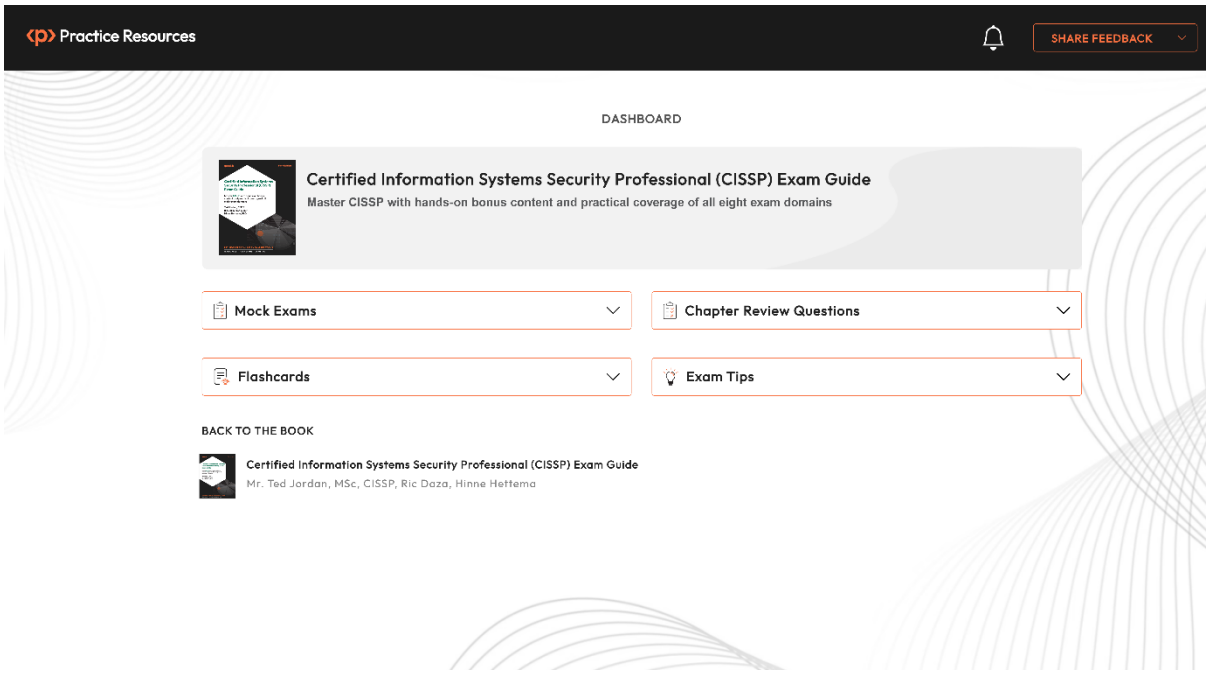
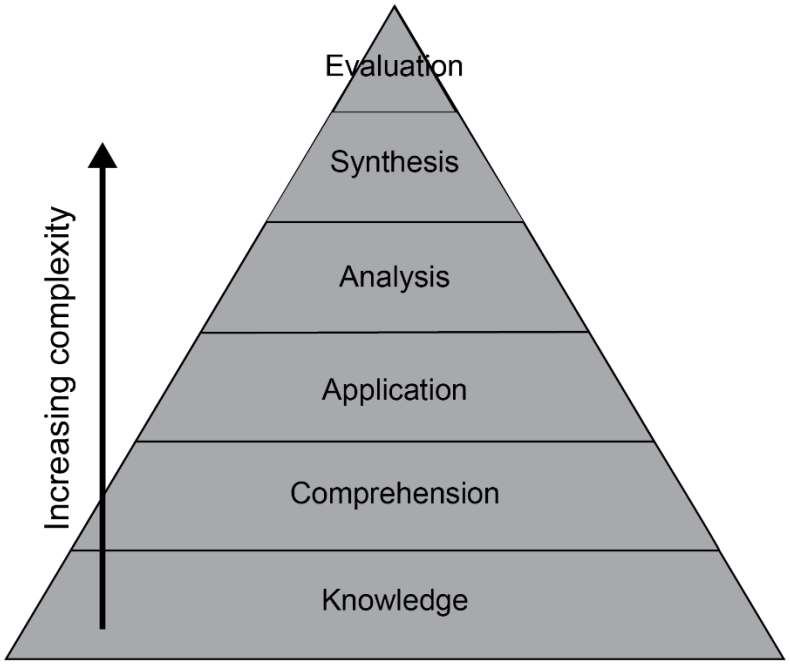
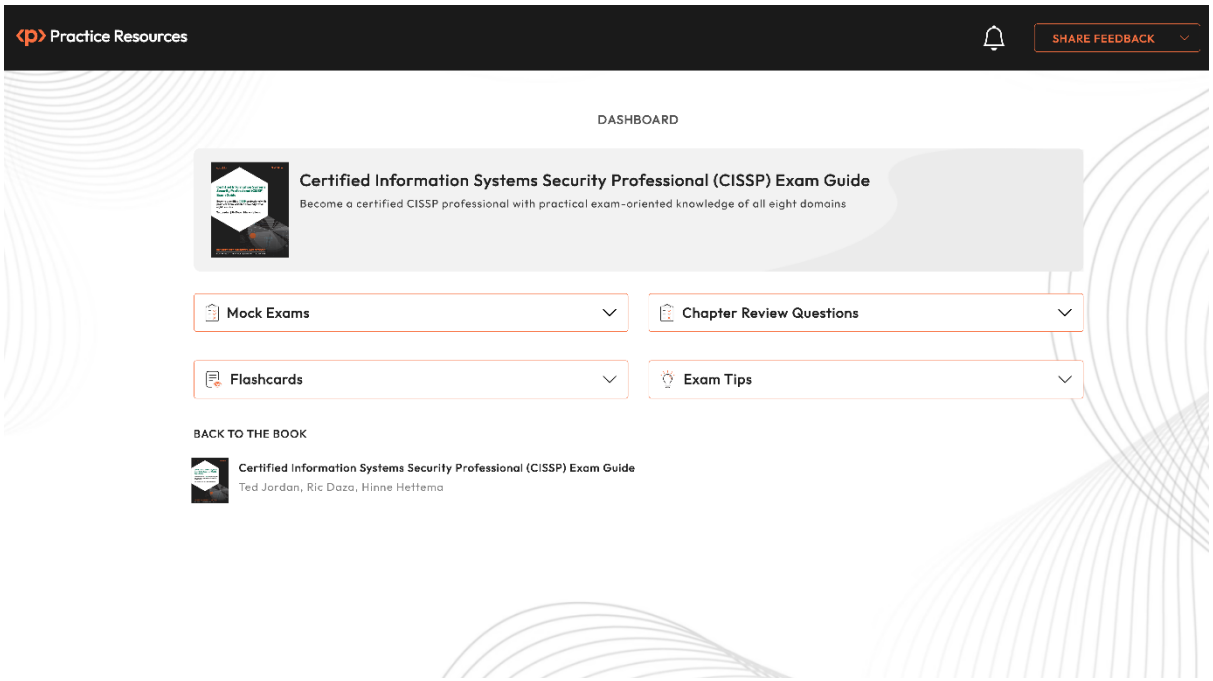
Certified Information Systems Security Professional (CISSP) Exam Guide

Introduction 1:

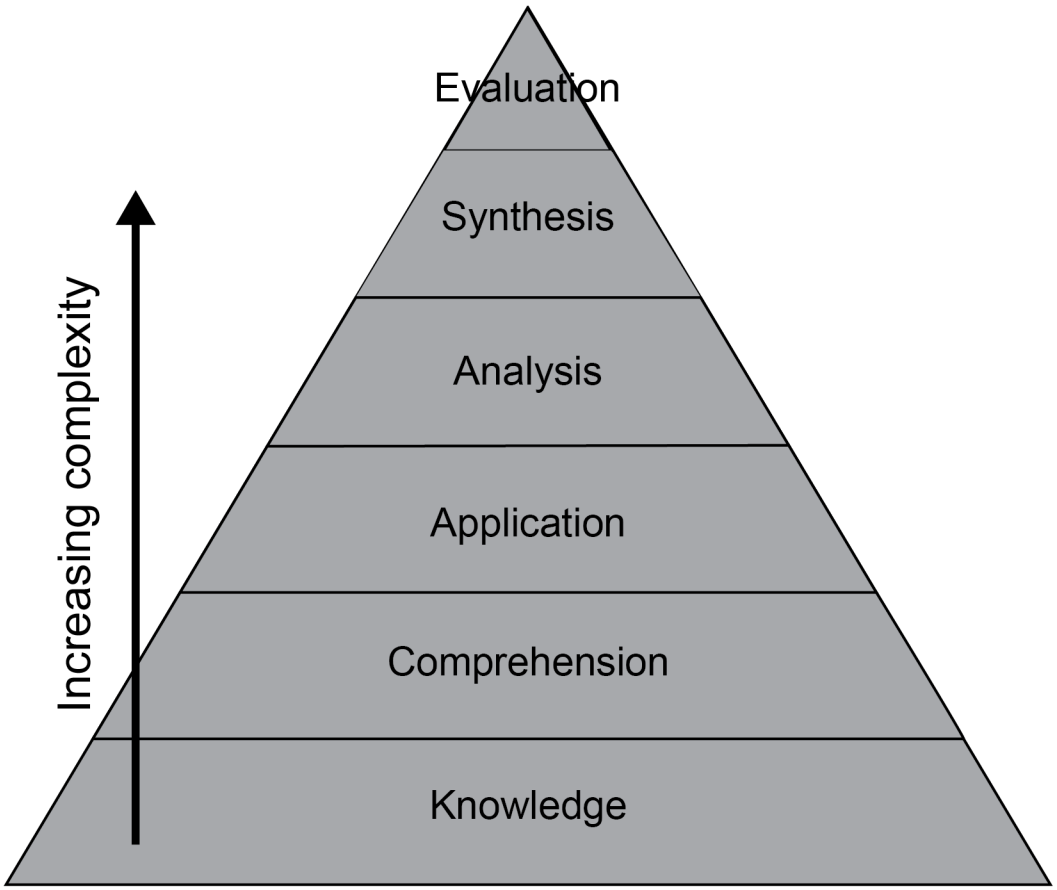




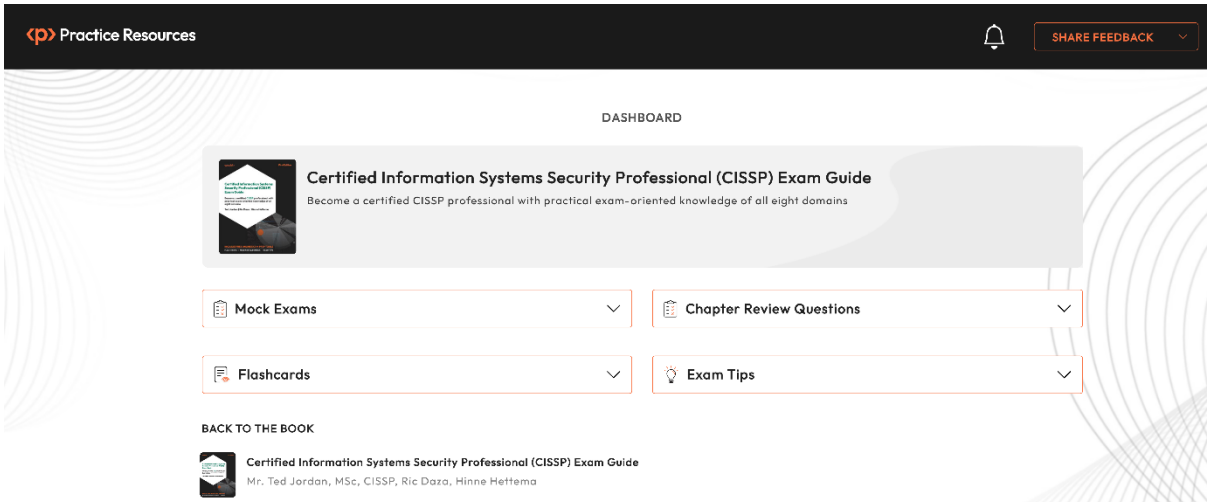
Preface:

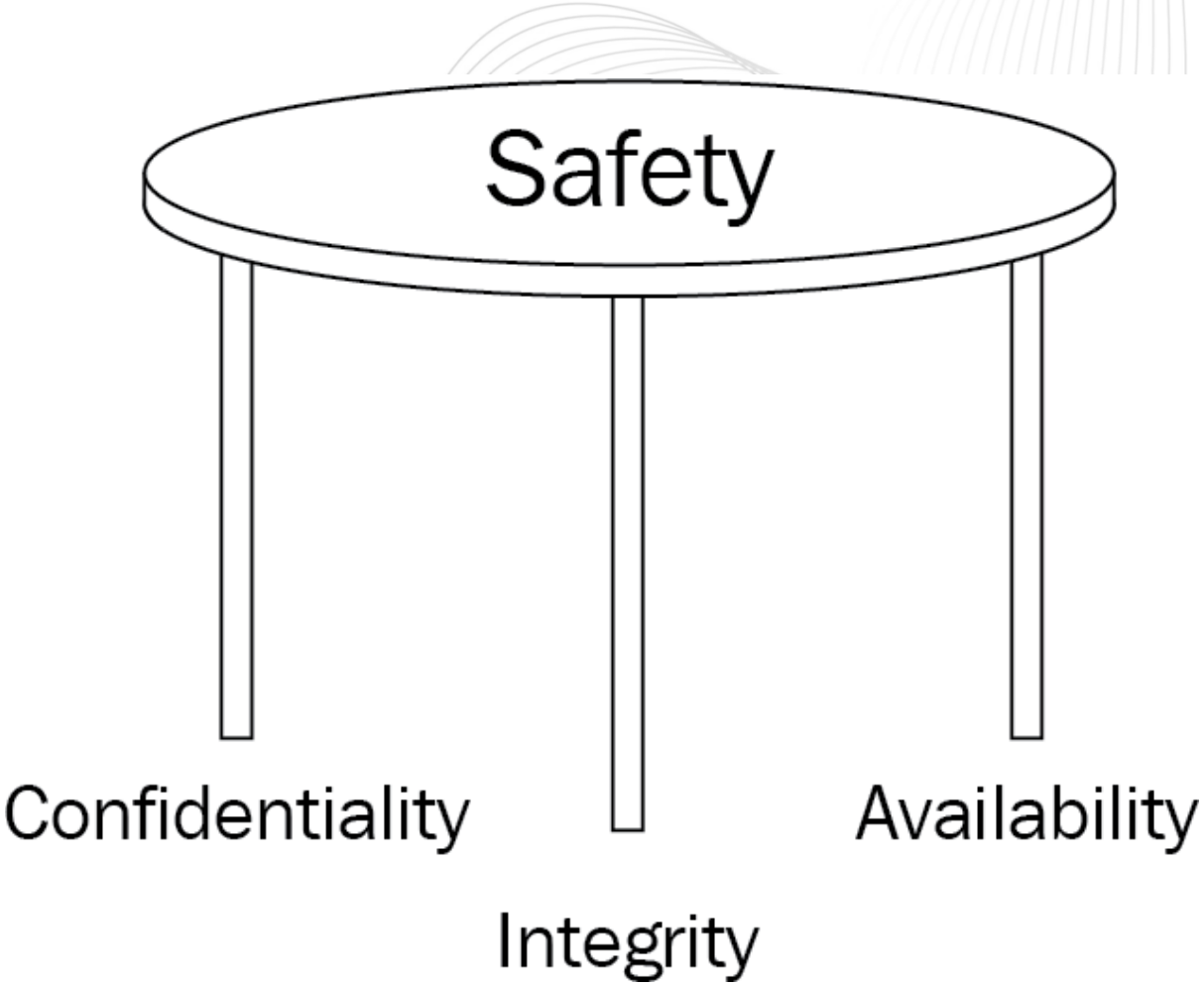

Practice Resources
SHARE FEEDBACK
DASHBOARD
Certified Information Systems Security Professional (CISSP) Exam Guide
Become a certified CISSP professional with practical exam-oriented knowledge of all eight domains
Mock Exams
Chapter Review Questions
Flashcards
Exam Tips
BACK TO THE BOOK
Certified Information Systems Security Professional (CISSP) Exam Guide
Ted Jordan, Ric Daza, Hinne Hettema

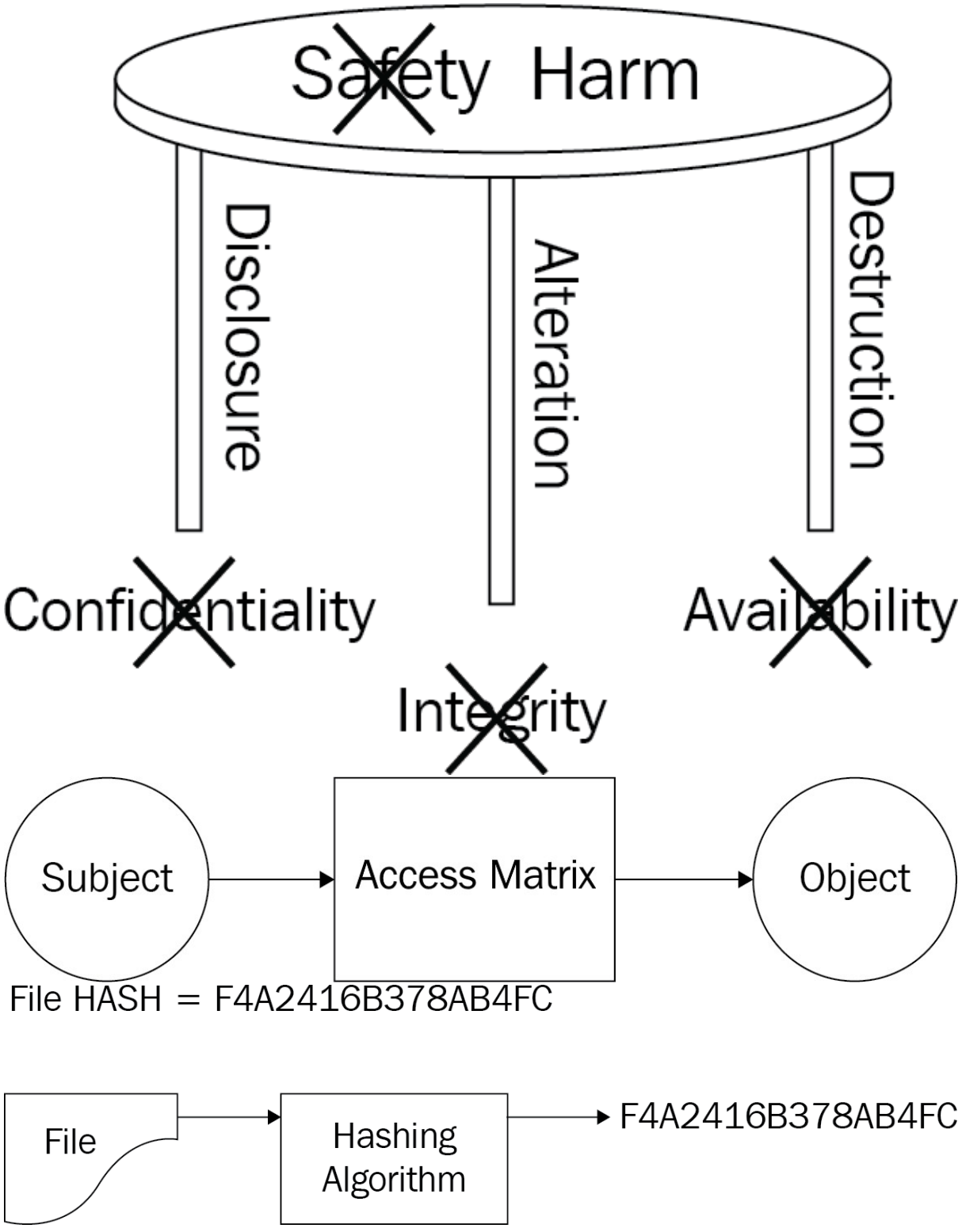
Introduction 1:

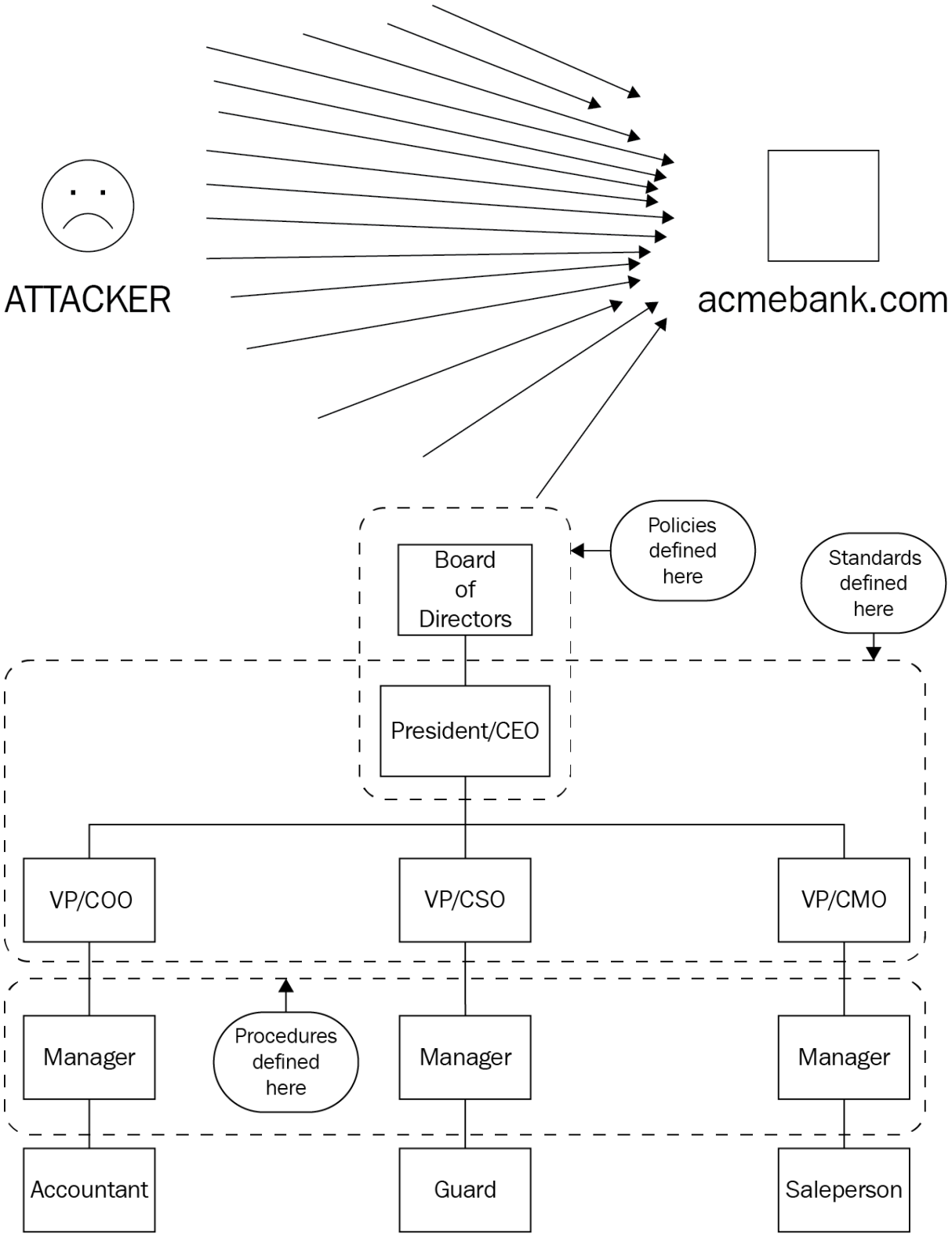


Chapter 1: ***Ethics, Security Concepts, and Governance Principles***






Safety Harm
Disclosure
Alteration
Destruction
Confidentiality
Availability
Integrity
Subject
Access Matrix
Object
File HASH = F4A2416B378AB4FC
File
Hashing Algorithm
F4A2416B378AB4FC


ATTACKER
acmebank.com
Board of Directors
Policies defined here
Standards defined here
President/CEO
VP/COO
VP/CSO
VP/CMO
Manager
Procedures defined here
Manager
Manager
Accountant
Guard
Saleperson

Ethics, Security Concepts, and Governance Principles

Summary

The important aspects of security revolve around three concepts: confidentiality, integrity, and availability. In this chapter, we learned that confidentiality allows users to protect data from being disclosed, integrity assures users that data has not been altered, and availability provides access to users when requested.

