavieren is currently a managing consultant at SimplifyNow. Throughout his career, he has helped many organizations bolster their security. His experience ranges from security engineering (at a FANG company) to architecture to the boardroom as a CISO. He holds an MSc in cybersecurity and a BSc in software engineering. Throughout his career, he has obtained a wide variety of (cloud) security certifications, including (but not limited to): CCSP, CISSP, CISM, CISSP-ISSEP, CISSP-ISSAP, CISSP-ISSMP, CSSLP, CGRC, Microsoft Certified: Cybersecurity Architect Expert, and the AWS Security Specialty.

About the Reviewers

- ❖ **Thomas** has a wealth of experience architecting and delivering cloud-native solutions to global organizations of all sizes. Being recognized as a ‘leader who coaches’, Thomas is proficient at leading teams as part of larger solution delivery projects or working independently within a virtual team to deliver on specific solution areas.

He has experience of working in the Microsoft channel and recently in a well-regarded Cyber Risk organization. Tom was responsible for the overall platform architecture of solutions delivered across several SIEM, EDR, NDR, and EASM vendors.

Tom has earned a mix of vendor certifications from Microsoft, Swimlane, and Armis and holds the ISC2 Certified Cloud Security Professional qualification, demonstrating expertise in multiple domains covering compliance, governance, and cloud security.

- ❖ **Fouad** is a seasoned Lead Consultant and Cloud Security Architect with 15 years of professional experience in the digital and software industry at global corporations. Fouad excels in designing and implementing comprehensive cloud solutions across multi-cloud platforms. He has assisted numerous businesses in effectively governing and safeguarding their information, proactively identifying cybersecurity risks, and enabling them to make informed and strategic business decisions. Fouad is CISSP, CISM, CASP+ certified.

- ❖ **Dwayne Natwick** is the CEO of Captain Hyperscaler, LLC, a technical cloud and cybersecurity training company. Dwayne was previously the Global Principal Cloud Security Lead at Atos, a multi-cloud GSI. He has been in IT, security design, and architecture for over 30 years. His love for teaching led him to become a Microsoft Certified Trainer (MCT) Regional Lead and a Microsoft Most Valuable Professional (MVP) for Security and Azure.

Dwayne has a master’s degree in Business IT from Walsh College, the CISSP, CGRC, SSCP, and CCSP from ISC2, CRISC from ISACA, and 18 Microsoft certifications, including Identity and Access Administrator, Azure Security Engineer, and Microsoft 365 Security Administrator. Dwayne can be found providing and sharing

information on social media, industry conferences, his blog site, and his YouTube channel.

Originally from Maryland, Dwayne currently resides in Michigan with his wife and three children.

- ❖ **Pushkar Nagle** is an InfoSec professional with 13 years of experience, holding professional IT certifications, including CCSP, CISSP, CISM, CEH, and CCNA. Pushkar attained a Licentiate Diploma in Electronics from VJTI, a B.Engg. in Electronics from Mumbai University. Pushkar has held several positions, including penetration tester, vulnerability manager, risk management advisor, and application security consultant. Pushkar has experience in handling large and complex penetration testing projects, providing risk advisory to businesses, and assisting organizations in vulnerability remediation.

Pushkar has managed 500+ onsite/offsite Web Application pentests, Mobile applications, Infrastructure, Build & Code reviews, and other risk-based security testing projects.

- ❖ **Andy Pantelli** is CISSP, CCSP, ACIIS, CCNP Security, CCNP Ent, CCDP, CCNA Cyber Ops, CCNA Security, JNCIP-E, VMware VCP, AWS Cloud Practitioner and Mimecast Secure Email Gateway certified. Previously serving in the Armed Forces, he completed 2 operational tours of duty before settling in the North West of England. He has over 20 years experience in Information Security across the Aviation, Financial, Legal, & Global Media sectors. He is currently a Cyber Security Architect consulting for the UK Central Government.

Acknowledgement

There are a few people I want to thank for their continued and ongoing support, both concerning this book and my cybersecurity career in general.

Firstly, I want to thank my wife for her tireless encouragement and support while writing my first book. I also want to thank my father for his extensive review work throughout the writing process.

Secondly, I want to thank my long-time mentors, “Coach Ron” Woerner and Ralph de Graaf. They have played a vital role in my security journey and have helped me get to where I am now.

Additionally, I want to thank my employer, SimplifyNow, for always supporting my professional growth and allowing me time to dedicate to this book. Together, we are building a safer world.

Lastly, I want to thank the publishing team at BPB for their extensive support, guidance, and assistance in making this book a reality.

Preface

The book will teach you the contrasts and similarities between cloud and on-premises computing. Show you reliable mechanisms to create a secure cloud environment, from the strategic to the operational level. It highlights what security controls help you create a secure cloud from the start and guides you into setting up security processes to keep your cloud secure over time.

The (ISC)2 CCSP is the industry's most sought-after vendor-agnostic cloud security certification. This book prepares you to pass the exam and excel within your business by providing tangible and concrete mechanisms to secure your organization's cloud environment.

The book takes you on a journey throughout all facets of secure cloud computing, from the policies an organization should have to the technical nitty-gritty of securing security groups. The book uses real-life examples, experiences, and tips and tricks from one of the industry's most broadly certified ISC2 professionals.

The book is divided into 24 chapters that cover the domains of the ISC2 CCSP exam. The details are listed below:

Chapter 1: Understanding Cloud Computing Concepts - Cloud computing is different from on-premise computing in many aspects. This chapter highlights definitions related to cloud computing and examines the shared responsibility model between Cloud Service Providers and customers. The chapter reviews cloud computing characteristics and common technologies in the cloud domain and explores the different levels and models for cloud computing

Chapter 2: Concepts and Design Principles of Cloud Security - Security in the cloud relies on foundational concepts and design principles. This chapter explores how cryptography, **Identity and Access Management (IAM)**, network security, and other concepts form the building blocks of cloud security.

Chapter 3: Evaluating Cloud Service Providers - In a world with a wide variety of Cloud Service Providers, it is challenging to pick a provider that meets your requirements. This chapter helps you pick a CSP by providing methods to evaluate different vendors against your business requirements

Chapter 4: Discover, Classify, and Manage Cloud Data - Storing data in the cloud may sound scary, however, implementing good mechanisms to discover, classify, and manage data in the cloud will offer you unprecedented data security.

Chapter 5: Cloud Storage Architectures and their Security Technologies - Now that you know how data “lives” in the cloud, it is time to explore how different architectures support data types. This chapter explores different architectures for data storage, the threats they face, and what security technologies should be implemented for them.

Chapter 6: Cloud Infrastructure and Components - Cloud infrastructure relies on similar components as on-premise computing. However, how cloud computing is managed is very different from on-premise computing. This chapter explores how cloud infrastructure is set up, used, and managed securely.

Chapter 7: Datacenter Security - You might have heard, “The cloud is just someone else’s computer”. In this chapter, we explore how data center security is a vital part of cloud computing, regardless of the service model.

Chapter 8: Risk Management in the Cloud - The cloud comes with new and familiar risks, this chapter examines how you can effectively manage and analyze risks within a cloud platform or cloud infrastructure.

Chapter 9: Cloud Security Controls - Understanding and managing risks is extremely important. However, picking the correct controls to (cost) effectively mitigate risk can be extra challenging in the cloud. This chapter covers how you can implement security controls within your cloud environment.

Chapter 10: Business Continuity and Disaster Recovery - While we design for systems and applications to be resilient, things go wrong sometimes. This chapter dives into ensuring your business continuity is ensured, even when things go wrong. The chapter also explains strategies on how to recover from disasters if they do occur.

Chapter 11: Secure Deployment, Awareness, and Training - The cloud offers new perspectives and tools for security, however, developing insecurely is as dangerous in the cloud as it is on-premise. This chapter explores common pitfalls, cloud-based vulnerabilities, and development tactics to ensure the software is developed securely within or outside of the cloud.

Chapter 12: Security Testing and Software Verification - Secure development is essential in creating a secure (cloud) ecosystem. However, while we always aim to develop securely, we must verify that we did so. This chapter explores the role of security testing methods such as static and dynamic code analysis, code review, penetration testing, and functional and non-functional testing. The chapter also sheds light on how APIs can be secured, and vulnerabilities within dependencies or open-source software can be detected.

Chapter 13: Specifics of Cloud Security Architecture - Cloud computing allows us to look at security from a different perspective. This means that we also have to use security

tooling in different places and in different ways. This chapter explores supplemental cloud security components such as web applications firewalls, API gateways, and database activity monitoring. Moreover, the chapter dives into encryption in the cloud, security of virtualization through containers, microservices, and sandboxing

Chapter 14: Identity and Access Management - Broad access is one of the characteristics of the cloud. However, to have broad access and be secure, we must manage identities effectively and securely. This chapter explores how SSO (single sign-on), IdP (identity providers), user federation, secrets management, multi-factor authentication, and **cloud access security brokers (CASB)** form the puzzle pieces of secure access in the cloud.