Authenticity ensures that the object originates from the source that is assigned to the file or data. Nonrepudiation ensures that messages are from the assigned sender, making them unable to deny sending the message.

A strong security governance principle uses multiple layers of protection, or defense in depth, because it provides the organization with a security backup if another control is defeated or fails.

Additionally, you learned about the importance of staff members following organizational policies. Failure to do so could result in data loss and human injury. Policies are defined by C-level executives and are created based on security governance and corporate goals.

To prevent companies from reinventing the wheel, there are security-governance frameworks that have been developed to help organizations create policies. These include ISACA, ISO, ITIL, NIST, HIPAA, and PCI-DSS. These frameworks are tested and trusted. Due care involves putting safety requirements in place, and due diligence is evidence that the mechanisms work. Finally, the CISSP must follow the ISC2 Code of Professional Ethics.

Chapter Review Questions

The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

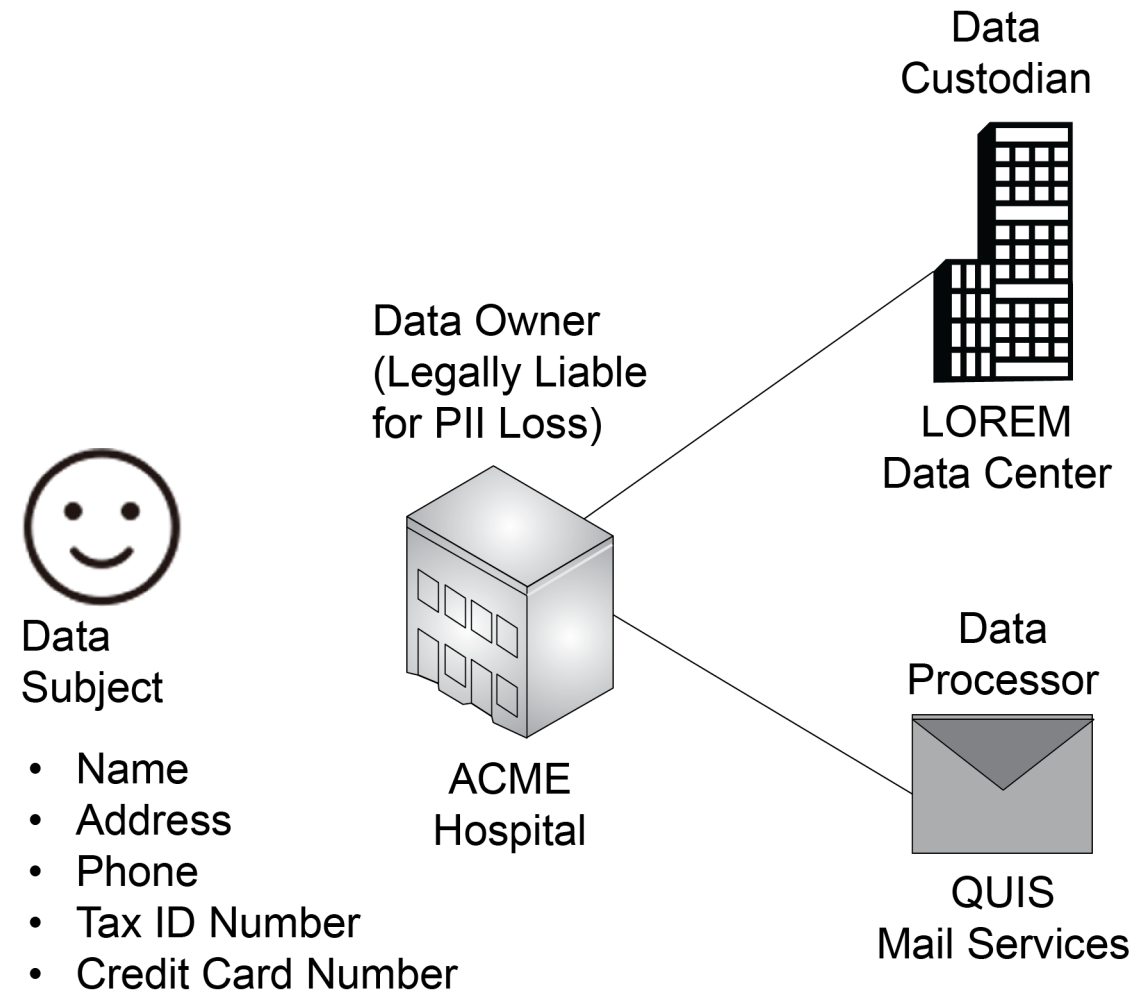
Select Quiz

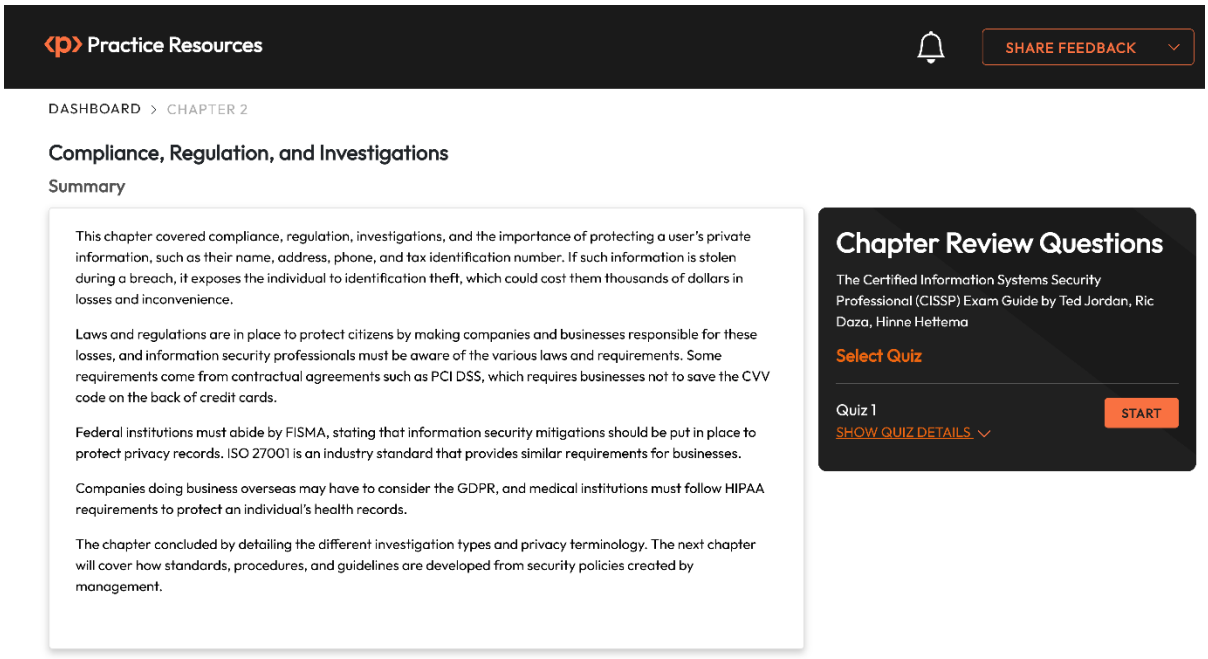
Quiz 1

START

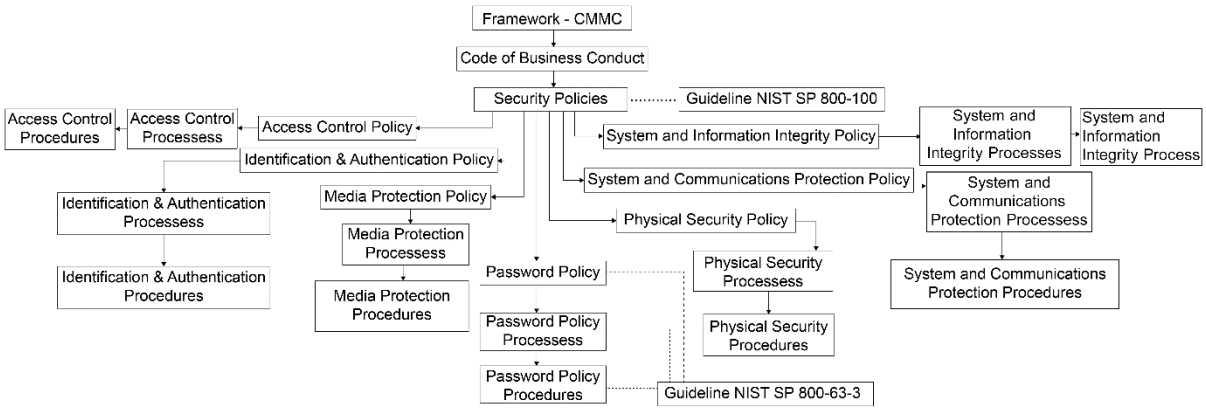
SHOW QUIZ DETAILS

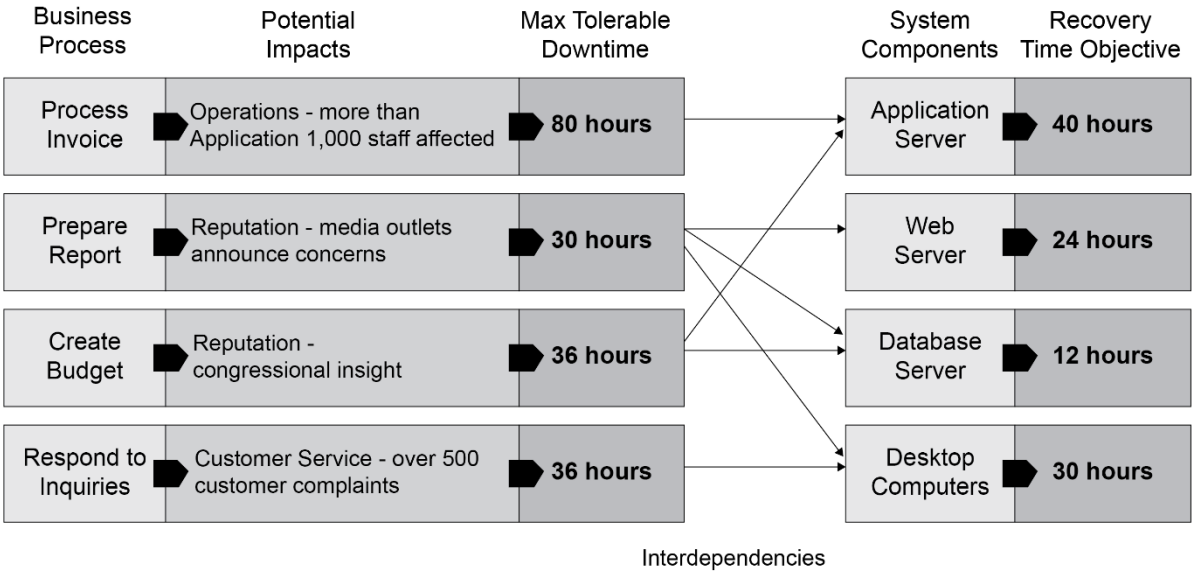
Chapter 2: *Compliance, Regulation, and Investigations*,

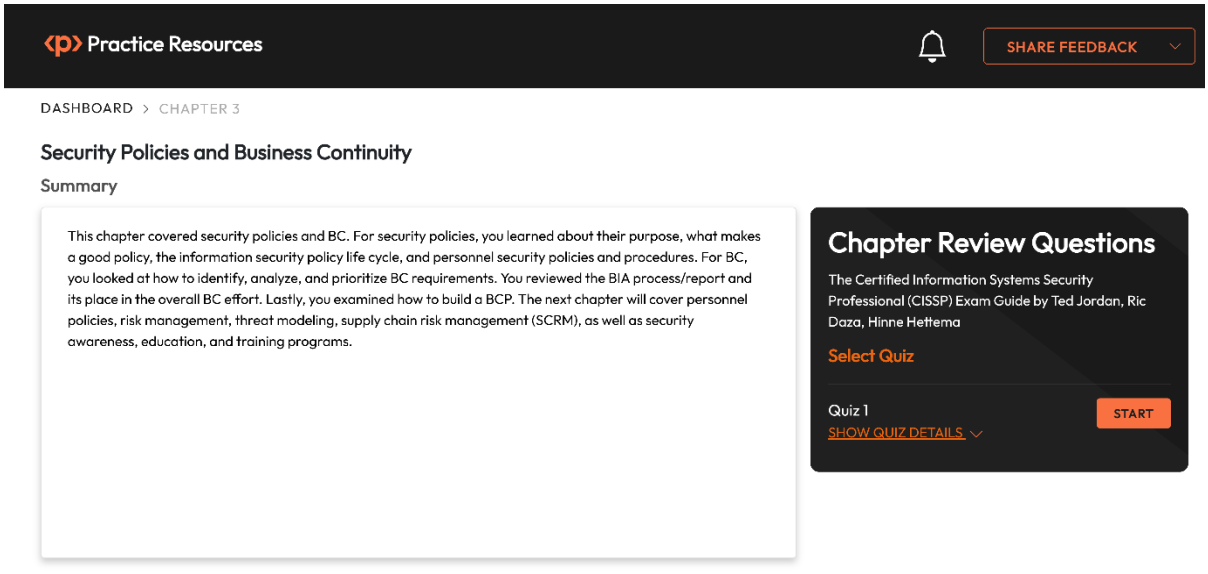




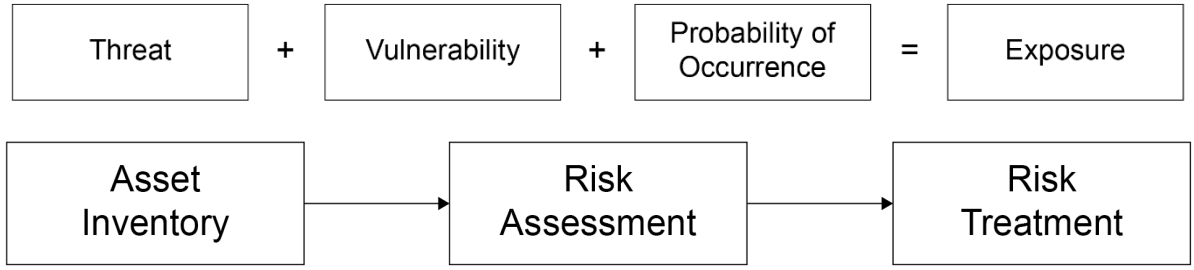
Chapter 3: *Security Policies and Business Continuity*

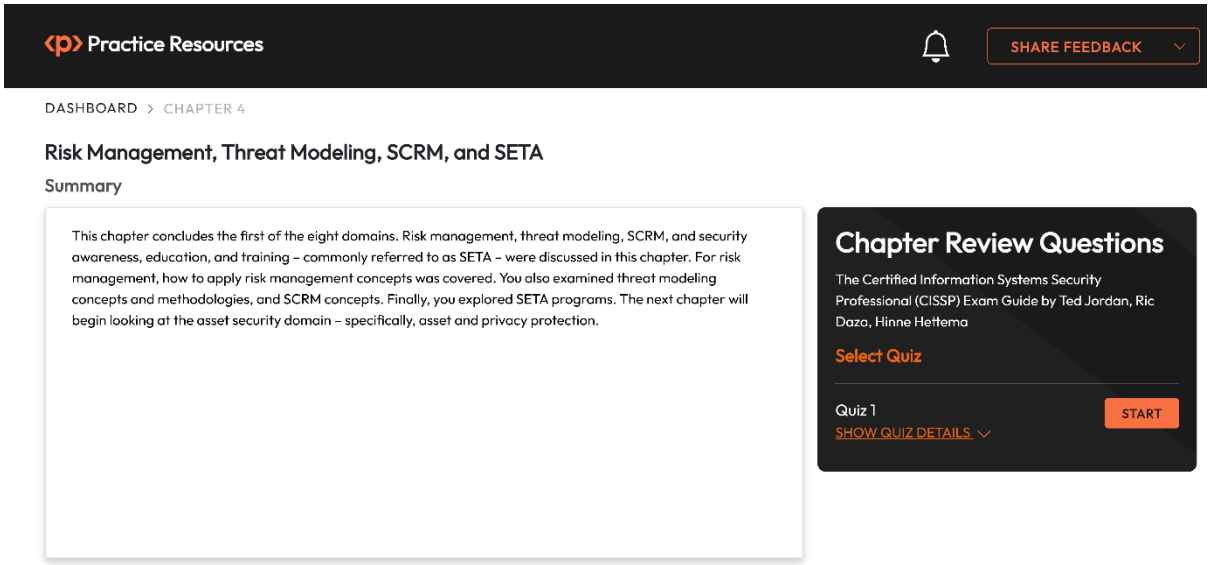




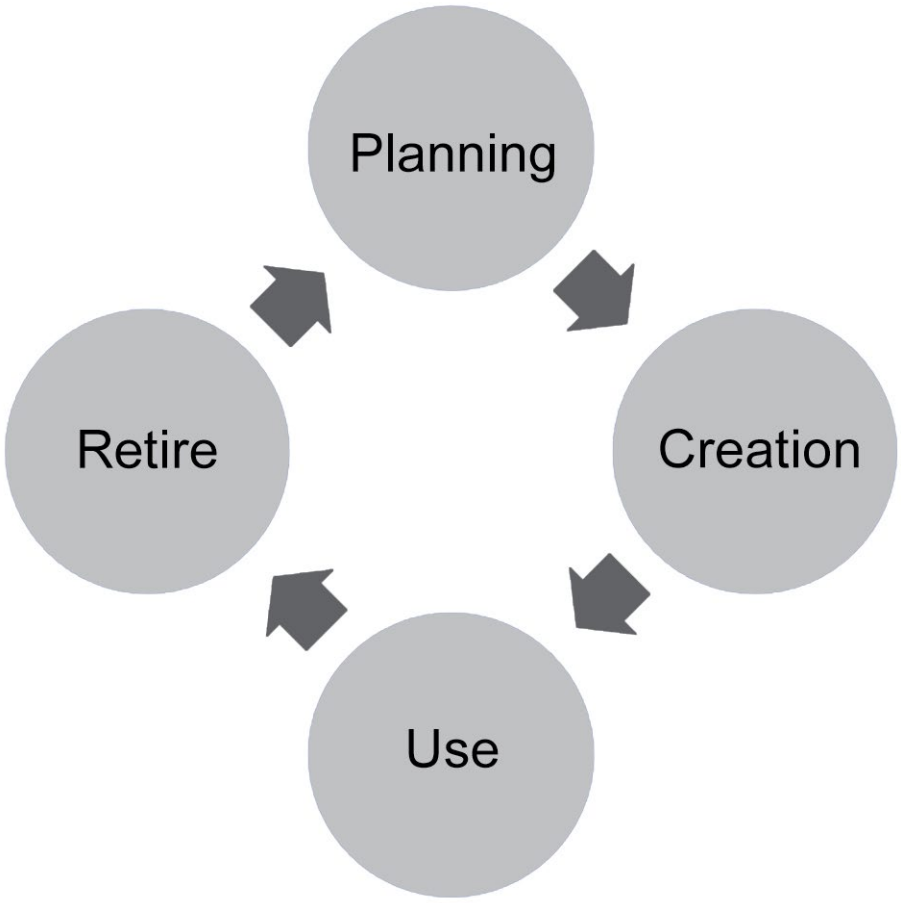


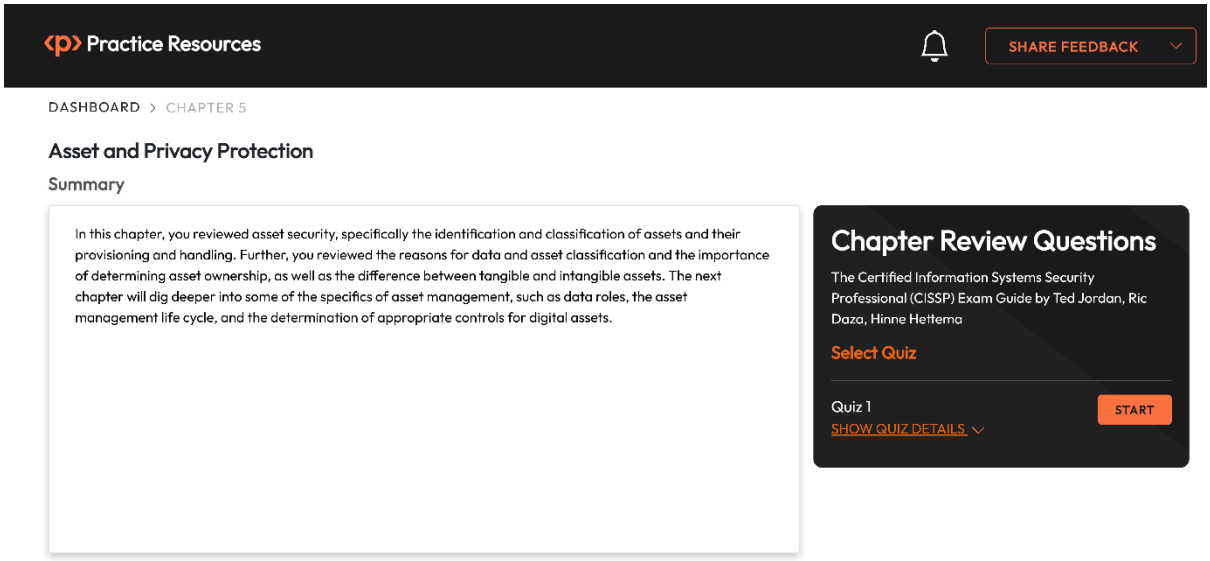
Chapter 4: ***Risk Management, Threat Modeling***



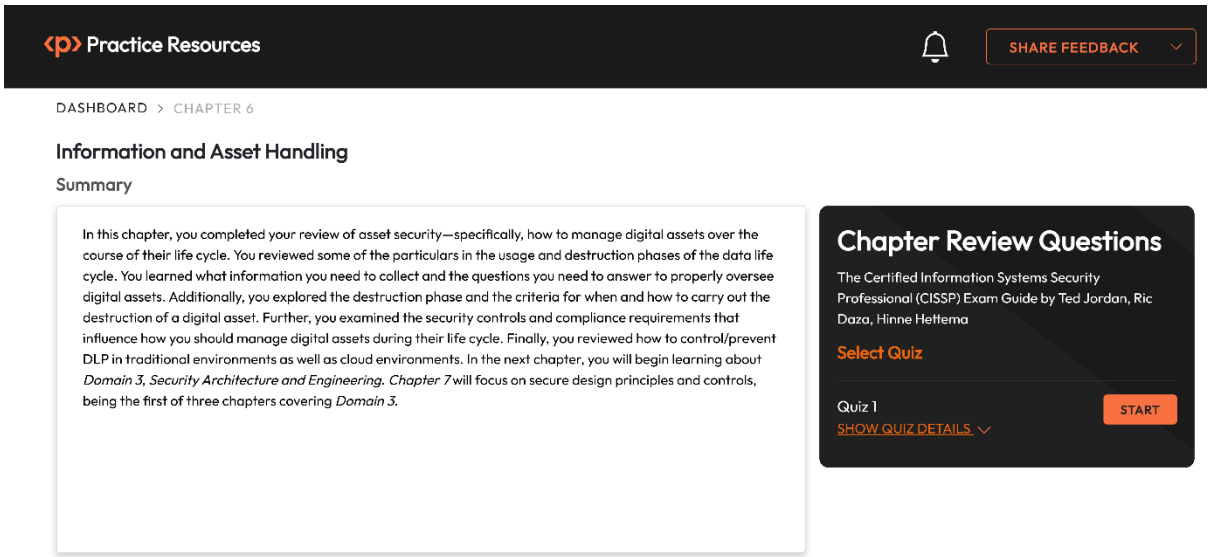


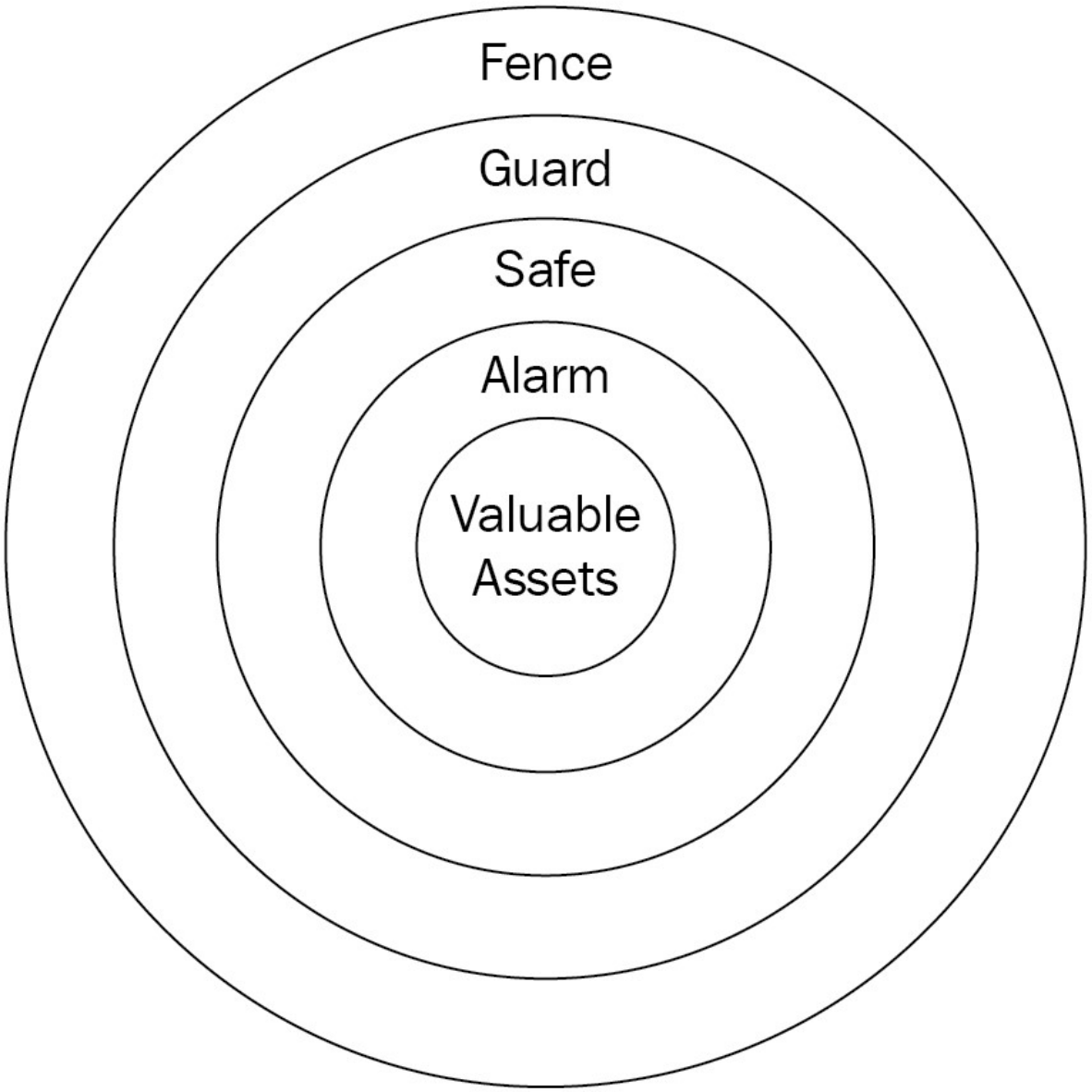
Chapter 5: ***Asset and Privacy Protection***

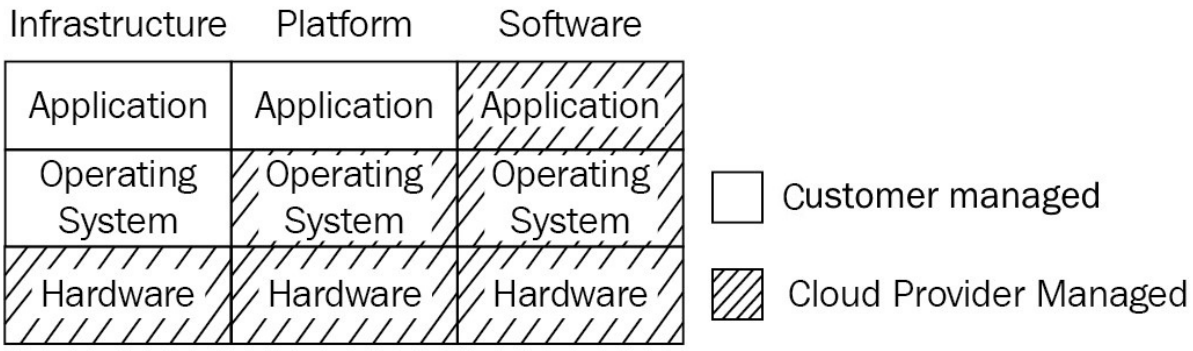


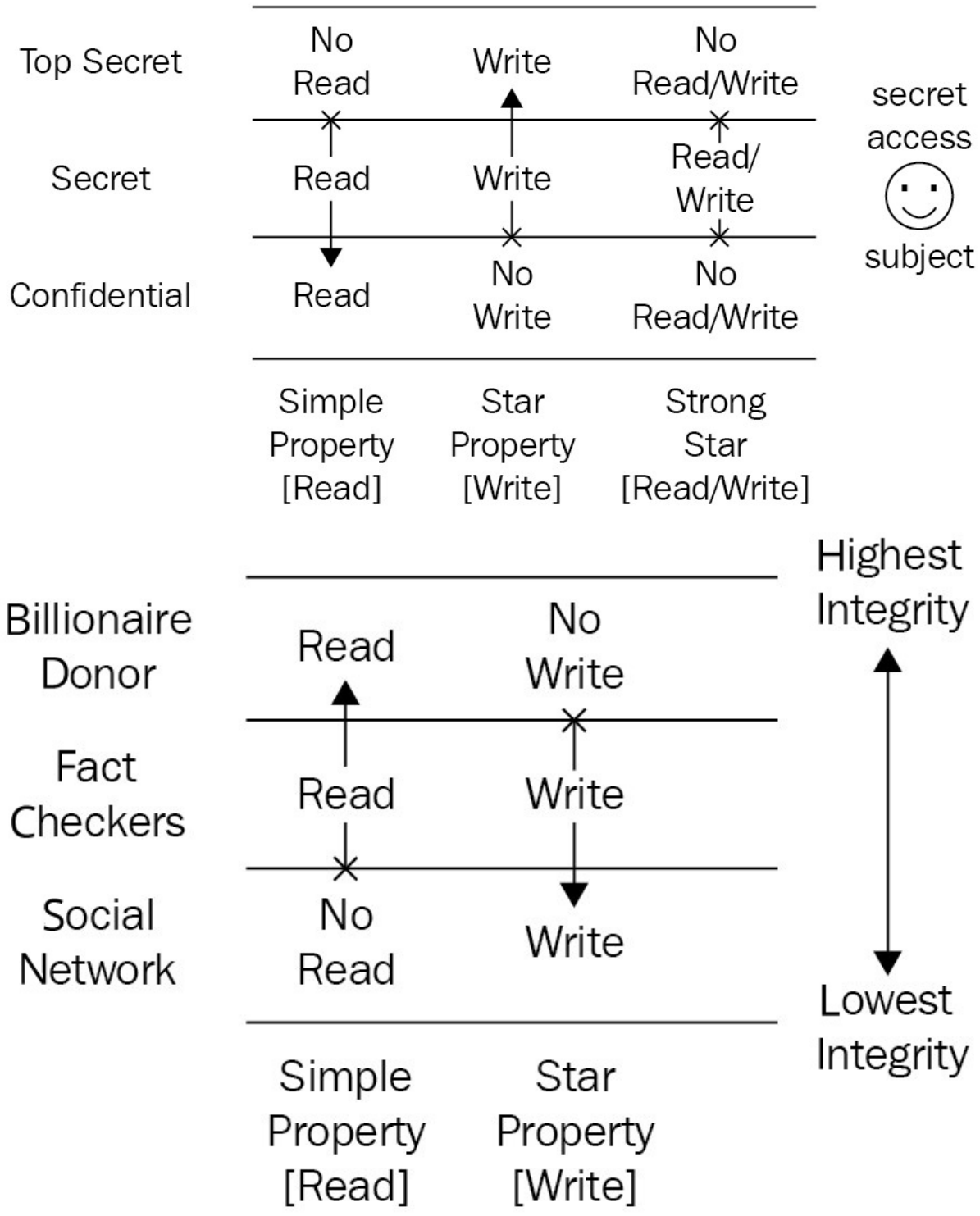


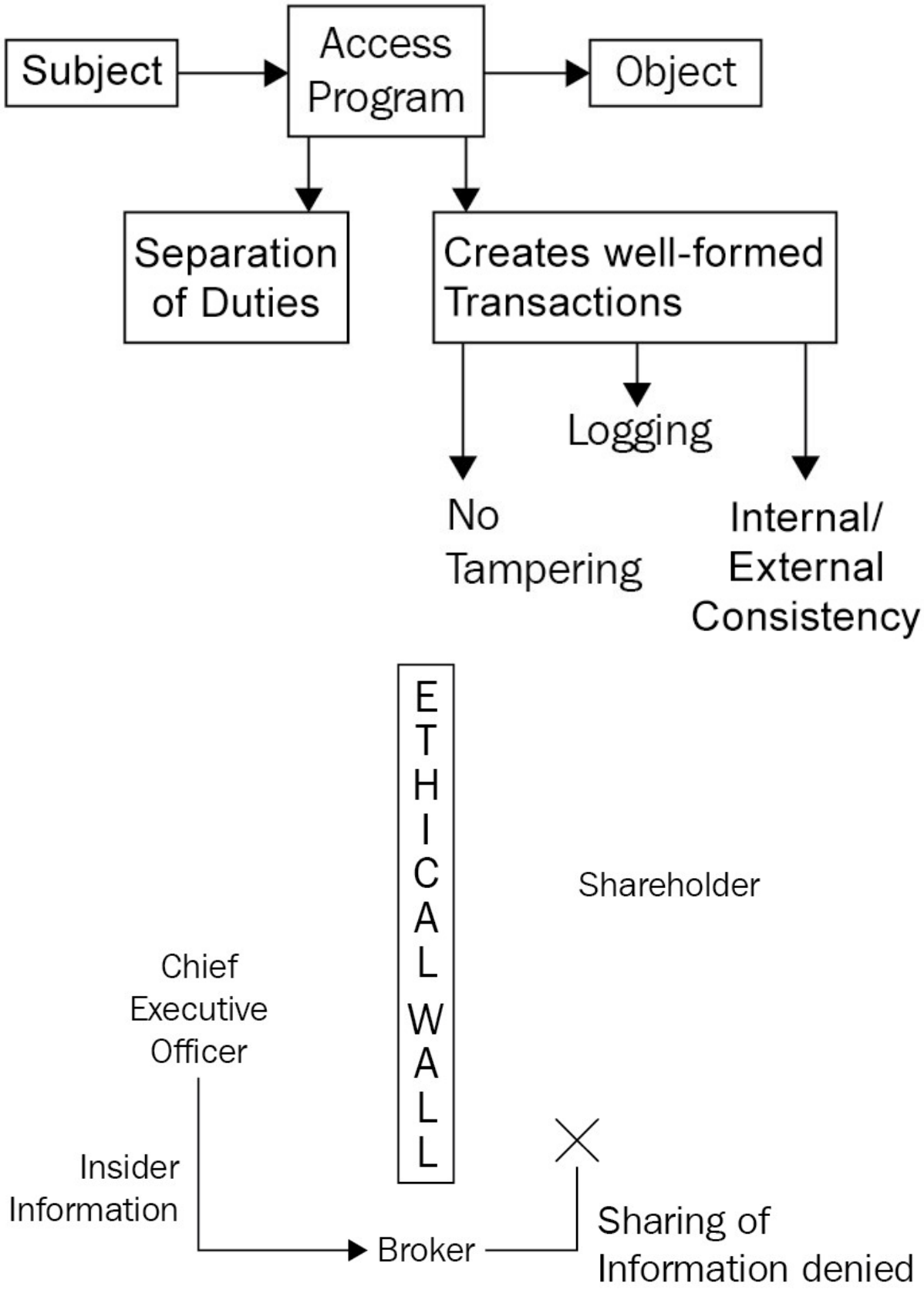
Chapter 6: *Information and Asset Handling*

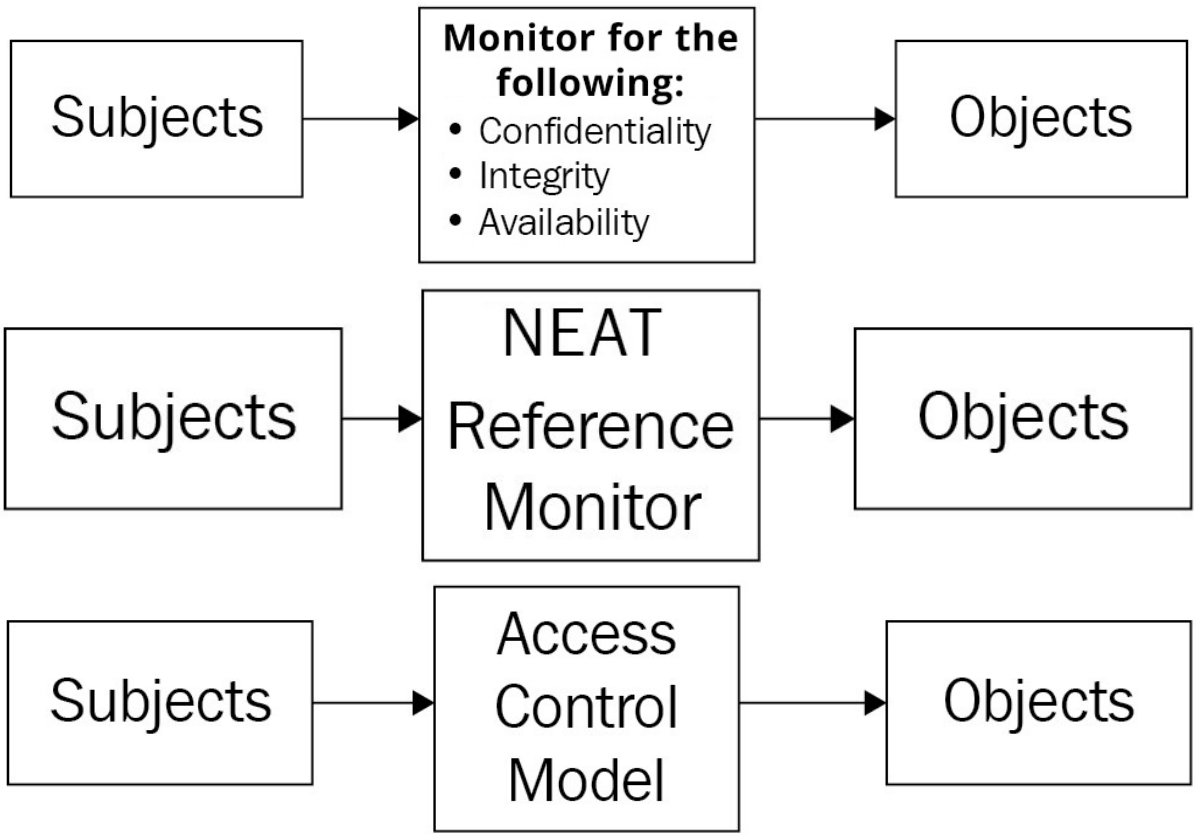


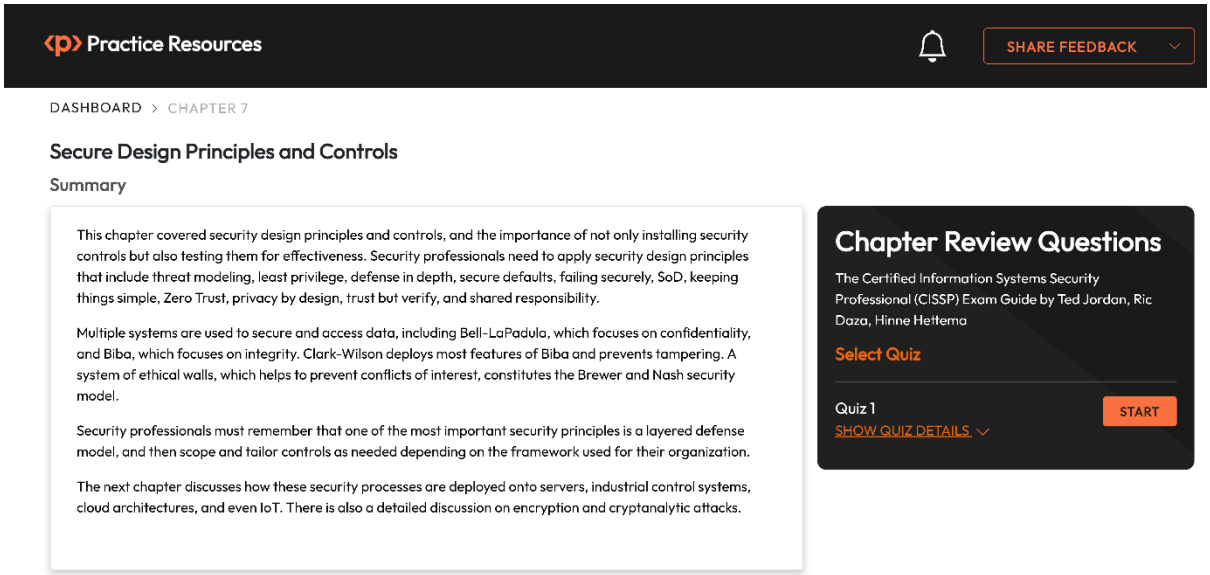

Fence
Guard
Safe
Alarm
Valuable Assets


Infrastructure
Platform
Software
Application
Application
Application
Operating System
Operating System
Operating System
Hardware
Hardware
Hardware
Customer managed
Cloud Provider Managed