Chapter 15: Infrastructure Security - While **cloud service providers (CSPs)** take over a lot of security responsibilities, it is essential to understand the underlying technologies that enable the security functions. This chapter explores how hardware security

models, trusted platform modules, and hypervisor security allow CSPs to create a secure computing environment for their customers.

Chapter 16: Secure Configuration - Security tooling and complex cloud architectures can improve security, however, the configuration powering the tools and systems is what ultimately decides if an ecosystem is secure. This chapter explores the different security policies that must be in place to create a secure environment. It dives into secure network configuration, network security controls, OS Hardening, patch management, Infrastructure as Code, High Availability, Monitoring of performance and hardware, backup, and restore.

Chapter 17: Security Operations - Policies and configuration are essential to create a secure baseline within your environment. However, security processes ensure your environment stays secure over time and adapts to emerging threats. This chapter further expands on security policies, digital forensics, security operations like SOC, SIEM, incident management, and how to communicate with customers, vendors, partners, and others if all our controls prove to be ineffective.

Chapter 18: Legal and Regulatory Requirements in the Cloud - Cloud computing has many benefits, it offers better availability, for example. Some of these characteristics have drawbacks. When talking about legal requirements, the dispersion of data can complicate the scope of regulations your organization must adhere to. This chapter explores various legal requirements and risks associated with computing in the cloud.

Chapter 19: Privacy - Similar to legal requirements, privacy issues can become more complicated in the cloud. It is essential to approach privacy with a well-thought out approach. This chapter zooms in on country-specific legislation, data categories, jurisdictions for privacy, standard privacy requirements, and privacy impact assessments.

Chapter 20: Cloud Auditing and Enterprise Risk Management - The work of developers, system admins, and security engineers is not the only work that changes when switching to cloud computing. Auditors have had to change their approach as well. In an environment with shared responsibilities, auditing can be challenging. This chapter equips you with tactics, tips, and tricks on auditing processes within the cloud, the types of audit reports you might require of a CSP, how you plan audits, and how you can provide auditors with the data they need before they ask for it.

Chapter 21: Contracts and the Cloud - When you decide to use cloud computing within your ecosystem, how you purchase services changes significantly. You will have to ensure the services you purchase live up to your organization's expectations. This chapter explores how you can use service-level agreements, master service agreements, and statements of work to ensure you get the services you need. While vendor, contract, and supply chain management ensure you can prevent issues now and in the future.

Chapter 22: Duties of a CCSP - Passing the CCSP exam allows you to join a select group of cloud security experts. However, being a CCSP or associate of ISC2 also bears Responsibilities. In this chapter, the responsibilities of a CCSP are highlighted based on the ISC2 code of ethics.

Chapter 23: Exam Tips - The exam tips section highlights a breakdown of the exam process and provides tips and tricks to approach the exam most effectively.

Chapter 24: Exam Questions - The exam prep section contains a CCSP practice exam to test your knowledge across the six different domains.

Code Bundle and Coloured Images

Please follow the link to download the *Code Bundle* and the *Coloured Images* of the book:

<https://rebrand.ly/kj3cv76>

The code bundle for the book is also hosted on GitHub at

<https://github.com/bpbpublications/ISC2-Certified-Cloud-Security-Professional-Exam-Guide>

In case there's an update to the code, it will be updated on the existing GitHub repository.

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. Understanding Cloud Computing Concepts	1
Introduction	1
Structure	1
Objectives	2
Essence of cloud computing	2
Cloud comes in many shapes.....	3
Operating (in) the cloud.....	6
Shared responsibility	8
Cloud reference architecture	10
Building block technologies	12
<i>Networking</i>	12
<i>Storage</i>	15
<i>Virtualization</i>	15
<i>Databases</i>	16
<i>Orchestration</i>	16
Impact of cloud computing on other technologies	17
Cloud shared considerations.....	18
Conclusion	20
Learning goals	20
2. Concepts and Design Principles of Cloud Security	21
Introduction	21
Structure	21
Objectives	22
Common threats.....	22
Cloud design patterns	26
Business impact analysis.....	26
Cloud secure data lifecycle	29

Identity management, access control, and authorization	32
Cryptography and key management	37
Data and media sanitization.....	38
Network security.....	39
<i>Regions</i>	39
<i>Availability zones: AVs</i>	40
<i>Access control lists: ACLs</i>	41
<i>Security groups: SGs</i>	41
<i>Private connections</i>	42
<i>Web application firewalls: WAFs</i>	43
Virtualization security	43
Security hygiene	44
DevOps security	45
Conclusion	49
Learning goals	50
3. Evaluating Cloud Service Providers	51
Introduction	51
Structure	51
Objectives	52
Portability	52
Interoperability	53
Availability	54
Security	56
Privacy	56
Auditability	57
Costs	58
Service level agreements	58
Legal and regulatory compliance	60
Product certifications.....	61
<i>Common Criteria</i>	61
<i>Federal Information Processing Standards (FIPS 140-2 and 140-3)</i>	62
Conclusion	63