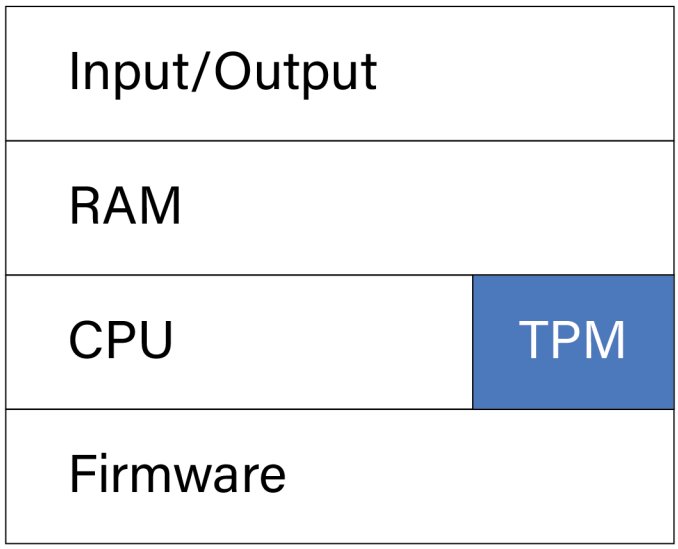

Top Secret
Secret
Confidential
No Read
Write
No Read/Write
Read
Write
Read/ Write
Read
No Write
No Read/Write
secret access
subject
Simple Property [Read]
Star Property [Write]
Strong Star [Read/Write]
Billionaire Donor
Fact Checkers
Social Network
Read
No Write
Read
Write
No Read
Write
Highest Integrity
Lowest Integrity
Simple Property [Read]
Star Property [Write]

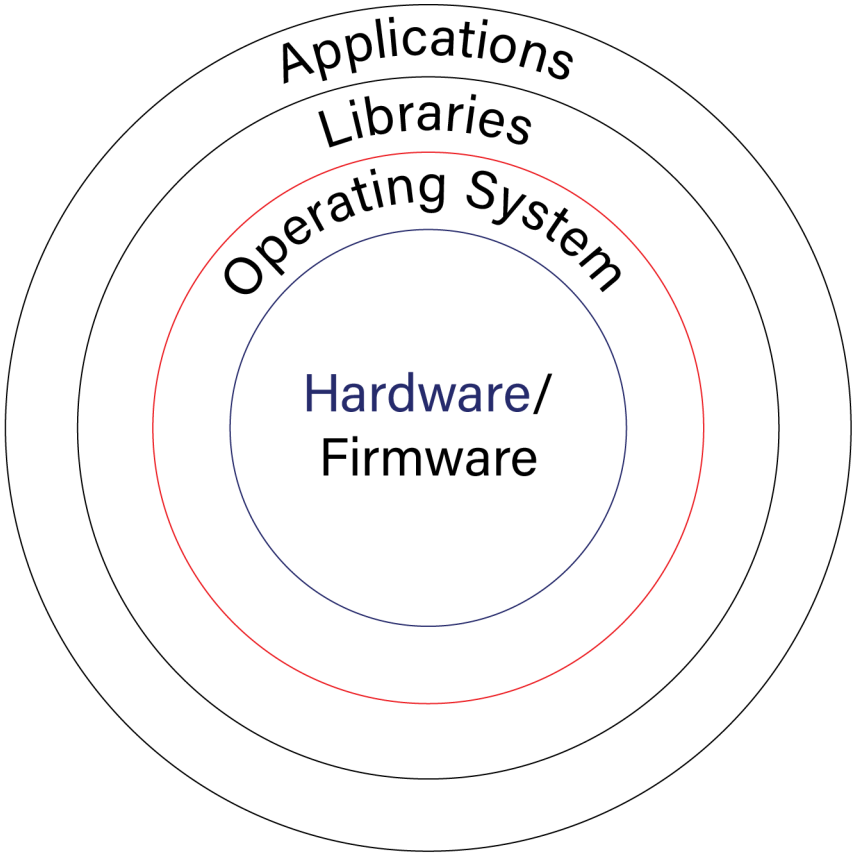

Subject
Access Program
Object
Separation of Duties
Creates well-formed Transactions
Logging
No Tampering
Internal/ External Consistency
ETHICAL WALL
Shareholder
Chief Executive Officer
Insider Information
Broker
Sharing of Information denied

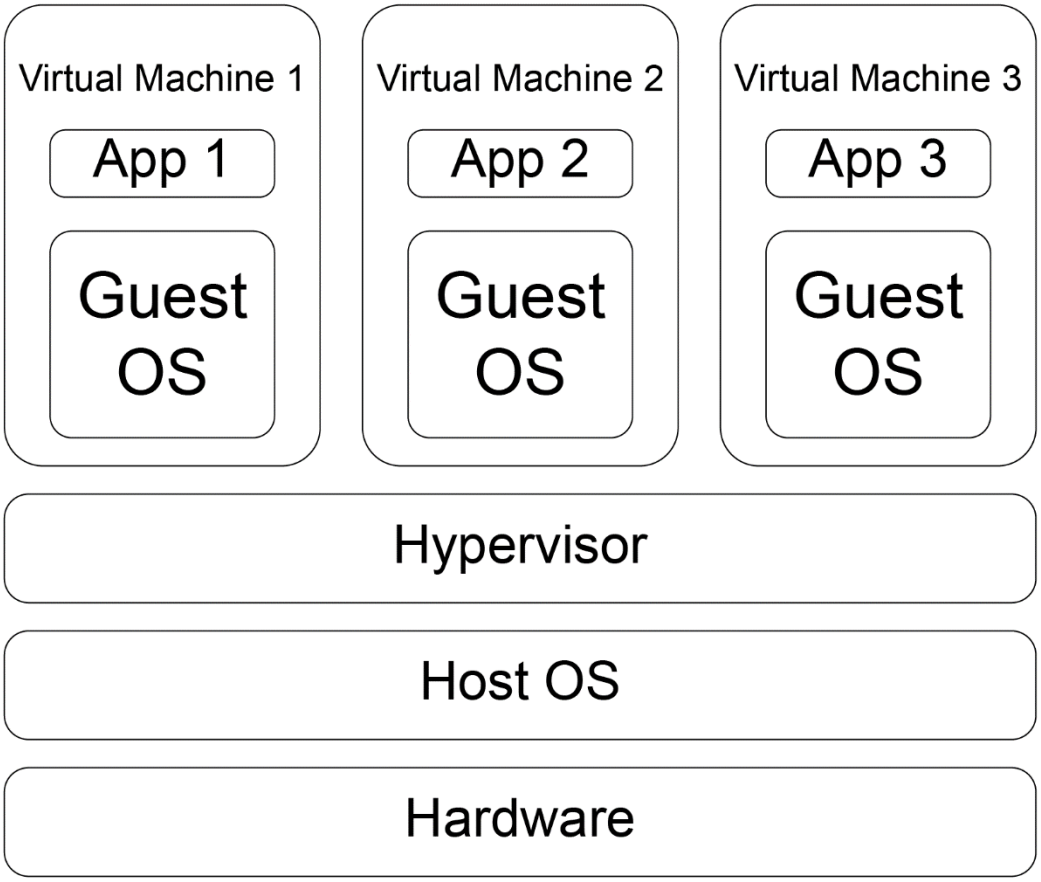

Subjects
Monitor for the following:
• Confidentiality
• Integrity
• Availability
Objects
Subjects
NEAT Reference Monitor
Objects
Subjects
Access Control Model
Objects


Practice Resources
SHARE FEEDBACK
DASHBOARD > CHAPTER 7
Secure Design Principles and Controls
Summary
This chapter covered security design principles and controls, and the importance of not only installing security controls but also testing them for effectiveness. Security professionals need to apply security design principles that include threat modeling, least privilege, defense in depth, secure defaults, failing securely, SoD, keeping things simple, Zero Trust, privacy by design, trust but verify, and shared responsibility.
Multiple systems are used to secure and access data, including Bell-LaPadula, which focuses on confidentiality, and Biba, which focuses on integrity. Clark-Wilson deploys most features of Biba and prevents tampering. A system of ethical walls, which helps to prevent conflicts of interest, constitutes the Brewer and Nash security model.
Security professionals must remember that one of the most important security principles is a layered defense model, and then scope and tailor controls as needed depending on the framework used for their organization.
The next chapter discusses how these security processes are deployed onto servers, industrial control systems, cloud architectures, and even IoT. There is also a detailed discussion on encryption and cryptanalytic attacks.
Chapter Review Questions
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema
Select Quiz
Quiz 1
SHOW QUIZ DETAILS
START

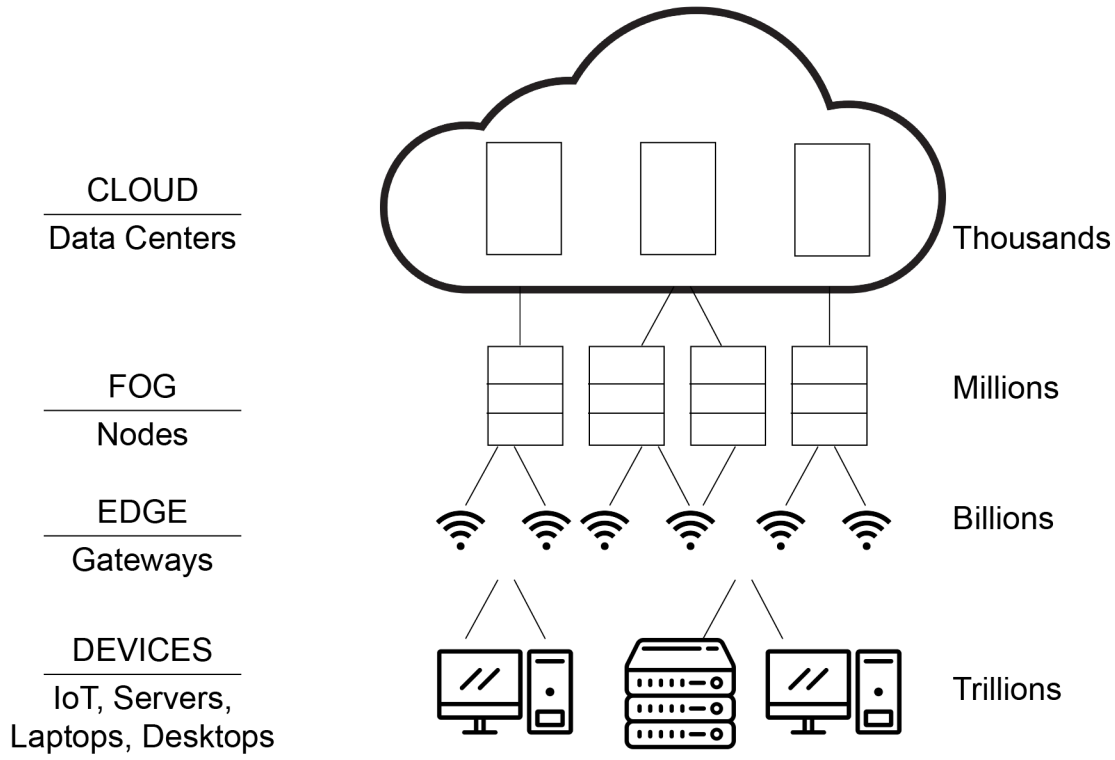
Chapter 8: ***Architecture Vulnerabilities and Cryptography***

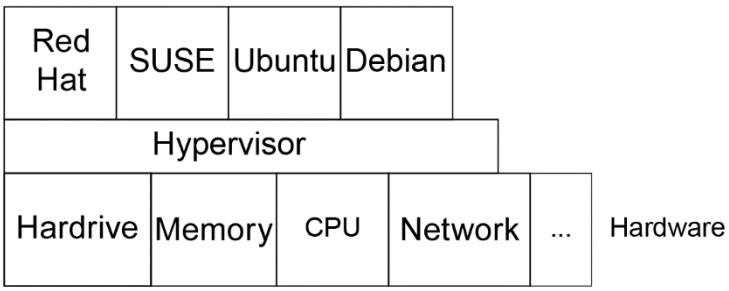

Input/Output
RAM
CPU
TPM
Firmware

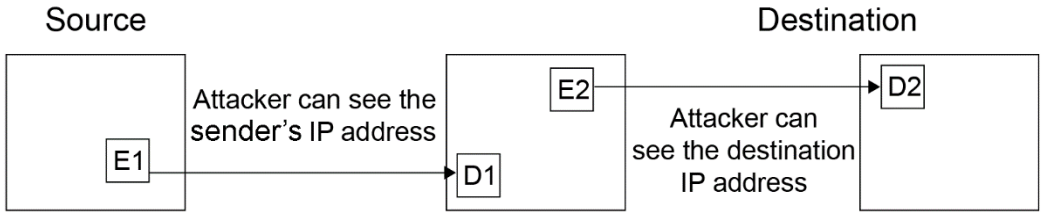

Applications
Libraries
Operating System
Hardware/
Firmware

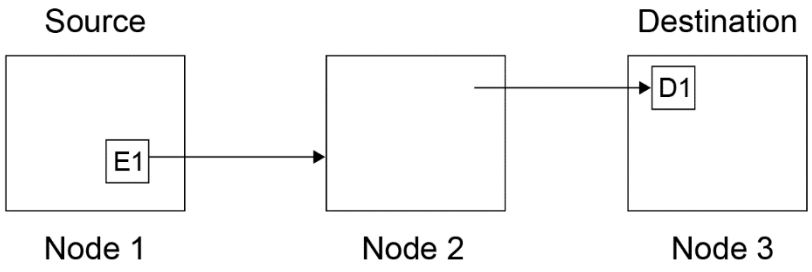


strong password, 2FA	SaaS	hardware, operating system, application
application, strong password, 2FA	PaaS	hardware, operating system
operating system, application, strong password, 2FA	IaaS	hardware









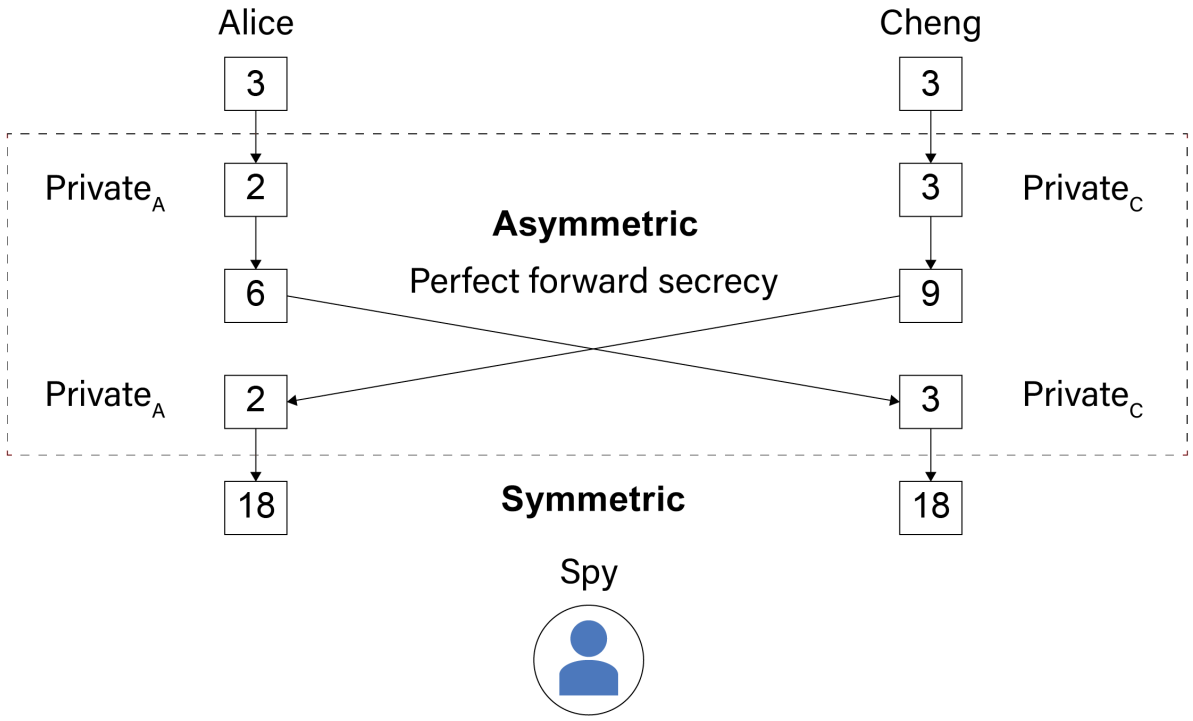
Attacker can see the sender and receiver's IP address

Original image

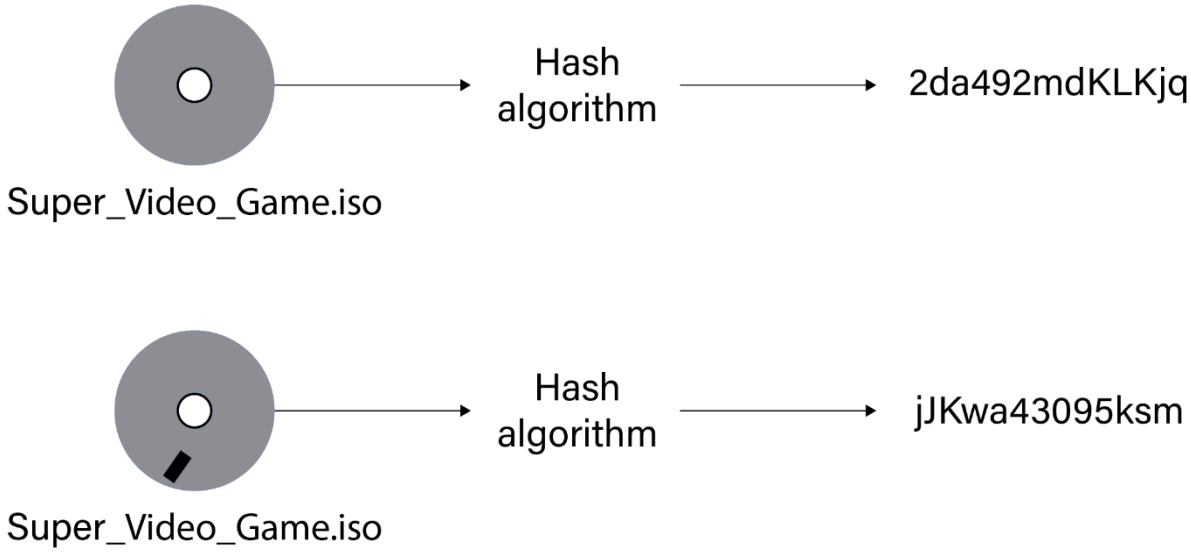
Original image plus hidden data

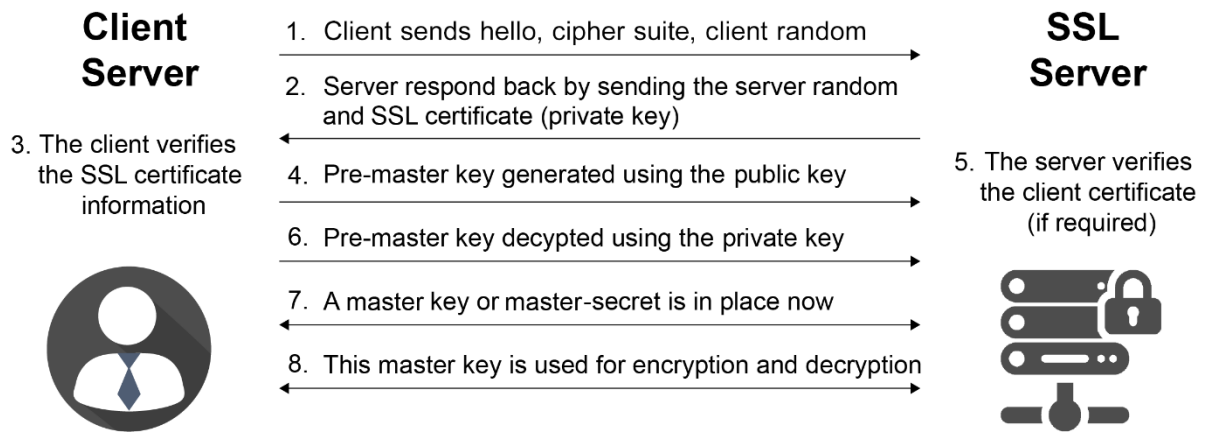
	Sender has	**Recipient has**
Signing	Sender private key	Sender public key
Encrypting	Recipient public key	Recipient private key

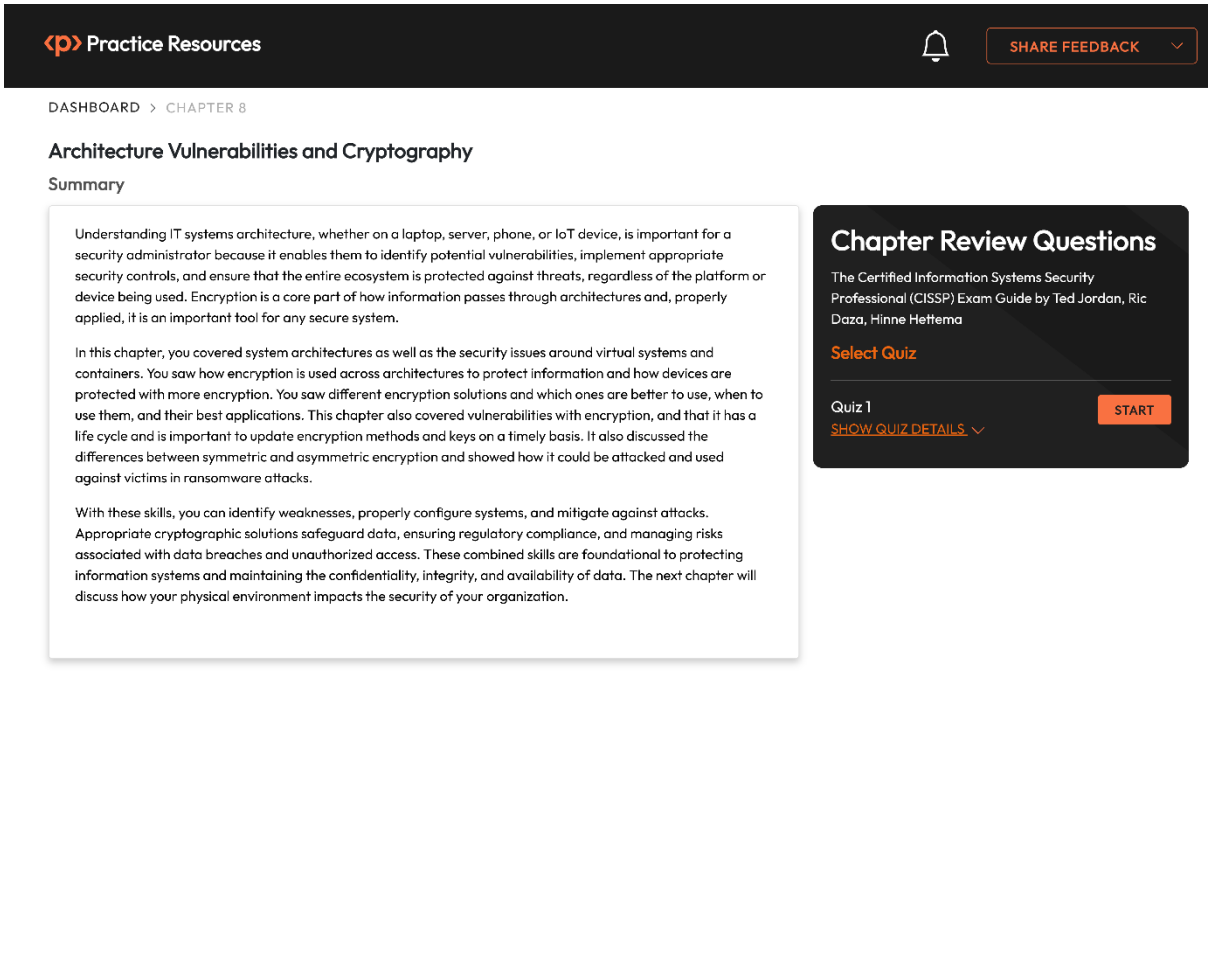
Diffie - Hellman



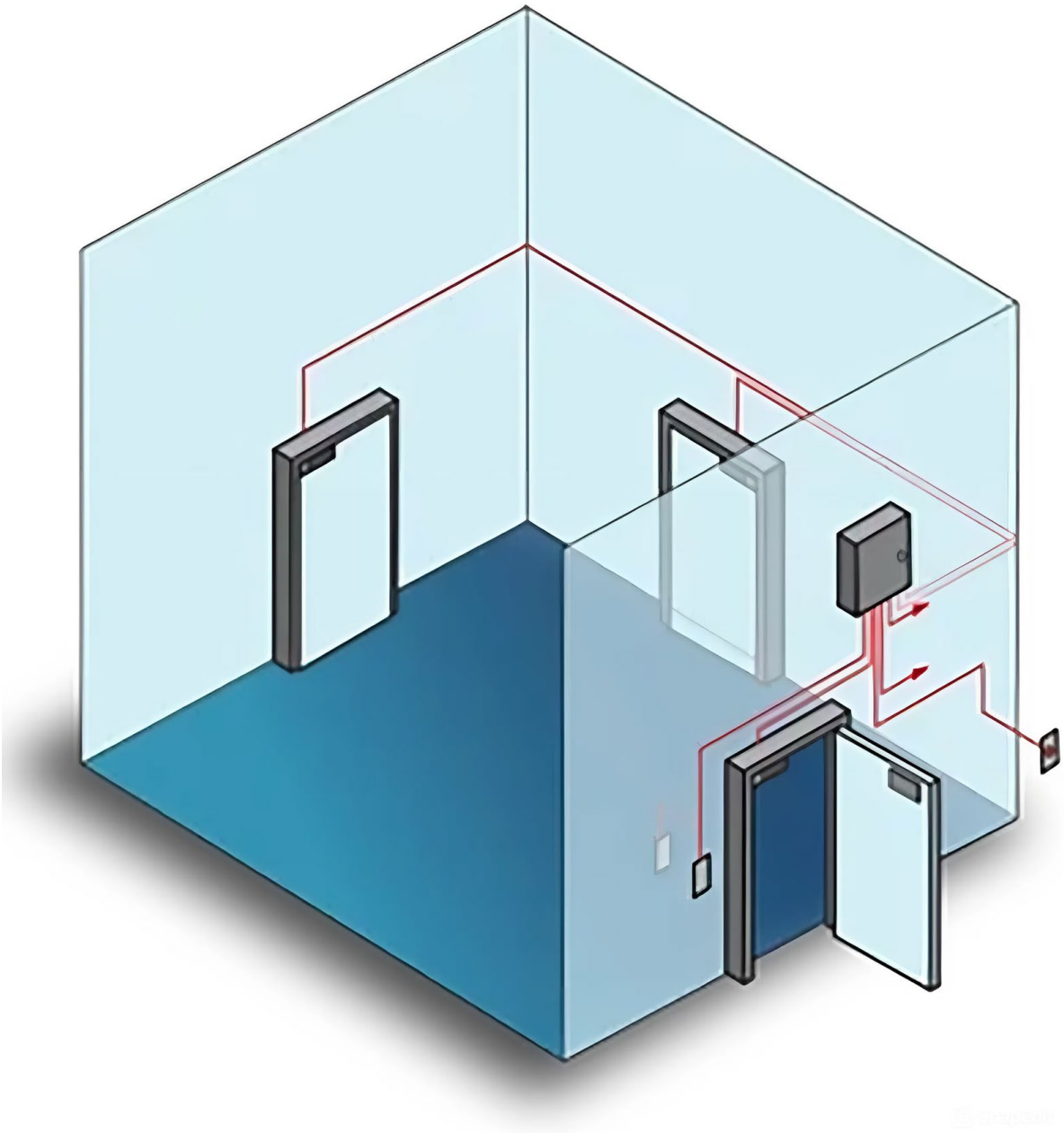
s

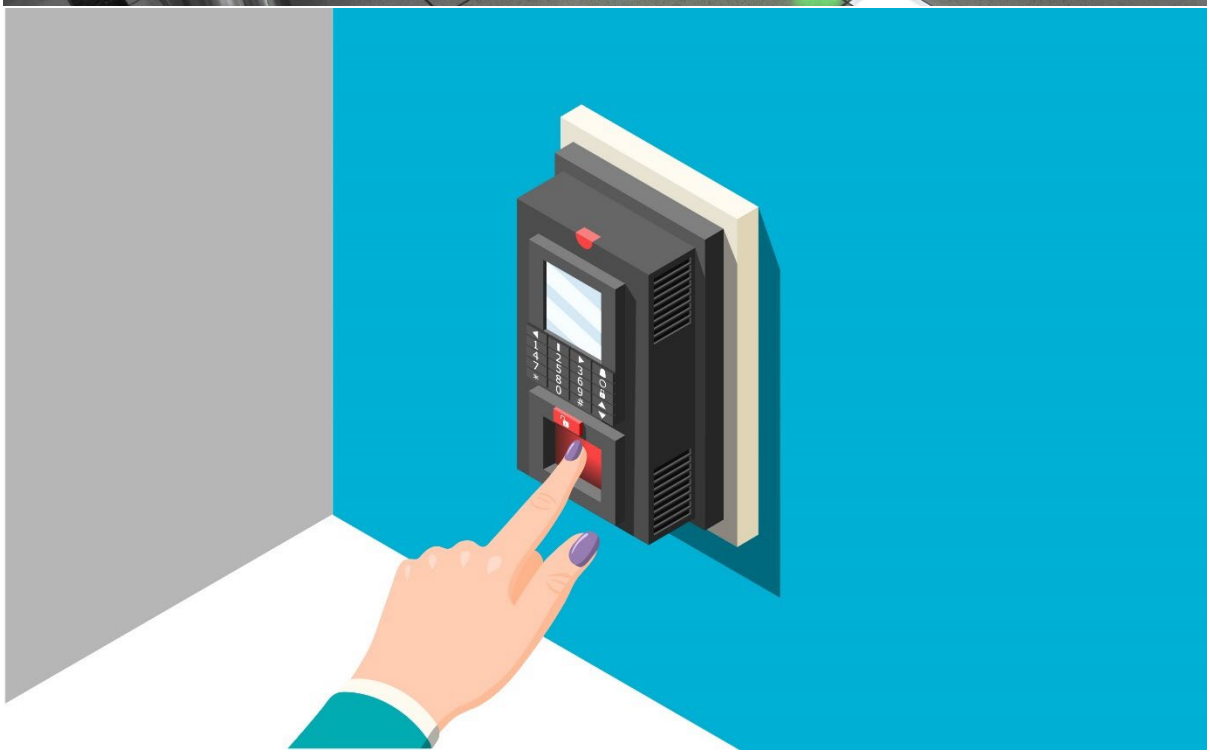



Client
Server
SSL
Server
1. Client sends hello, cipher suite, client random
2. Server respond back by sending the server random and SSL certificate (private key)
3. The client verifies the SSL certificate information
4. Pre-master key generated using the public key
5. The server verifies the client certificate (if required)
6. Pre-master key decypted using the private key
7. A master key or master-secret is in place now
8. This master key is used for encryption and decryption


Practice Resources
SHARE FEEDBACK
DASHBOARD > CHAPTER 8
Architecture Vulnerabilities and Cryptography
Summary
Understanding IT systems architecture, whether on a laptop, server, phone, or IoT device, is important for a security administrator because it enables them to identify potential vulnerabilities, implement appropriate security controls, and ensure that the entire ecosystem is protected against threats, regardless of the platform or device being used. Encryption is a core part of how information passes through architectures and, properly applied, it is an important tool for any secure system.
In this chapter, you covered system architectures as well as the security issues around virtual systems and containers. You saw how encryption is used across architectures to protect information and how devices are protected with more encryption. You saw different encryption solutions and which ones are better to use, when to use them, and their best applications. This chapter also covered vulnerabilities with encryption, and that it has a life cycle and is important to update encryption methods and keys on a timely basis. It also discussed the differences between symmetric and asymmetric encryption and showed how it could be attacked and used against victims in ransomware attacks.
With these skills, you can identify weaknesses, properly configure systems, and mitigate against attacks. Appropriate cryptographic solutions safeguard data, ensuring regulatory compliance, and managing risks associated with data breaches and unauthorized access. These combined skills are foundational to protecting information systems and maintaining the confidentiality, integrity, and availability of data. The next chapter will discuss how your physical environment impacts the security of your organization.
Chapter Review Questions
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema
Select Quiz
Quiz 1
SHOW QUIZ DETAILS
START

Chapter 9: ***Facilities and Physical Security***





Facilities and Physical Security

Summary

Without robust physical security, even the most advanced cybersecurity strategies can be undermined. Securing data not only requires technical and management solutions but also physical solutions that keep an attacker from walking into a building and carrying out attacks on physical infrastructure. This chapter highlighted the importance of securing both external and internal boundaries, using strategies such as perimeter fencing, surveillance systems, and controlled access points to prevent unauthorized access and protect against natural disasters.

We started the discussion with parking lot security, covering fencing, lighting, and cameras. Attackers seek vulnerabilities and notice when a facility is uncared for. Using principles of crime prevention through environmental design reduces the likelihood of attack because the facility appears to be tended to.

Then, the chapter discussed how to ensure building security with security guards and by logging who is entering and exiting the building and when. Alarm systems can alert security guards of intruders and security cameras can capture these events in action.

You covered secure storage, including knowing whether it's data on tapes or hard drives and whether it's evidence. Evidence storage requires stricter controls, including tamper-evident bags. Finally, you learned about maintaining the server room and ensuring clean electrical power. Hot and cold aisles help maintain a consistent environment in the server room, and redundant power controls and generators can provide electricity for some time if the power plant goes down.

For security professionals, these concepts are vital because they play a part in ensuring comprehensive protection for an organization's assets and help manage risks that could lead to significant data breaches or operational disruptions. In the next chapter, you will look at various networking technologies and how to secure them.

Chapter Review Questions

The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

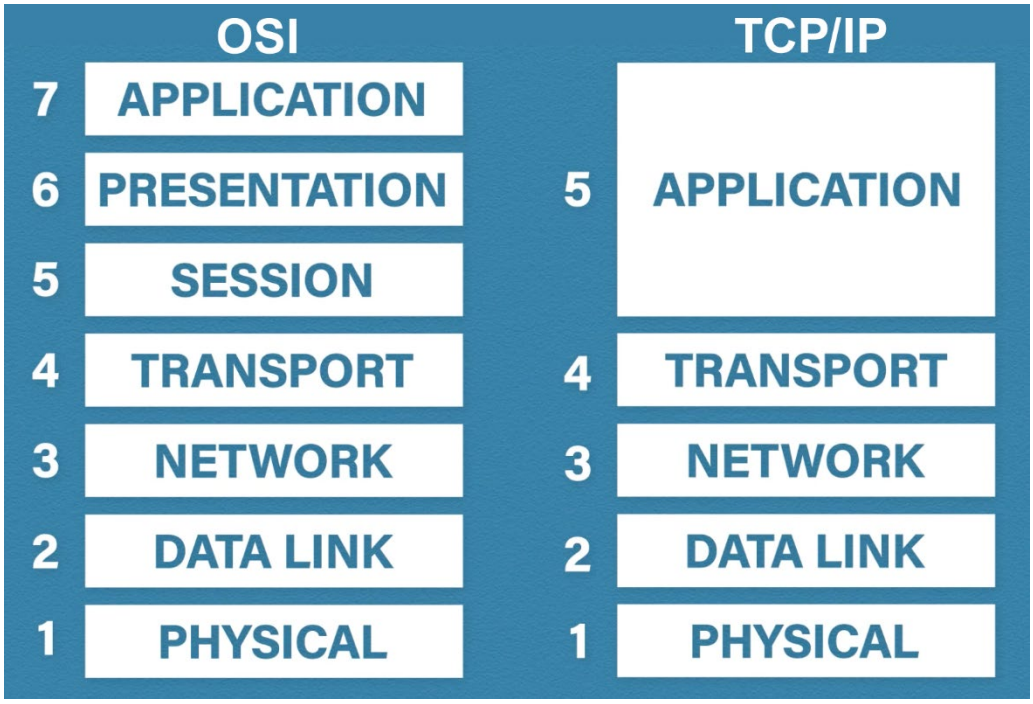
Select Quiz

Quiz 1

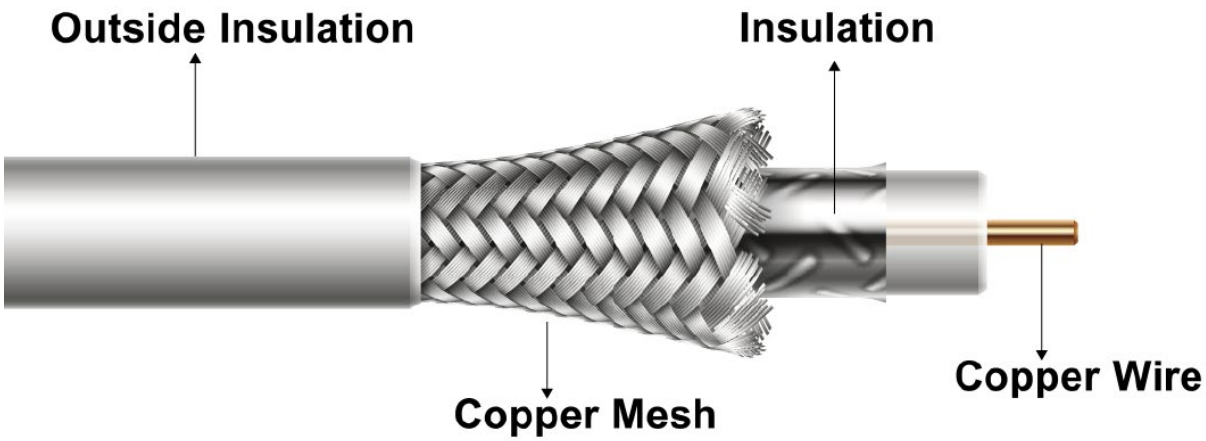
SHOW QUIZ DETAILS

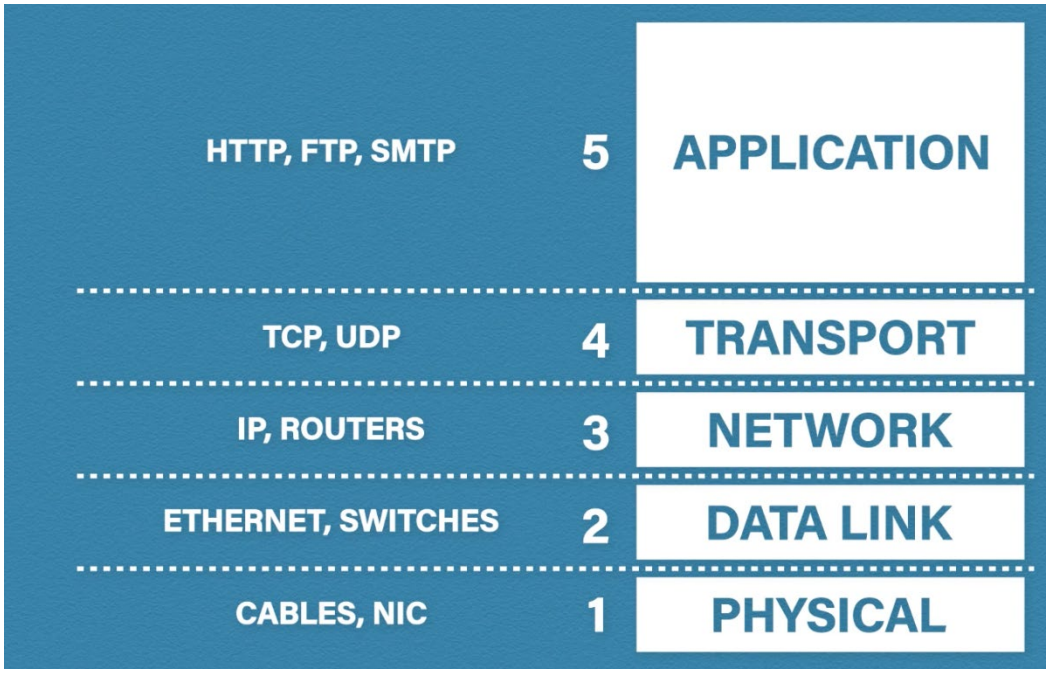
START

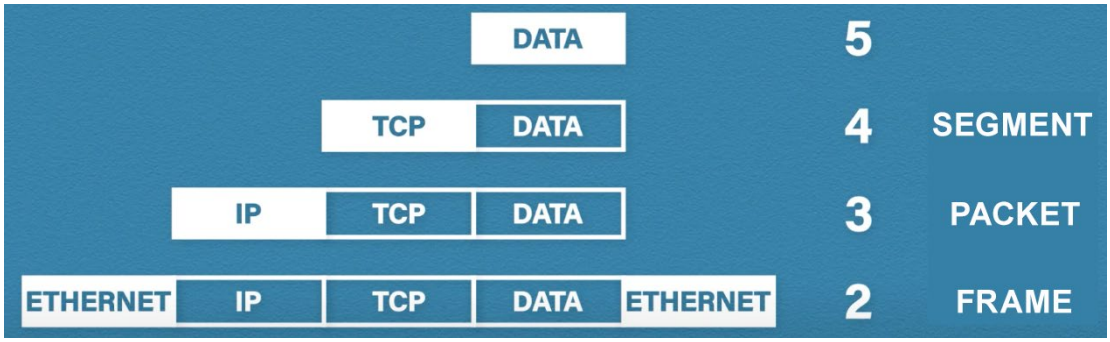
Chapter 10: ***Network Architecture Security***