Learning goals	63
4. Discover, Classify, and Manage Cloud Data.....	65
Introduction	65
Structure	65
Objectives	66
Data types.....	66
Data classification	68
Data flows	70
Data mapping	70
Data labeling.....	72
Policies	72
Data dispersion.....	75
Data retention and storage.....	76
Deletion and archival	77
Legal holds.....	79
Information Rights Management.....	80
Conclusion	81
Learning goals	82
5. Cloud Storage Architectures and their Security Technologies.....	83
Introduction	83
Structure	83
Objectives	84
Storage types.....	84
Threats to storage types	85
Encryption and key management.....	86
<i>Symmetric encryption</i>	<i>86</i>
<i>Asymmetric encryption or public key encryption.....</i>	<i>88</i>
<i>Block and Stream Ciphers</i>	<i>92</i>
<i>Common algorithms</i>	<i>93</i>
<i>Common attacks</i>	<i>93</i>
<i>Key size.....</i>	<i>94</i>
Hashing	95

Applications of encryption	99
Key, secrets, and certificate management	100
<i>Secure key generation</i>	101
<i>Key, secret, and certificate storage</i>	102
<i>Bring Your Own Key</i>	103
<i>Key Management System</i>	103
<i>Secrets management</i>	103
<i>Certificate Management System</i>	105
Data obfuscation, tokenization, masking, and anonymization.....	106
Data loss prevention	108
Tiering, CDNs, replication, and backups.....	110
Sample architecture.....	112
Conclusion	114
Learning goals	115
6. Cloud Infrastructure and Components	117
Introduction	117
Structure	117
Objectives	118
Physical environment.....	118
Network and communications.....	118
<i>Virtual networks/ virtual private clouds</i>	118
<i>Elastic IPs/ static public IPs</i>	121
<i>Load balancing</i>	122
<i>Stepping stones</i>	123
<i>Security groups/Access control lists</i>	124
<i>Encryption in transit</i>	125
<i>Zero Trust</i>	126
<i>VNet/VPC peering</i>	127
<i>VPNs</i>	127
<i>Direct connections</i>	129
<i>Web Application Firewall</i>	130

<i>Denial of Service protection</i>	131
<i>API Management</i>	133
Compute and virtualization	134
<i>Serverless</i>	134
<i>Containers</i>	136
<i>Virtual machines</i>	138
<i>Underlying infrastructure</i>	138
<i>Scaling</i>	138
<i>Hypervisor attacks</i>	139
<i>Other compute technologies</i>	139
Storage	139
<i>File storage, object storage, and block storage</i>	140
<i>Data lakes</i>	140
Management Plane	140
<i>Cloud console</i>	140
<i>Command Line Interface</i>	141
<i>APIs</i>	142
<i>Infrastructure as Code</i>	142
<i>Security</i>	143
Conclusion	143
Learning goals	144
7. Datacenter Security	145
Introduction	145
Structure	145
Objectives	145
Physical design	146
<i>Buy, lease, or build</i>	146
<i>Location</i>	147
<i>Security and safety</i>	148
<i>Intrusion detection</i>	153
<i>Construction materials</i>	153

<i>Regulatory requirements</i>	153
Environmental design	154
<i>Electric</i>	154
<i>Heating, cooling, and ventilation</i>	156
<i>Fire detection and suppression</i>	156
<i>Cabling</i>	158
<i>Multi-vendor pathway connectivity</i>	158
Resilient design	158
Logical design.....	160
<i>Tenant partitioning</i>	160
<i>Access control and identities</i>	160
Conclusion	161
Learning goals	162
8. Risk Management in the Cloud	163
Introduction	163
Structure	163
Objectives	164
Risks 164	
Risk assessments	167
Risk treatment and mitigation strategies.....	170
Risk frameworks	171
Metrics for risk management	173
Vendor risk management.....	175
Cloud vulnerabilities, threats, and attacks.....	176
Roles in data handling.....	176
Common laws and regulations.....	177
<i>Breach notification laws</i>	177
GDPR	178
California Consumer Privacy Act.....	178
Sarbanes-Oxley	179
<i>Other laws and the exam</i>	179
Conclusion	179