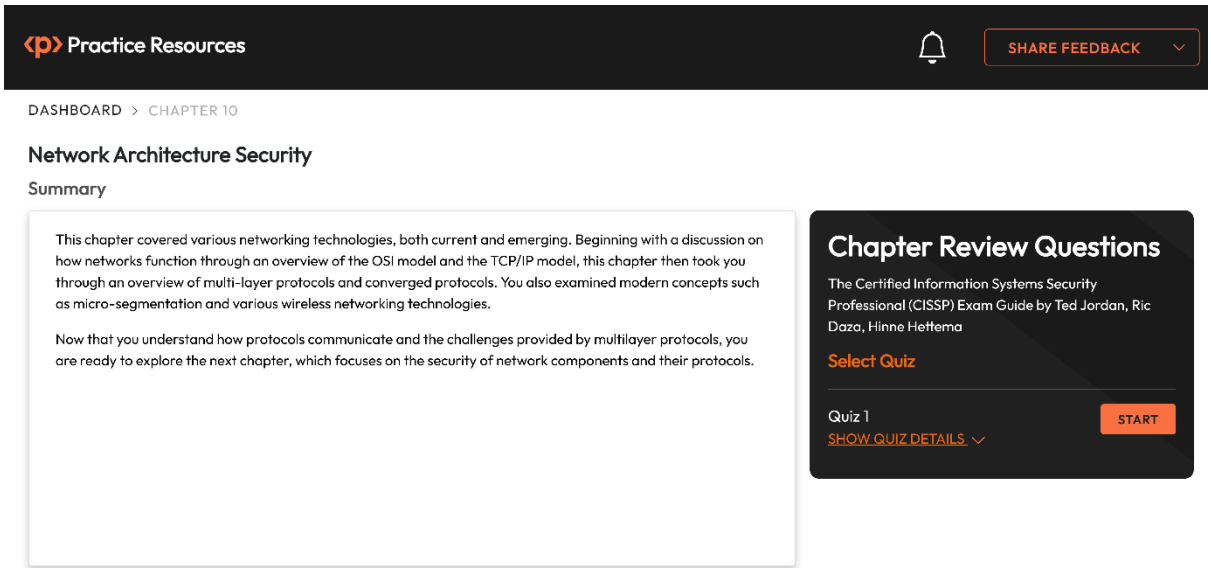


Coaxial cable

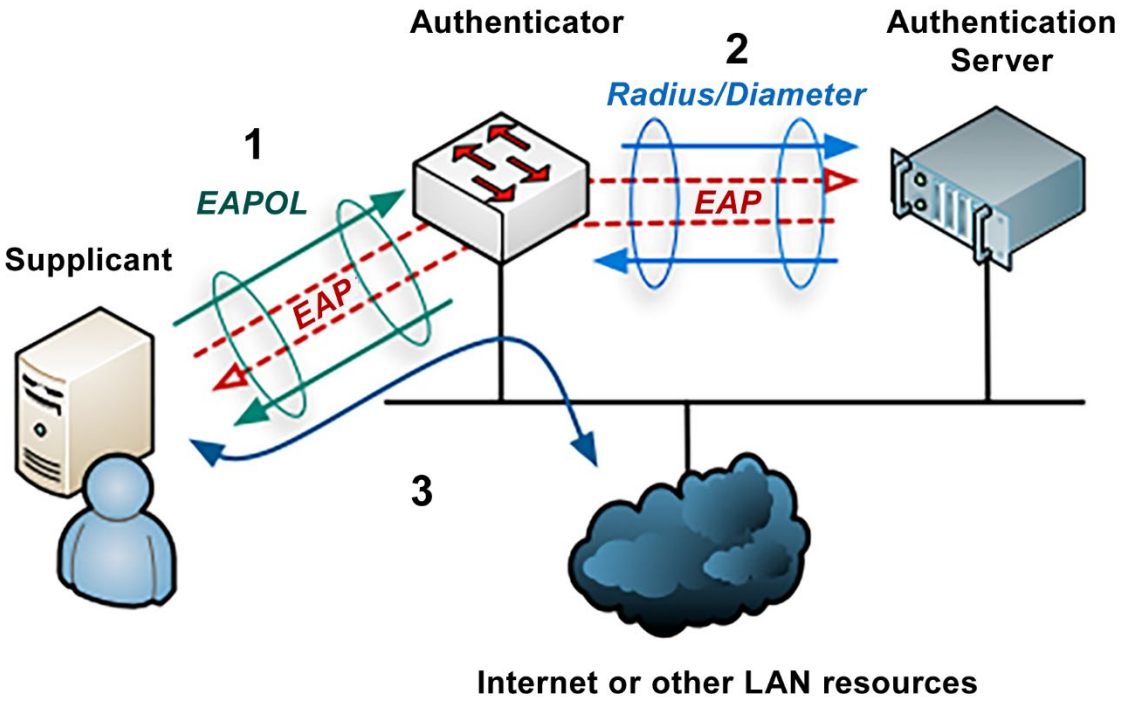



HTTP, FTP, SMTP
5
APPLICATION
TCP, UDP
4
TRANSPORT
IP, ROUTERS
3
NETWORK
ETHERNET, SWITCHES
2
DATA LINK
CABLES, NIC
1
PHYSICAL


DATA
5
TCP
DATA
4
SEGMENT
IP
TCP
DATA
3
PACKET
ETHERNET
IP
TCP
DATA
ETHERNET
2
FRAME


Practice Resources
SHARE FEEDBACK
DASHBOARD > CHAPTER 10
Network Architecture Security
Summary
This chapter covered various networking technologies, both current and emerging. Beginning with a discussion on how networks function through an overview of the OSI model and the TCP/IP model, this chapter then took you through an overview of multi-layer protocols and converged protocols. You also examined modern concepts such as micro-segmentation and various wireless networking technologies.
Now that you understand how protocols communicate and the challenges provided by multilayer protocols, you are ready to explore the next chapter, which focuses on the security of network components and their protocols.
Chapter Review Questions
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema
Select Quiz
Quiz 1
SHOW QUIZ DETAILS
START

Chapter 11: *Securing Communication Channels*



Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 11

Securing Communication Channels

Summary

This chapter reinforced the core security concepts of confidentiality, integrity, availability, authenticity, and non-repudiation and how they come into play when securing communications channels. It emphasized the importance of securing various network elements, focusing on HA and fault tolerance, NAC, and endpoint security. You looked at the difference between HA and fault tolerance, and how they both aim to ensure network availability but differ in cost and implementation. Fault tolerance offers zero service interruption using redundant hardware, while HA uses a holistic approach combining hardware and software to restore services quickly after a failure, making it more cost-effective. The chapter also highlighted that power redundancy, warranties, and support are crucial in maintaining robust network architecture, with components such as UPSs providing backup during power outages.

You also looked at network security components, including transmission media, NAC devices, and endpoint security. NAC was presented as a critical tool in controlling the security posture of devices joining a network, employing methods such as IEEE 802.1X standards, authenticators, and authentication servers to enforce access control. Endpoint security, a vital aspect of network defense, has also evolved beyond basic antivirus solutions to include comprehensive systems such as EPPs and XDR.

Lastly, the chapter explored secure communication channels, particularly for voice, multimedia collaboration, and remote access. It highlighted the security challenges associated with VoIP systems, such as eavesdropping and DoS attacks, and suggested encryption and network segmentation as countermeasures. Multimedia collaboration tools such as Zoom and Microsoft Teams require vigilance to prevent unauthorized access, while remote access technologies such as VPNs and desktop virtualization ensure secure connectivity over the internet.

In the next chapter, you will look at how to secure agents in your system by looking at identity, access management, and federation.

Chapter Review Questions

The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

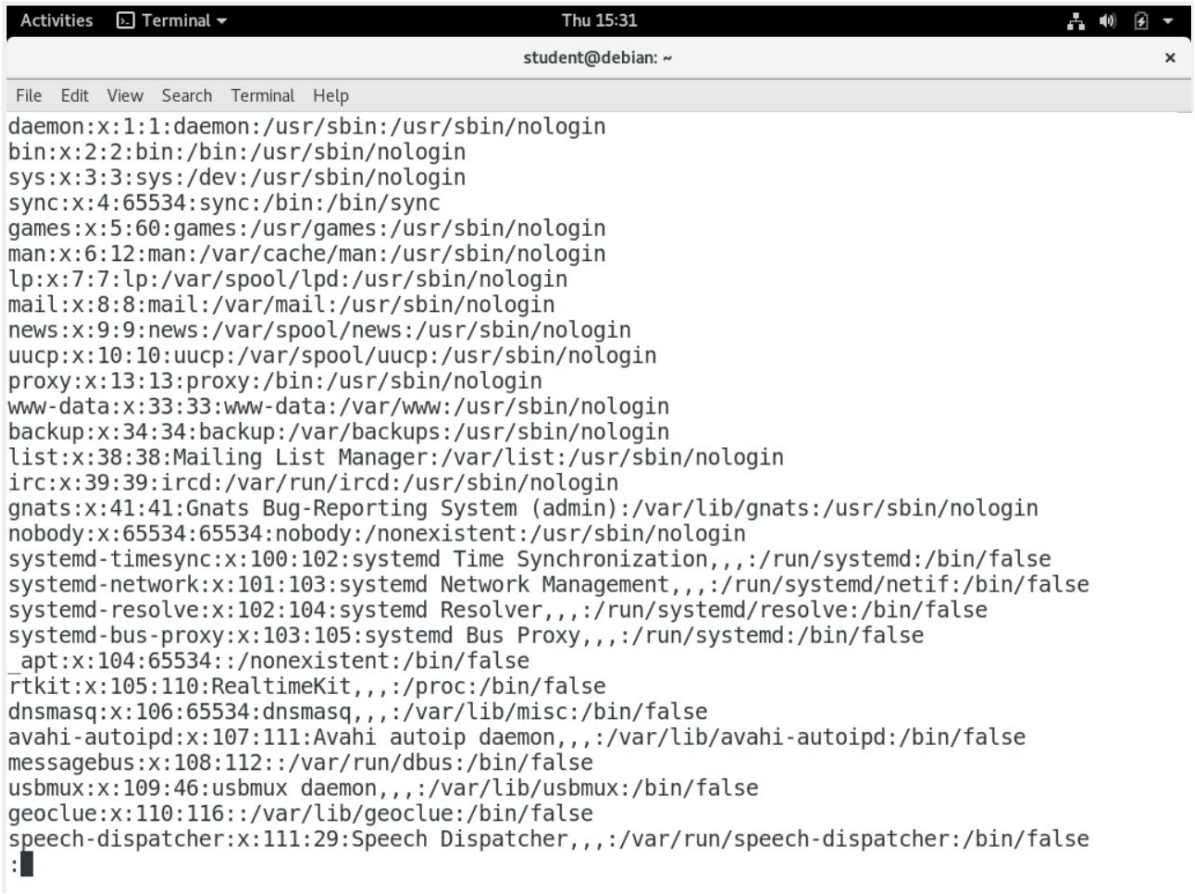
Select Quiz

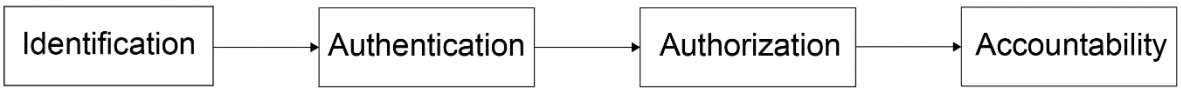
Quiz 1

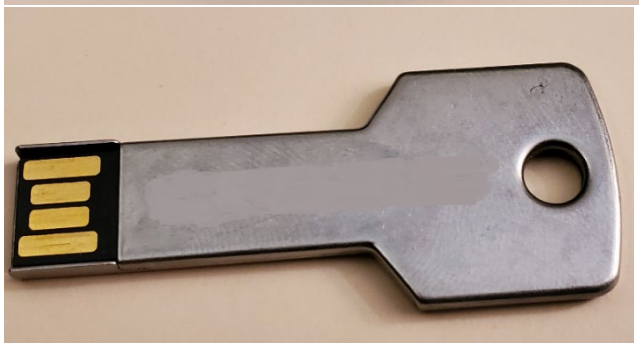
SHOW QUIZ DETAILS

START

Chapter 12: ***Identity, Access Management, and Federation***







Identity, Access Management, and Federation

Summary

This chapter covered user access controls and management and reviewed some measures you can take to protect your organization from attackers using either physical or technical controls to breach the firm. A major role of the CSO and CISSP is to secure identity access with centralized utilities such as single sign-on so that users can do their jobs. Users enhance security by using strong passwords.

Next, you learned the differences between logical and physical controls and the security frameworks that organizations need to use, whether it be NIST, ISO, or another, to ensure they understand the risks of granting user access. Several devices can be used to identify a user for access to an organization's systems. When setting up new users, make sure they are provisioned properly and given only superuser or administrator access if required. Otherwise, they should only be given the privileges to do their job. This is called least privilege. Also, make sure that when an employee or contractor leaves a company, their access to the organization is removed through the deprovisioning process.

Identity can be managed with multiple methods. These include *something-you-know*, *something-you-have*, or *something-you-are* authentication factors. Identity security is enhanced by combining these methods as either two-factor or multi-factor authentication. Although two users might have the same level of security or access, such as Top Secret, that does not automatically give them top-secret access to every project. This is known as *need-to-know* access. As users move through different positions in their organization, system administrators must protect the organization by removing past privileges and granting the required rights to do their jobs; otherwise, users will have more rights than needed. This is known as authorization creep.

The chapter ended with a discussion on the credential life cycle, which is the process of provisioning, securing, and deprovisioning users that helps administrators establish that users are authorized properly, and ensures their credentials are being used appropriately within LAN and cloud systems. The next chapter takes you through identity management implementation.

Chapter Review Questions

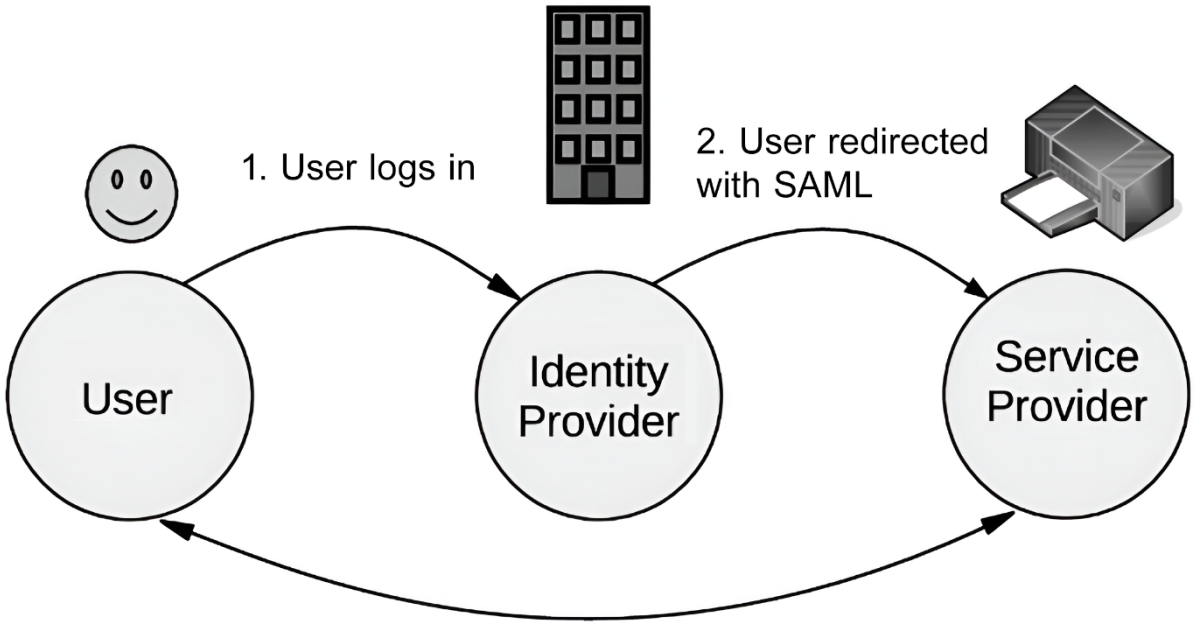
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