Learning goals	180
9. Cloud Security Controls.....	181
Introduction	181
Structure	181
Objectives	182
Physical and environmental protection	182
System, storage, and communication protection	182
<i>Host-based intrusion detection and prevention</i>	183
<i>Data loss prevention and proxying</i>	183
<i>Host-based firewall</i>	184
<i>Anti-virus</i>	185
<i>Vulnerability scanning and secure configuration</i>	185
<i>Baselining and secure configuration</i>	185
<i>Principle of least privilege</i>	186
<i>Infrastructure as code and immutable systems</i>	187
<i>Mobile device management</i>	187
Identity and access management.....	188
<i>Role-based access control</i>	188
<i>Attribute-based access control</i>	189
<i>Discretionary access control</i>	189
<i>Mandatory access control</i>	190
Access controls	190
<i>Two-factor authentication/ multi-factor authentication</i>	190
<i>Separation of duties</i>	190
<i>Two-person control</i>	191
<i>Passphrases and passwords</i>	191
<i>Lockouts</i>	191
<i>Rotation and invalidation</i>	192
<i>Session lifespan</i>	192
<i>Out-of-band management and emergency credentials</i>	193
<i>Mutual certificate authentication</i>	193
Audit mechanisms	194

Logging.....	194
Monitoring	195
Security incident and event monitoring	196
Security operations center	196
Security orchestration, automation, and response	197
Job rotation and mandatory vacations.....	198
Conclusion	198
Learning goals	198
10. Business Continuity and Disaster Recovery	199
Introduction	199
Structure	199
Objectives	200
Business continuity and disaster recovery strategy	200
NIST 800-34: Information system contingency planning process	202
Business requirements.....	202
RTO, RPO, and recovery service levels	203
Controls	203
Backups.....	203
Redundancy/ fail-over	204
Hot site	204
Warm site.....	205
Cold site.....	205
Mutual agreements	205
On-premises and cloud	205
Succession planning.....	206
Testing of BC/DR plans	206
Actors	206
Testing	207
Walkthrough.....	207
Table-top	207
Failover/parallel tests	207

<i>Simulation tests</i>	207
Conclusion	208
Learning goals	208
11. Secure Development, Awareness, and Training	209
Introduction	209
Structure	209
Objectives	210
Development methodologies	210
<i>Waterfall</i>	210
<i>Agile</i>	211
<i>Rapid application development</i>	211
<i>DevOps</i>	212
<i>DevSecOps</i>	212
Secure software development life cycle	212
<i>Planning</i>	213
<i>Feasibility or requirements analysis</i>	213
<i>Designing</i>	214
<i>Development</i>	214
<i>Testing</i>	215
<i>Secure operations and maintenance</i>	219
<i>Disposal</i>	219
<i>Secure software development framework</i>	220
Secure coding and development.....	220
<i>Shift-left</i>	220
<i>Requirements gathering</i>	221
<i>Design</i>	221
<i>Threat modeling</i>	222
<i>STRIDE</i>	222
<i>DREAD</i>	223
<i>ATASM</i>	224
<i>PASTA</i>	224

<i>Threat intelligence</i>	225
<i>Code review</i>	225
<i>Linting</i>	226
<i>Code testing</i>	226
<i>Version control</i>	226
<i>Commit signing</i>	227
<i>Open-Source software and dependencies</i>	228
<i>Software Bill of Materials</i>	229
<i>Configuration and secrets</i>	229
<i>Deployment, building, and CI/CD</i>	230
<i>Separating environments</i>	230
<i>Monitoring and logging</i>	231
<i>OWASP</i>	231
<i>SANS Top 25</i>	233
<i>ASVS</i>	235
<i>Penetration testing</i>	235
<i>SAST and DAST</i>	236
Security awareness and training	236
<i>Awareness versus training</i>	237
Recurrence	238
<i>Positivity</i>	238
Conclusion	238
Learning goals	239
12. Security Testing and Software Verification	241
Introduction	241
Structure	241
Objectives	242
Functional and non-functional testing	242
Security testing methodologies	243
<i>Abuse case testing</i>	243
Black, gray, and white box penetration testing	245

<i>Static application security testing and dynamic application security testing</i>	246
<i>Software composition analysis</i>	247
<i>Interactive application security testing</i>	247
Quality assurance.....	247
Supply-chain.....	249
<i>SOC II type II</i>	250
<i>ISO 27001 certification</i>	250
Third-party and open-source software	251
Conclusion	252
Learning goals	252
13. Specifics of Cloud Security Architecture	253
Introduction	253
Structure	253
Objectives	253
Web application firewall	254
Database activity monitoring.....	257
API gateways.....	257
Virtualization and orchestration.....	258
<i>Sandboxing</i>	259
<i>Honey potting</i>	259
Conclusion	259
Learning goals	260
14. Identity and Access Management	261
Introduction.....	261
Structure	261
Objectives	262
Identity and access management.....	262
Identity providers	265
Single sign-on	267
Multi-factor authentication.....	271
Cloud access security brokers	273