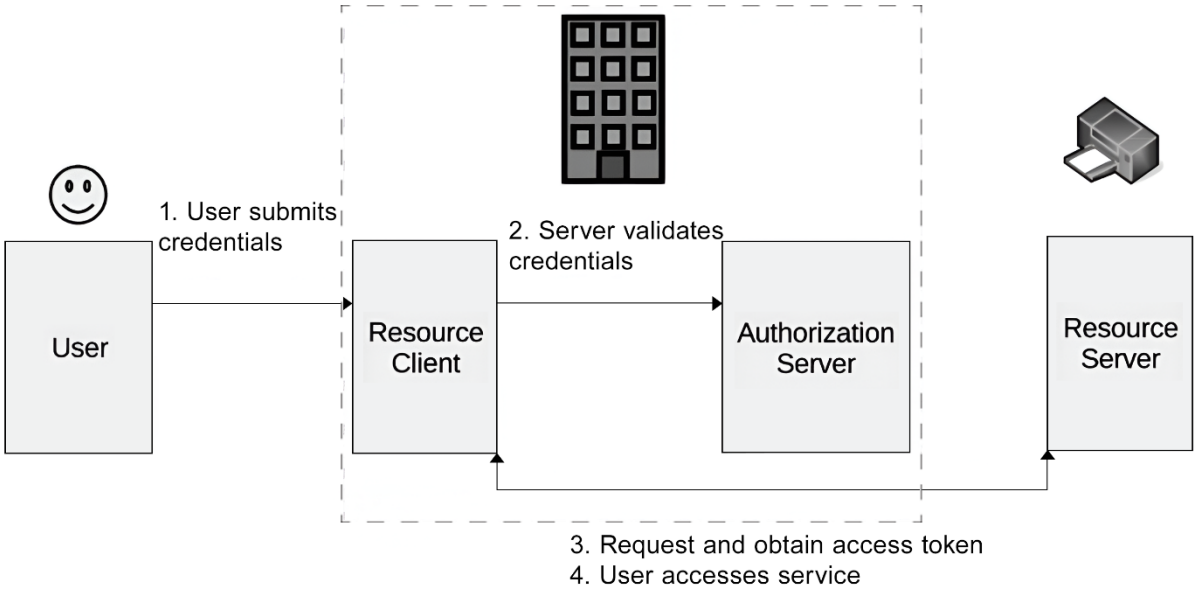
Select Quiz

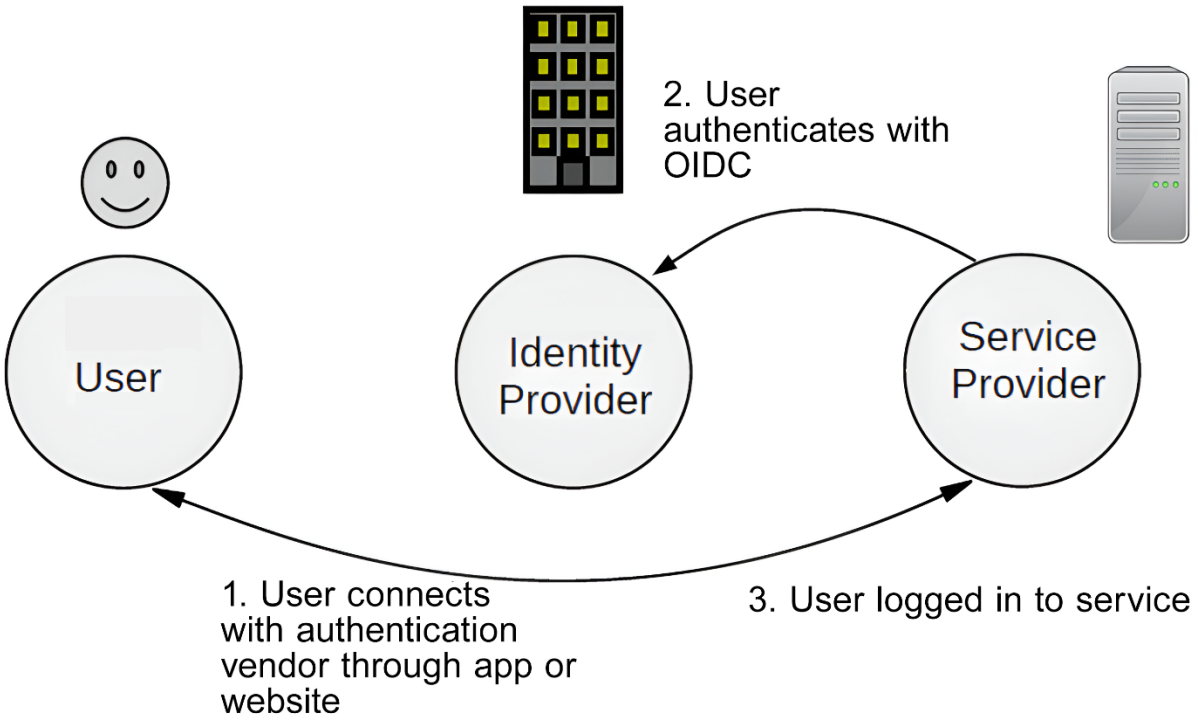
Quiz 1

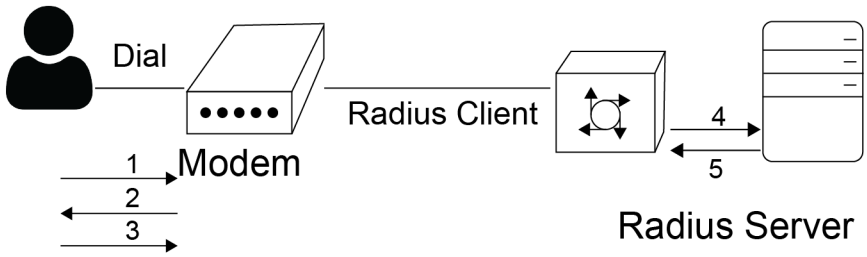
START

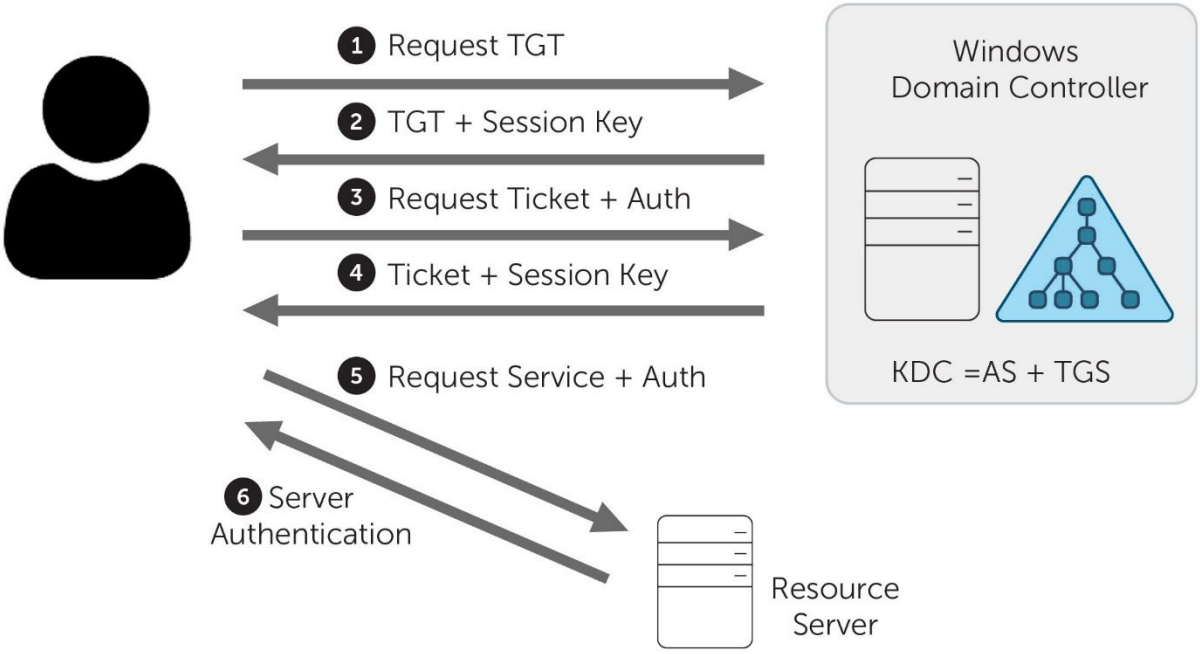
SHOW QUIZ DETAILS

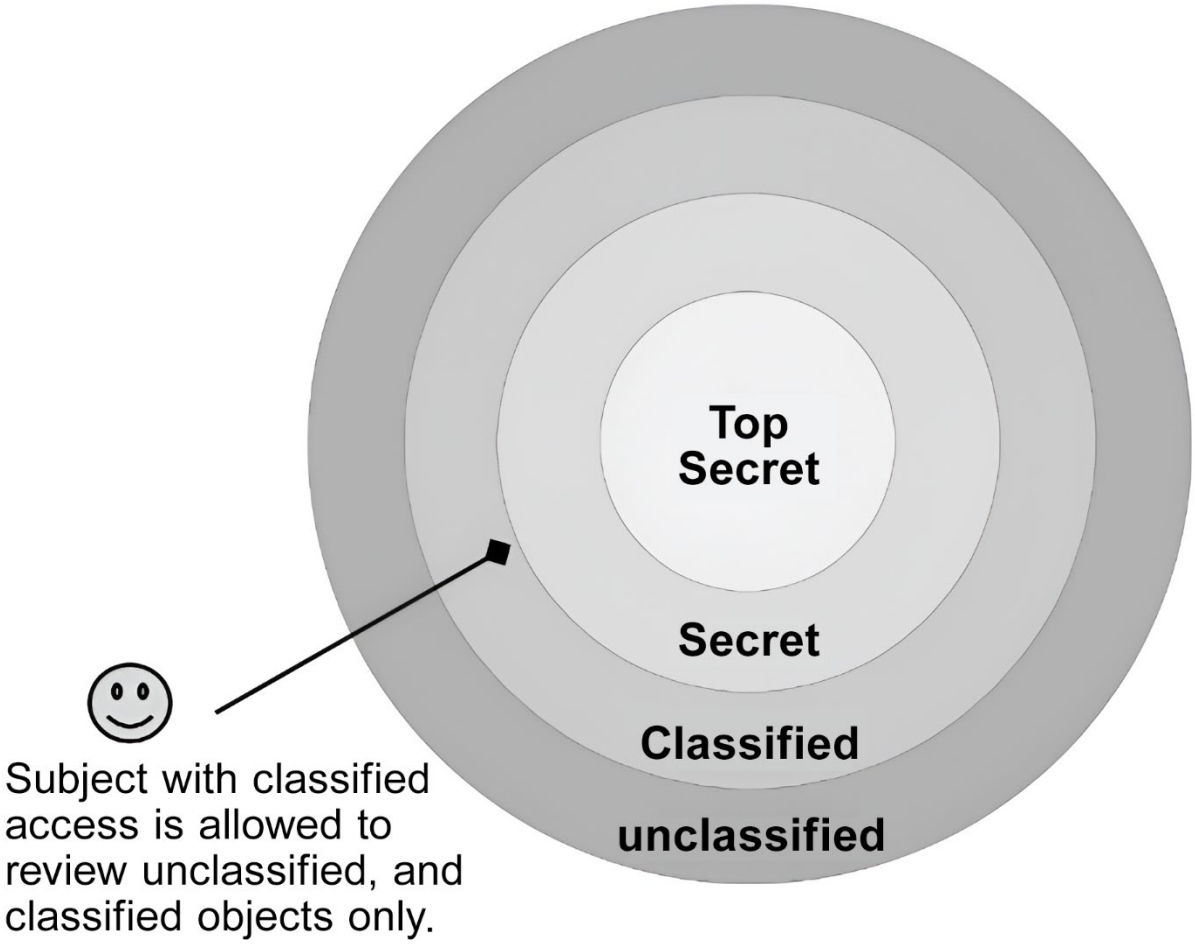

1. User logs in
2. User redirected with SAML
User
Identity Provider
Service Provider
3. User logged in to service


1. User submits credentials
2. Server validates credentials
User
Resource Client
Authorization Server
Resource Server
3. Request and obtain access token
4. User accesses service


2. User
authenticates with
OIDC
User
Identity
Provider
Service
Provider
1. User connects
with authentication
vendor through app or
website
3. User logged in to service


Dial
Radius Client
4
5
1
2
3
Modem
Radius Server


1 Request TGT
2 TGT + Session Key
3 Request Ticket + Auth
4 Ticket + Session Key
5 Request Service + Auth
6 Server
Authentication
Windows
Domain Controller
KDC =AS + TGS
Resource
Server



Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 13

Identity Management Implementation

Summary

This chapter covered user access controls and management. It discussed how organizations can protect against attackers using either physical or technical controls to breach their systems. A major role of the chief security officer and the CISSP is to secure identity access with centralized utilities such as SSO so that users can do their jobs. Users add to security by using strong passwords.

You learned how user access to ancillary products, either within the organization or online, can be simplified if system administrators enable SAML or OAuth 2.0, which provides user identity federation. This keeps users from having to re-authenticate when working on ancillary systems or purchasing related products. These systems use a type of service provider or resource server to manage the identity on the ancillary service.

You also examined **identity as a service** (**IDaaS**), a feature for managing identity federation. Through IDaaS, corporations can hire firms to ease their authentication, authorization, and accounting overhead.

Finally, the chapter discussed access control models. Government systems use **MAC**, or **mandatory access control**, to manage their subjects' interaction with some object. Most corporate organizations use DAC to manage access to objects where availability is more important than confidentiality. In the next chapter you will look at the importance of security assessment and how to design them to be effective.

Chapter Review Questions

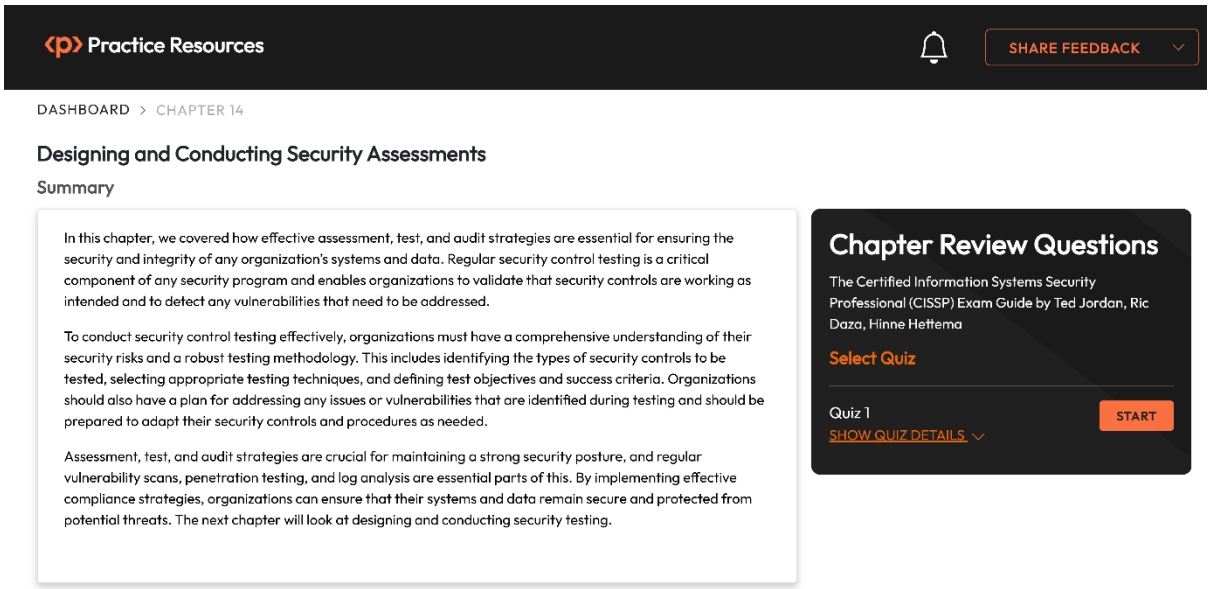
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

Select Quiz

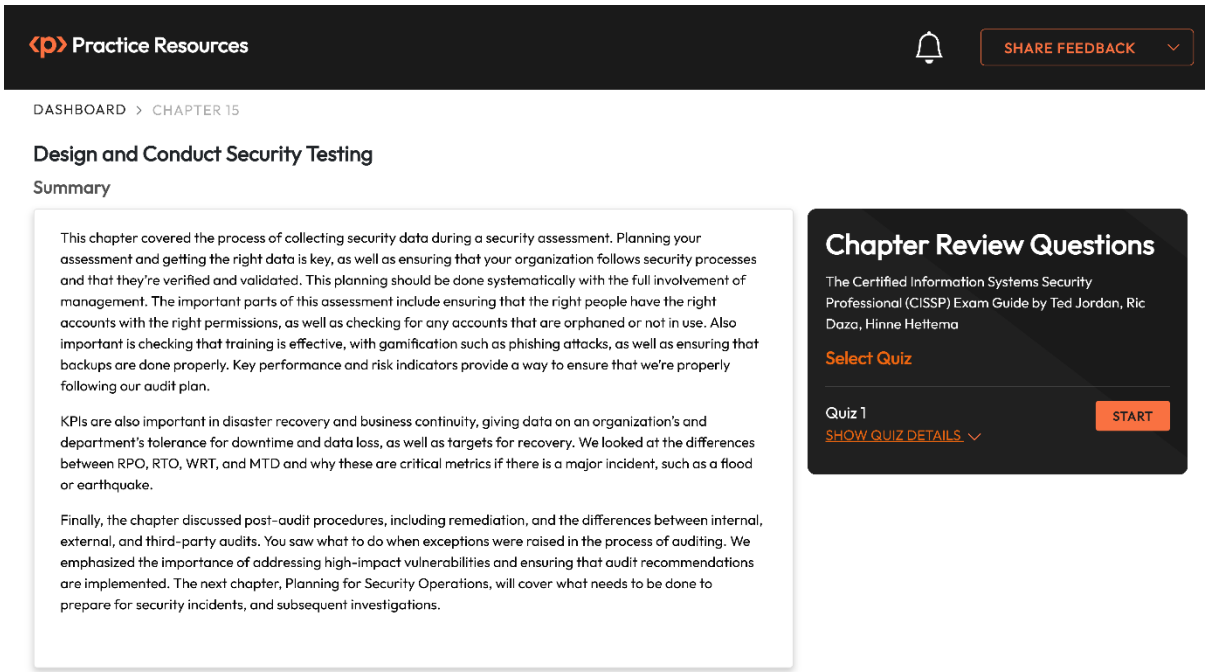
Quiz 1 START

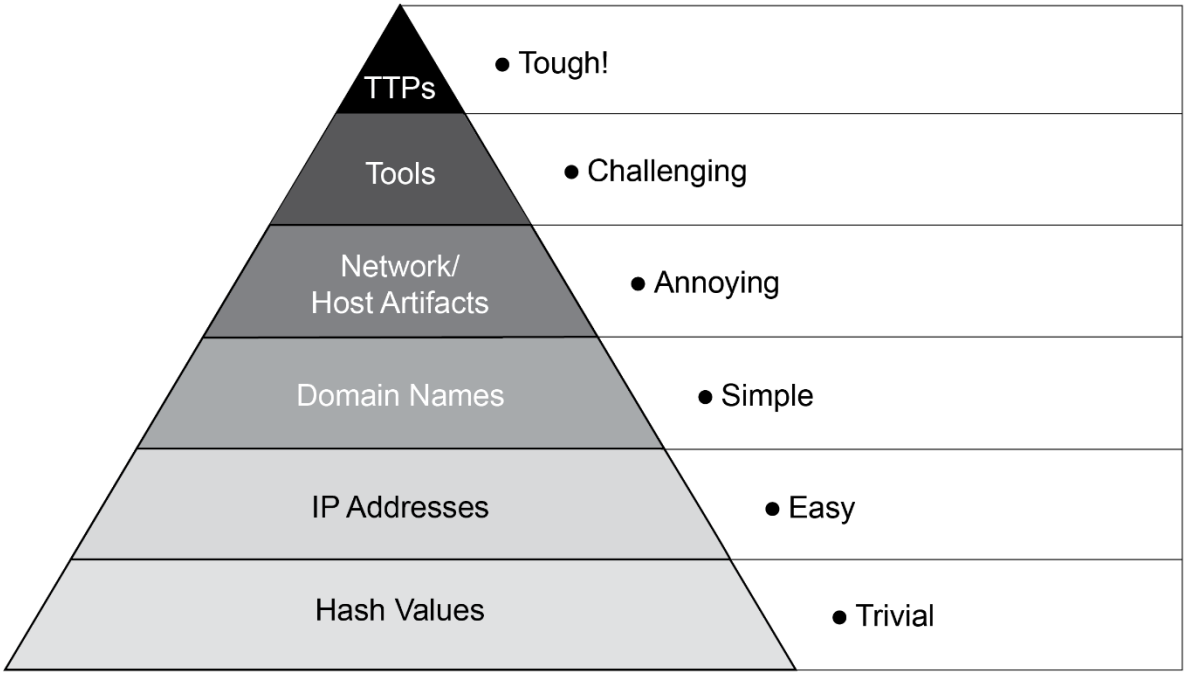
SHOW QUIZ DETAILS

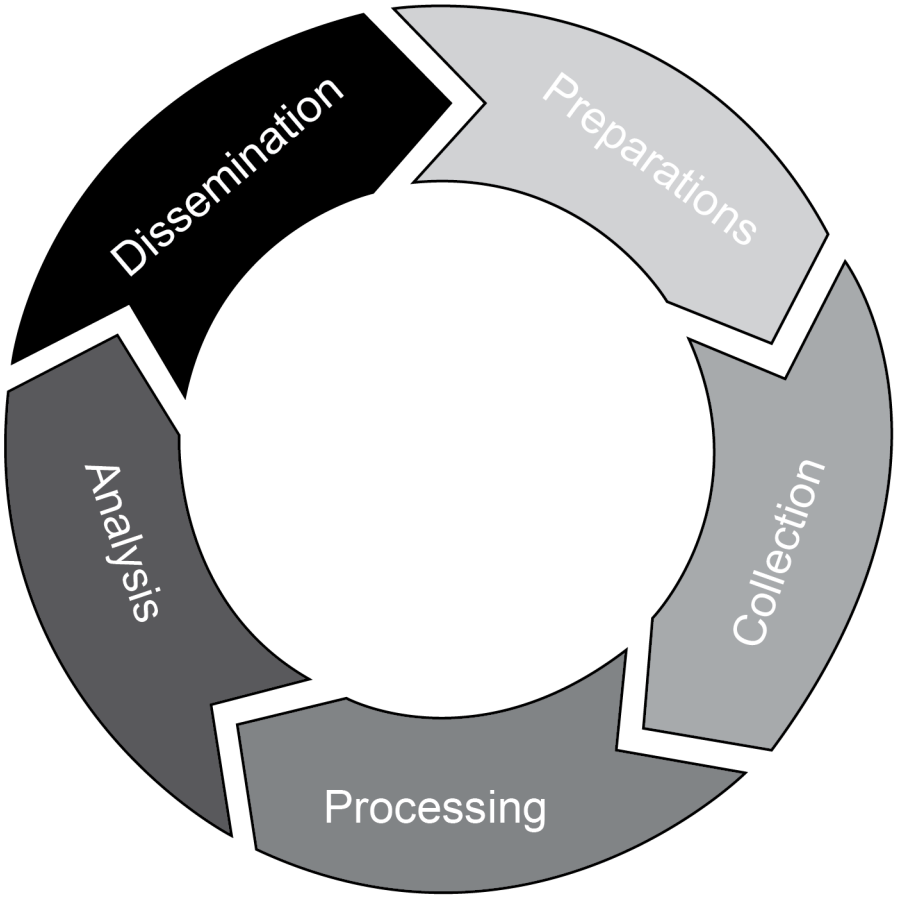
Chapter 14: *Designing and Conducting Security Assessments*

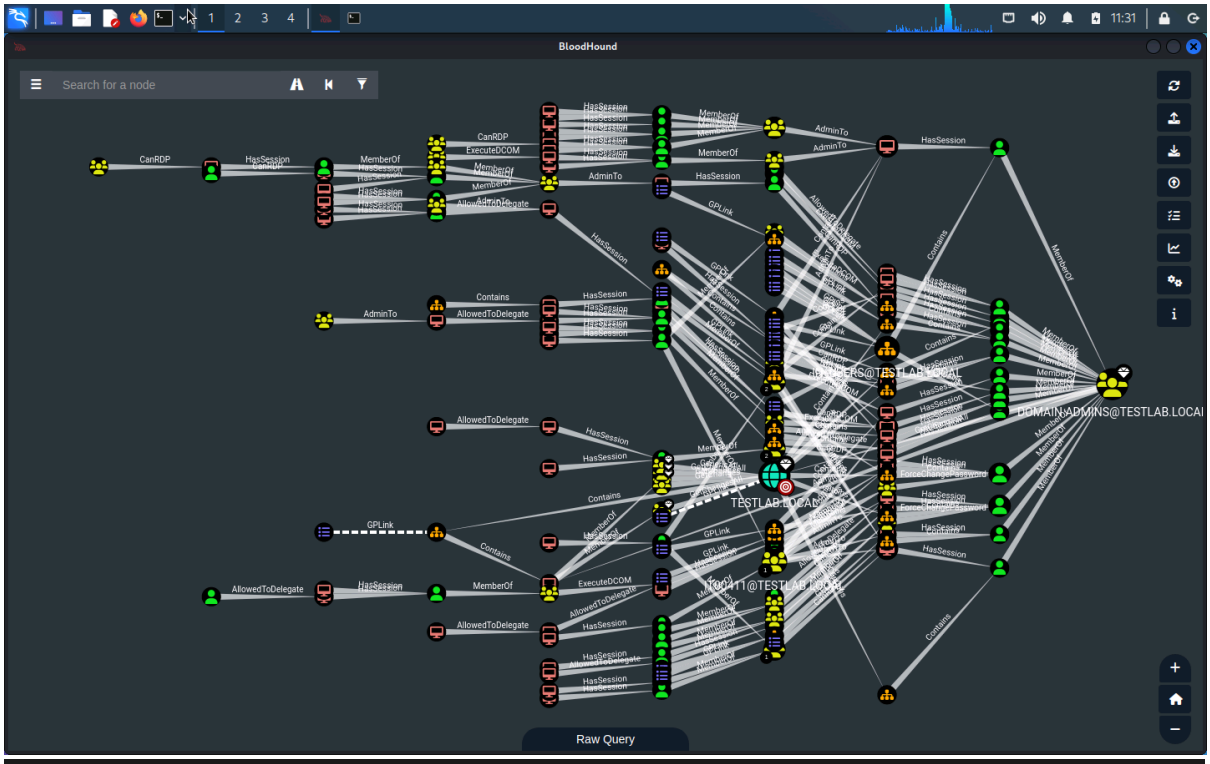


Chapter 15: *Designing and Conducting Security Testing*




TTPs
Tools
Network/
Host Artifacts
Domain Names
IP Addresses
Hash Values
● Tough!
● Challenging
● Annoying
● Simple
● Easy
● Trivial


Dissemination
Preparations
Collection
Processing
Analysis



Planning for Security Operations

Summary

This chapter focused on all the preparation necessary to resolve incidents. As you must have understood by now, there is a lot to think about when it comes to incident resolution. Some of the policies required for security teams were discussed, as well as the corresponding foundational security concepts. This chapter also discussed privileged account management, approaches to logging and monitoring, endpoint protection, and device forensics.

These areas are continually evolving as new technologies and approaches are introduced into the technology landscape, and managers of security programs need to consider the impact of new technologies in light of the requirements also discussed in this chapter.

In the next chapter, we will focus on security operations itself—that is, how security teams put all the things we have discussed in this chapter into practice.