Secrets management	275
Conclusion	275
Learning goals	276
15. Infrastructure Security	277
Introduction	277
Structure	277
Objectives	278
Infrastructure and multi-tenancy.....	278
Hardware security module.....	279
<i>FIPS 140-2 and FIPS 140-3</i>	281
<i>PCI-DSS</i>	282
Trusted Platform Module.....	282
Hypervisor security	284
Guest OS security	287
Conclusion	291
Learning goals	292
16. Secure Configuration	293
Introduction	293
Structure	293
Objectives	294
Technology and service hardening.....	294
<i>Access control technologies</i>	295
OS hardening.....	302
<i>Updates, patches, and immutable infrastructure</i>	302
<i>Monitoring and logging</i>	307
<i>Host-based security controls</i>	308
Infrastructure as Code.....	309
Information Technology Infrastructure Library and ISO/IEC 20000.....	310
Change management.....	311
Continuity management.....	312
Information security management.....	312

Continual service improvement management	312
Incident management.....	313
Problem management.....	314
Release management	315
Deployment management	316
Configuration management	317
Service level management	318
Availability management.....	319
Capacity management.....	319
Conclusion	320
Learning goals	321
17. Security Operations	323
Introduction	323
Structure	323
Objectives	324
Security policy and operations.....	324
Security processes	327
Security operations center	328
Security incident and event monitoring	332
Security orchestration, automation, and response.....	335
Artificial intelligence	337
Incident management and disclosure	338
Forensics	342
Chain of custody	345
Types of evidence.....	347
E-Discovery.....	347
Conclusion	349
Learning goals	350
18. Legal and Regulatory Requirements in the Cloud	351
Introduction	351
Structure	351
Objectives	352

Conflicting international legislation.....	352
General Data Protection Regulation.....	356
California Customer Privacy Act.....	357
Payment Card Industry: Data Security Standard.....	358
Evaluating legal risks in cloud environments	358
Legal frameworks and guidelines	360
Intellectual property	362
E-discovery (ISO/IEC 27050)	363
Forensics	364
Conclusion	364
Learning goals	365
19. Privacy	367
Introduction	367
Structure	367
Objectives	368
Privacy	368
Contractual versus regulated data	369
Data privacy and jurisdictions	372
Standard privacy requirements.....	373
Data Breach Notification Laws.....	378
Safe harbor agreements.....	378
Conclusion	379
Learning goals	380
20. Cloud Auditing and Enterprise Risk Management.....	381
Introduction	381
Structure	382
Objectives	383
Risk appetite	383
Risk management frameworks	384
Metrics for risk management	386
Data roles.....	386

Audit requirements.....	386
Internal and external audits.....	387
Logs and auditability.....	389
Audit challenges in the cloud.....	390
Audit scope	391
Stakeholder identification.....	392
Audit planning	392
Audit execution.....	393
Audit reports.....	393
Audit follow-up.....	394
Audit process summary	394
Systems and Organization Controls.....	395
Sarbanes-Oxley Act.....	397
CSA STAR.....	397
Gap analysis.....	397
Information security management system.....	398
Information security controls.....	398
PCI-DSS	398
HIPAA.....	399
HITECH.....	400
NERC/CIP	400
GDPR	400
Legal and regulatory landscape.....	400
Conclusion	401
Learning goals	402
21. Contracts and the Cloud.....	403
Introduction	403
Structure	403
Objectives	404
Service-level agreements.....	405
Master service agreement	407
Statement of work.....	407

Vendor management.....	408
Vendor assessments	408
Vendor lock-in risks	408
Vendor viability	409
Escrow.....	409
Contract management	409
Right to audit	410
Metrics	411
Definitions.....	411
Termination.....	412
Litigation	413
Assurance	414
Compliance	414
Access to cloud data	415
Cyber risk insurance.....	415
Supply-chain management.....	416
Conclusion	416
Learning goals	417
22. Duties of a CCSP	419
Introduction	419
Structure	419
Objectives	420
ISC2 code of ethics	420
How to certify	421
Certification requirements	422
Endorsement.....	422
Evidence	422
Maintaining certification.....	422
Local chapters.....	423
Cloud community	423
Conclusion	423

Learning goals	424
Further reading.....	424
23. Exam Tips.....	425
Introduction	425
Structure	425
Objectives	426
Exam scheduling.....	426
Testing center	427
Exam contents and requirements	428
Question types.....	429
Keywords	429
Breaks.....	430
Conclusion	430
24. Exam Questions	431
Introduction	431
Structure	431
Quick self-assessment.....	432
Self-assessment answer key.....	436
Practice exam	438
Practice exam answer key	463
Index	471-484

CHAPTER 1

Understanding Cloud Computing Concepts

Introduction

Cloud computing is different from on-premise computing in many ways. This chapter helps you understand the various forms of cloud computing. This chapter will introduce you to the characteristics of cloud computing and standard technologies found in the cloud. It also examines the cloud reference architecture, which outlines responsibilities between **Cloud Service Providers (CSPs)**, cloud consumers, brokers, and auditors.

Structure

This chapter covers the following topics:

- Cloud computing characteristics
- Public cloud, private cloud, hybrid cloud, community, and multi-cloud
- Cloud operating models (IaaS, PaaS, and SaaS)
- Shared responsibility model
- Cloud reference architecture
- Building block technologies (virtualization, storage, networking, databases, and orchestration)

- Cloud computing characteristics
- The impact of cloud technology

Objectives

In this chapter, you will be able to understand the concepts of cloud computing. You will gain an understanding of the different shapes of cloud computing, the related service models, and the characteristics of cloud computing overall. The chapter will outline how cloud computing environments can integrate with an organization's IT landscape. It will also cover the strengths and weaknesses every cloud computing service model presents and help you determine which model is suitable in what situation. The chapter covers all building block technologies you will see in cloud computing environments while also helping you outline the responsibilities within the cloud.

Essence of cloud computing

Cloud computing. Many people do not know what to expect when they hear this term. However, the essence of cloud computing is simple. Cloud computing is using someone else's computing resources for your computation needs.

Throughout the past decades, we have already been working with forms of cloud computing. Think of web applications offered by third-party providers (**Software as a Service**) or even companies like **Azure** that allow you to rent servers and infrastructure (**Infrastructure as a Service**).

The main difference between current-day cloud computing and the examples above is that companies have branded themselves as **cloud service providers (CSPs)**. These CSPs have adopted a business model of providing computing services to their customers through on-demand self-service in a scalable fashion. A web hosting company allows you to rent a pre-defined number of servers. But a CSP lets you (automatically) start and create new servers to accommodate more traffic or stop servers or instances when you no longer need them. We call this rapid concept elasticity.

Cloud computing has more benefits than past-day hosting models. One of them is called **measured service**. Measured service means that your usage of the CSPs services is continuously measured, and you only pay for what you use. Combined with rapid elasticity, this offers some attractive benefits.

For example, if your company uses an internal application only during work hours, you can shut down the servers that support the application after work hours. Meaning you would only pay for the hours that the servers were running. If you have a workday from 9 am until 5 pm, you would only pay for 8 hours of operation.

Of course, you could do this in your data center, but you would have to shut down an entire server to save on energy costs. Since you already paid for the servers, turning

them off does not save as much money. If you use virtualization within your data center, shutting down a server might also impact other applications. In short, rapid elasticity can be challenging to achieve in **on-premise computing**.

CSPs use an operating model called **resource pooling** to facilitate rapid elasticity and measured service. Resource pooling means the provider has a pool of computing resources. For example, storage is assigned to a specific customer **on-demand**. On-demand assignment of resources means the following;

In the example above, your company only uses a server during work hours. Once the server shuts down, the available computing resources return to the pool. Similarly, if another CSP customer requires more resources, the compute capacity you just released becomes available to another customer.

EXAM TIP: Resource pooling is a significant risk of cloud computing as it involves sharing hardware resources with other organizations.

The effect of resource pooling is significant to CSPs as it allows them to serve multiple customers without having dedicated hardware for every customer. Limiting the amount of required hardware lets the CSPs control costs. However, it can also bring risks to the table. If customers demand more service than is available, the CSP might not have enough resources to satisfy demand, leading to service outages. On the flip side of this coin, when a CSP overprovisions its resources, and there is little demand, the CSP is incurring high costs for no returns. Many CSPs will offer customers reduced rates if they commit to a minimal pre-determined usage level. Such commitments allow the CSP to determine better how much hardware should be available, preventing the resources from being over- or under-leveraged.

The last characteristic of cloud computing is called **broad network access**. Broad network access means cloud computing resources are available to customers online. Most CSPs (like **AWS**, **Microsoft Azure**, and **GCP**) offers an online portal that allows you to log in and provision your resources on demand over the internet. Contrary to on-premise computing, where the need for new resources requires the purchase of new servers and access to the physical site of the devices. Broad network access makes cloud computing easy.

To summarize, NIST defines the five characteristics of cloud computing: on-demand self-service, broad network access, rapid elasticity, measured service, and resource pooling. These characteristics will be the red line throughout this book, presenting many significant strengths and specific security challenges.

Cloud comes in many shapes

Cloud computing is applicable in different ways. An organization might use cloud computing for all or some of its workloads. A computing cloud environment is creatable at different scopes as well. Some clouds serve a single company, while others might help

a whole community of companies. Regardless of the shape of cloud computing used, every model has its benefits and drawbacks. Lets us explore the different forms of cloud computing that exist.

Public cloud is probably one of the most well-known shapes of cloud computing. In a public cloud, a CSP provides cloud computing services to virtually anyone wanting to purchase them. The CSP wants to make it easy for customers to consume their services. Because a public cloud provides services to a broad audience, they usually are very good at self-service provisioning. However, a public cloud also means many customers share the available resources. When you share resources with other organizations, you must realize that this creates security risks.

An attacker on a completely unrelated company could cause service outages (or worse) to your organization. For example, if another customer is hosting a virtual machine on the same server your virtual machine is running, and an attacker can break out of the virtual machine of the other company, they can potentially disrupt the availability of the underlying server. Of course, cloud providers take measures to prevent such events from occurring, and we will examine those measures throughout the book.

Private cloud is a form of cloud computing where the hardware (and infrastructure) used is exclusive to a single customer, or the company itself owns and manages the hardware. A private cloud is generally more secure but almost always more costly. If the organization operates the private cloud, it also involves more effort and knowledge of secure design and operations. Many CSPs provide private cloud services to the customer by allowing them to reserve hardware for their organization only. Other large parties, like governmental agencies, even build their cloud computing environments in their data centers. When a company or governmental agency creates its cloud, they act as the CSP and the consumer. The consumer can then still benefit from the characteristics of cloud computing without having to share underlying infrastructure with other organizations.

Hybrid Cloud is a form of cloud computing where private and public clouds are combined. A hybrid cloud allows an organization to pick and choose where they want to process specific workloads. Determining where you process a workload will enable you to separate sensitive workloads. You might not want to process in a public cloud from everyday computing that does not require dedicated infrastructure. Public and private cloud environments are often connected using dedicated connections such as VPNs or even leased lines. The following table shows examples of the composition of different cloud shapes:

Public cloud	Private cloud	Hybrid cloud	Multi cloud
Microsoft	on-premise	on-premise	Microsoft
Azure	data center	data center	Azure
OR		AND	AND

Public cloud	Private cloud	Hybrid cloud	Multi cloud
Amazon Web Services (AWS)		Amazon Web Services (AWS)	Amazon Web Services (AWS)
OR			AND
Google Cloud Platform (GCP)			Google Cloud Platform (GCP)

Table 1.1: Examples of public, private, hybrid, and multi-cloud setups

Community cloud is a form of cloud computing where multiple organizations share the same computing environment. Community clouds are common for organizations that collaborate. For example, universities that perform research projects can benefit from using a shared cloud environment to process and share research results. Sharing a computing environment with other organizations can pose security risks, as every organization must ensure its internal security practices are in line.

For example, if university A uses usernames and passwords to authenticate and University B uses **Multi-Factor Authentication (MFA)**. Attackers would be far more likely to gain access to the environment through a compromised university A user. Therefore, it is essential to create a standard set of controls that establishes a security baseline of how the community cloud should be secured, configured, and operated between all organizations.

Multi-cloud is the last form of cloud computing to cover. A multi-cloud environment is an environment that exists out of multiple cloud environments. For example, a multi-cloud environment might have a **Microsoft Azure environment** and an **Amazon Web Services (AWS) environment**. Separating your computation needs over multiple clouds allows you to leverage specific tools that a CSP has to offer. Those tools might work better at one CSP than the other, or costs might be lower at one CSP than the other. However, many organizations also choose a multi-cloud environment to fight the risk of vendor lock-in. Vendor lock-ins are not specific to cloud computing and mean that you establish a dependency on a single vendor that might force you to keep doing business with them as your operations are highly dependent on the vendor.

In some cases, this dependency on a vendor can be dangerous. For example, a vendor promises to perform security patches daily per their **service level agreement (SLA)**. But it turns out your vendor does not do this. Your organization confronts the vendor, but the vendor refuses to fix the issue. Your organization might choose to pull out of the contract, but if all your online services are hosted at this vendor, pulling out might mean you have to shut down your services. Shutting down the services for a prolonged period can significantly damage an organization. Multi-cloud attempts to solve this, allowing you to build the same online services at two vendors. If you properly sync data between the environments, you can shut down the environment at the vendor you no longer want to work with and continue with the other vendor. Remember that not every multi-cloud