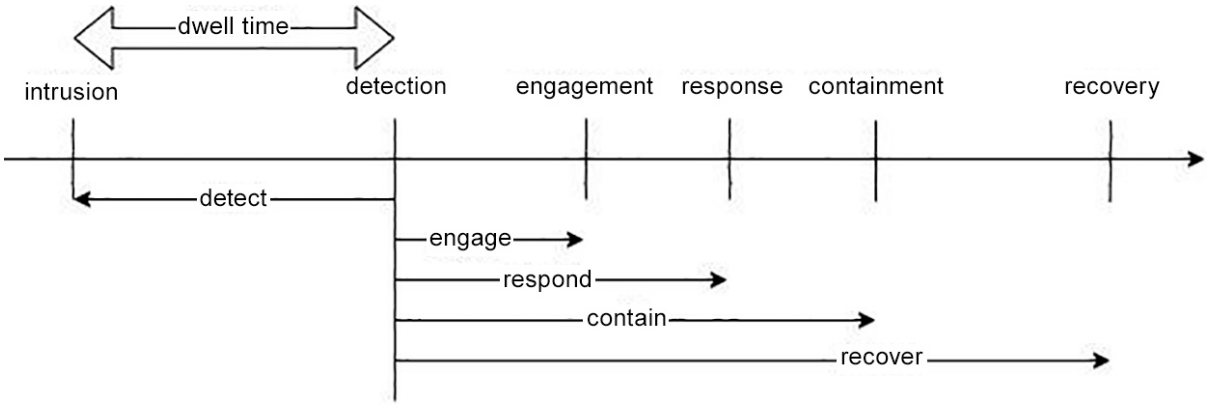
Chapter Review Questions

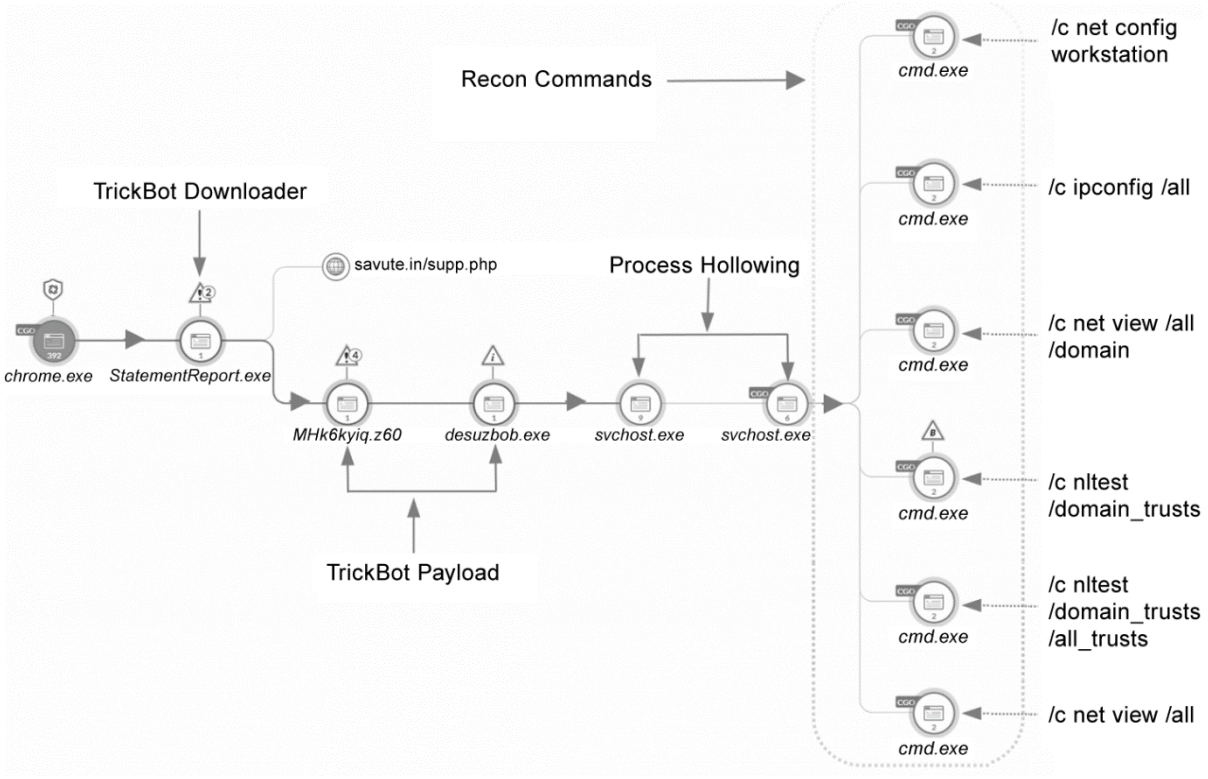
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

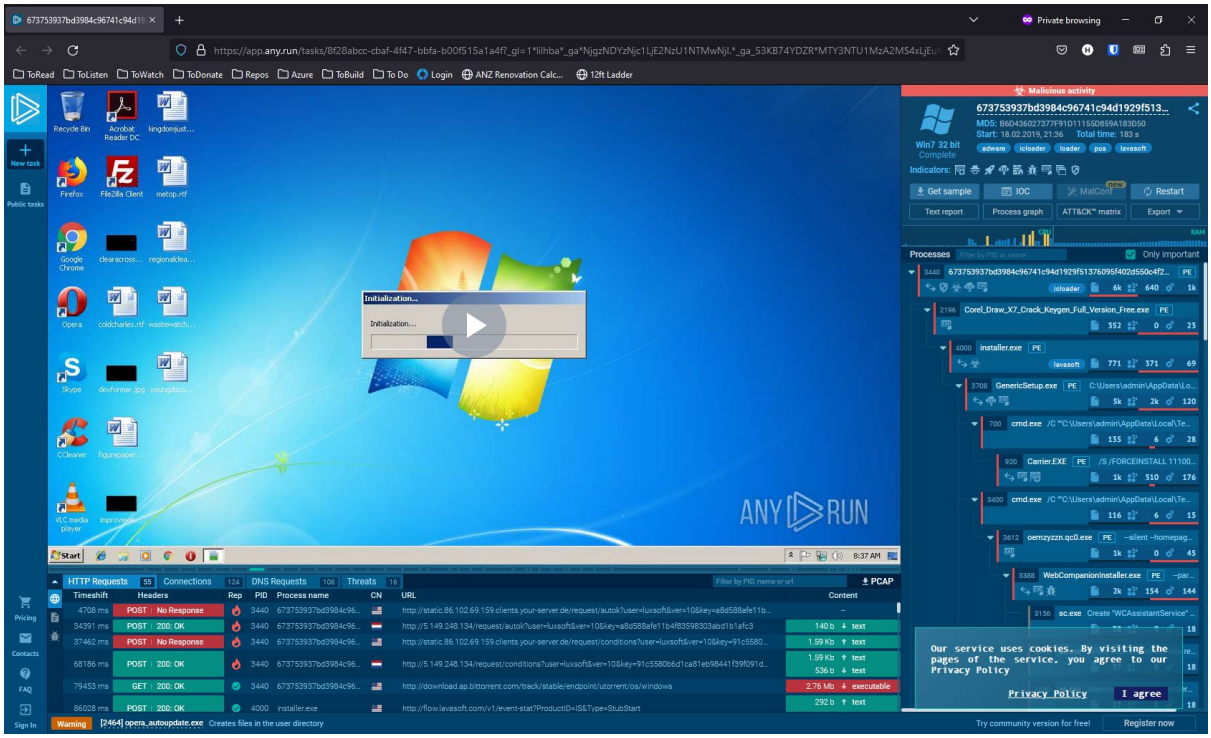
Select Quiz

Quiz 1 START

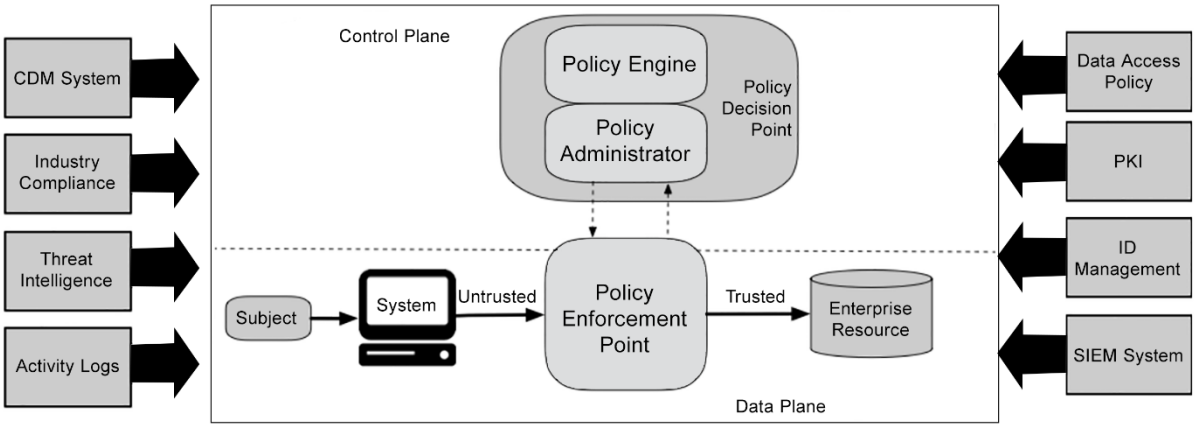
SHOW QUIZ DETAILS

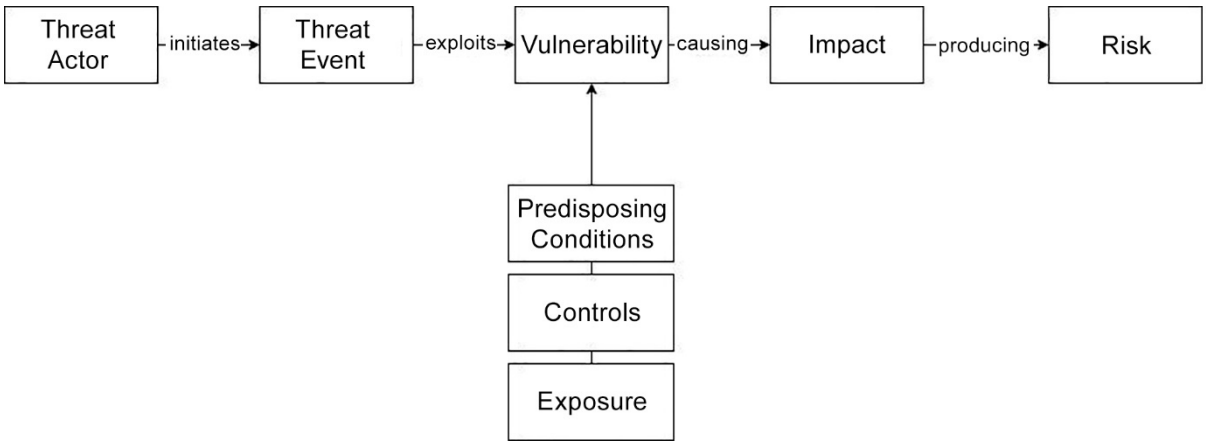

dwell time
intrusion
detection
engagement
response
containment
recovery
detect
engage
respond
contain
recover


Recon Commands
TrickBot Downloader
savute.in/supp.php
Process Hollowing
chrome.exe
StatementReport.exe
MHk6kyiq.z60
desuzbob.exe
svchost.exe
svchost.exe
TrickBot Payload
cmd.exe
/c net config workstation
cmd.exe
/c ipconfig /all
cmd.exe
/c net view /all /domain
cmd.exe
/c nltest /domain_trusts
cmd.exe
/c nltest /domain_trusts /all_trusts
cmd.exe
/c net view /all


Private browsing
Malicious activity
Initialization...
ANY RUN
Our service uses cookies. By visiting the pages of the service, you agree to our Privacy Policy
Privacy Policy
I agree

S


Control Plane
CDM System
Industry Compliance
Threat Intelligence
Activity Logs
Policy Engine
Policy Administrator
Policy Decision Point
Subject
System
Untrusted
Policy Enforcement Point
Trusted
Enterprise Resource
Data Plane
Data Access Policy
PKI
ID Management
SIEM System


Threat Actor
initiates
Threat Event
exploits
Vulnerability
causing
Impact
producing
Risk
Predisposing Conditions
Controls
Exposure

Security Operations

Summary

In this chapter, you explored the nitty-gritty of security operations and what an actual implementation looks like. The chapter discussed the management of cybersecurity incidents and some of the settings for operating and maintaining an operational security practice. How this works in practice depends, in many ways, on the nature of the organization, its culture, and how it generally manages its IT environment when it comes to monitoring, incidents, and changes.

Security teams need to work with the rest of the organization to ensure that their practices align with what is already established practice in an organization but also ensure that in doing so they can and will maintain an acceptable security baseline. That is a difficult undertaking.

Despite all the best efforts of the security and IT team, disasters, in the form of system compromise or natural disasters, sometimes do occur. That is the topic of the next chapter.

Chapter Review Questions

The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

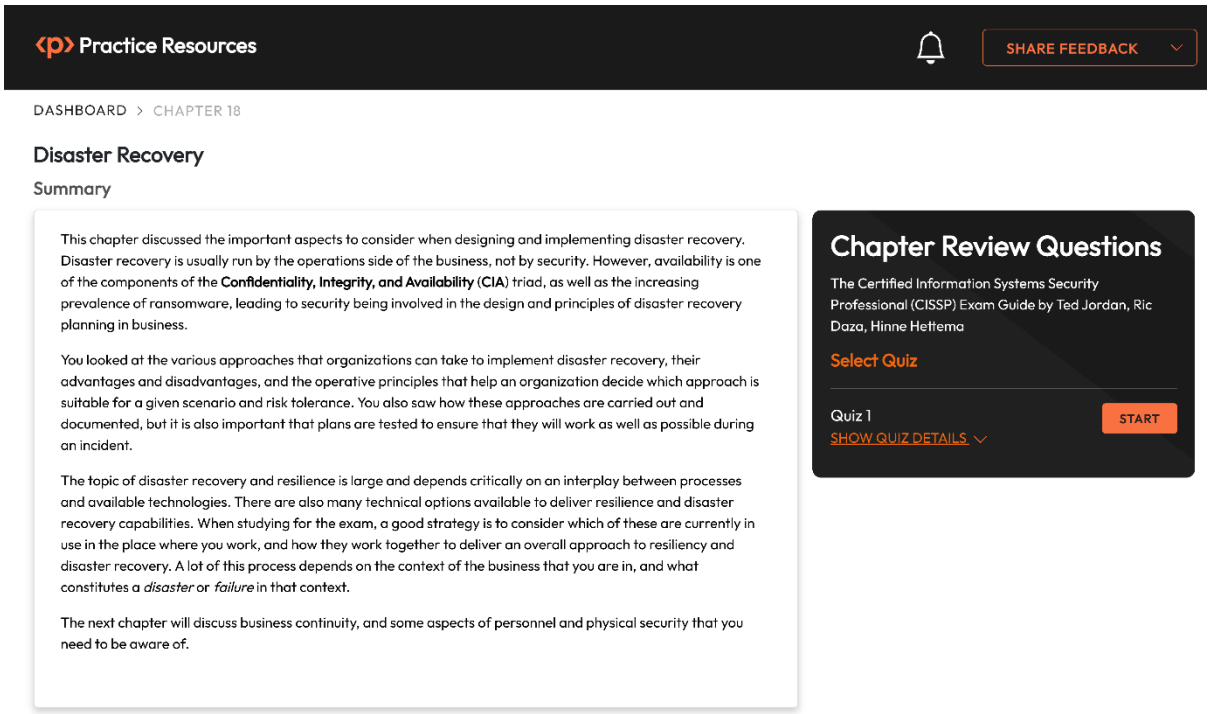
Select Quiz

Quiz 1

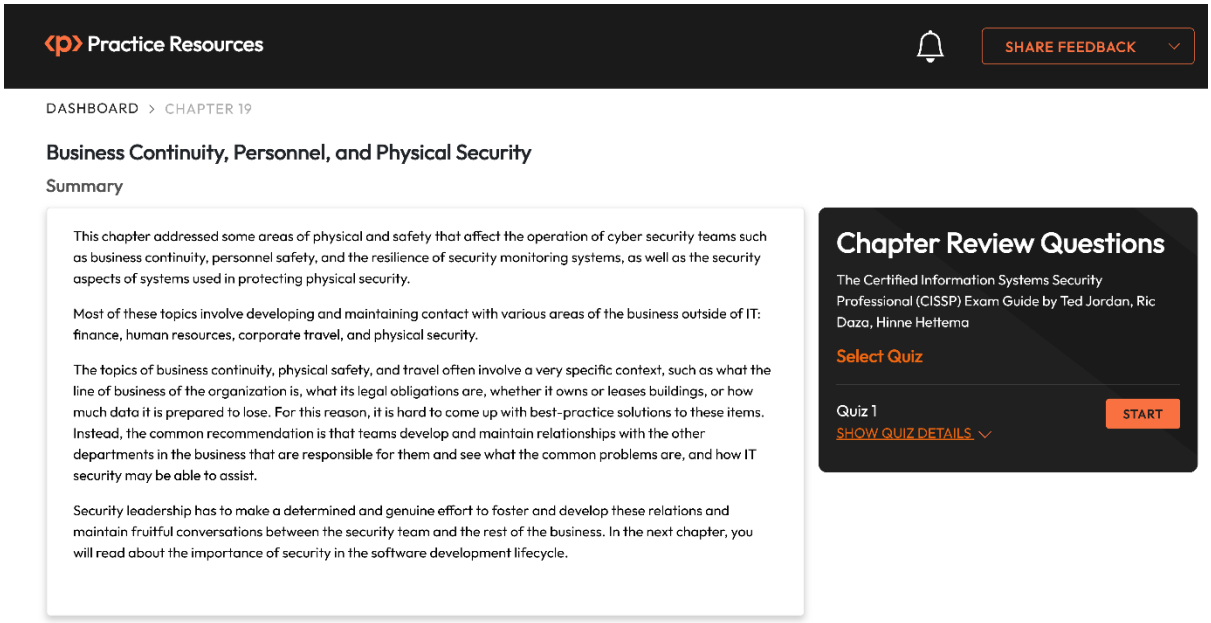
START

SHOW QUIZ DETAILS

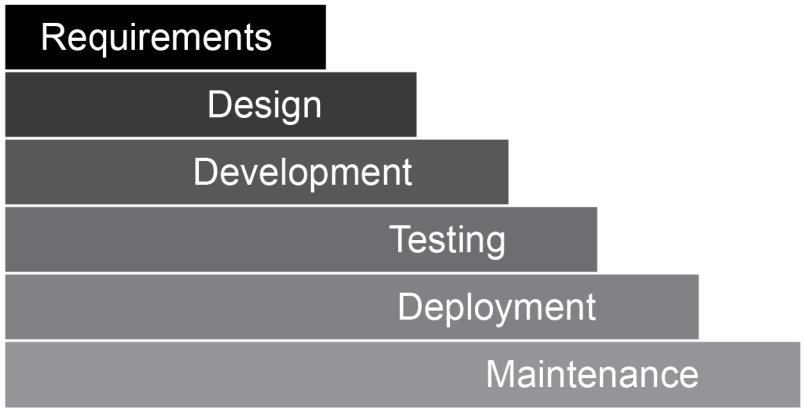
Chapter 18: *Disaster Recovery*

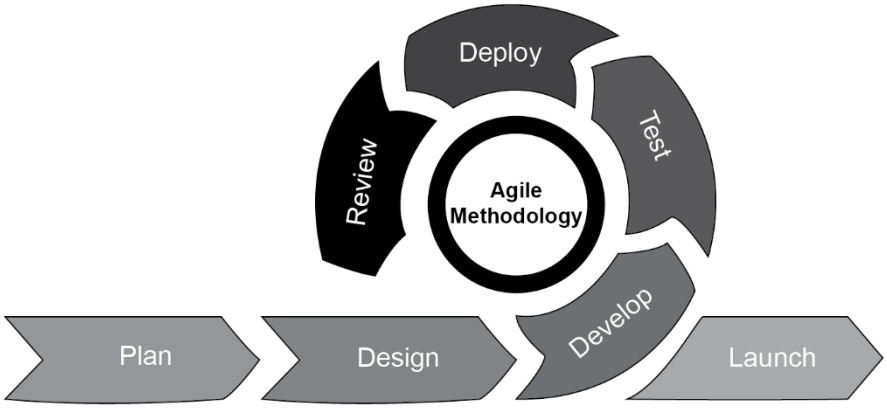


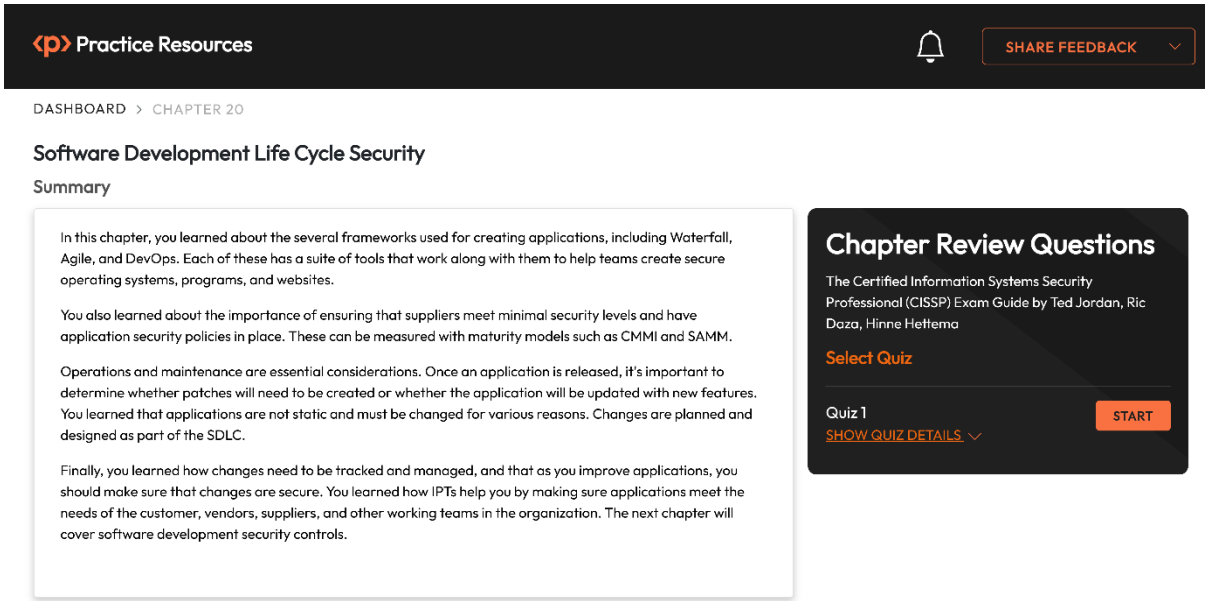
Chapter 19: *Business Continuity*



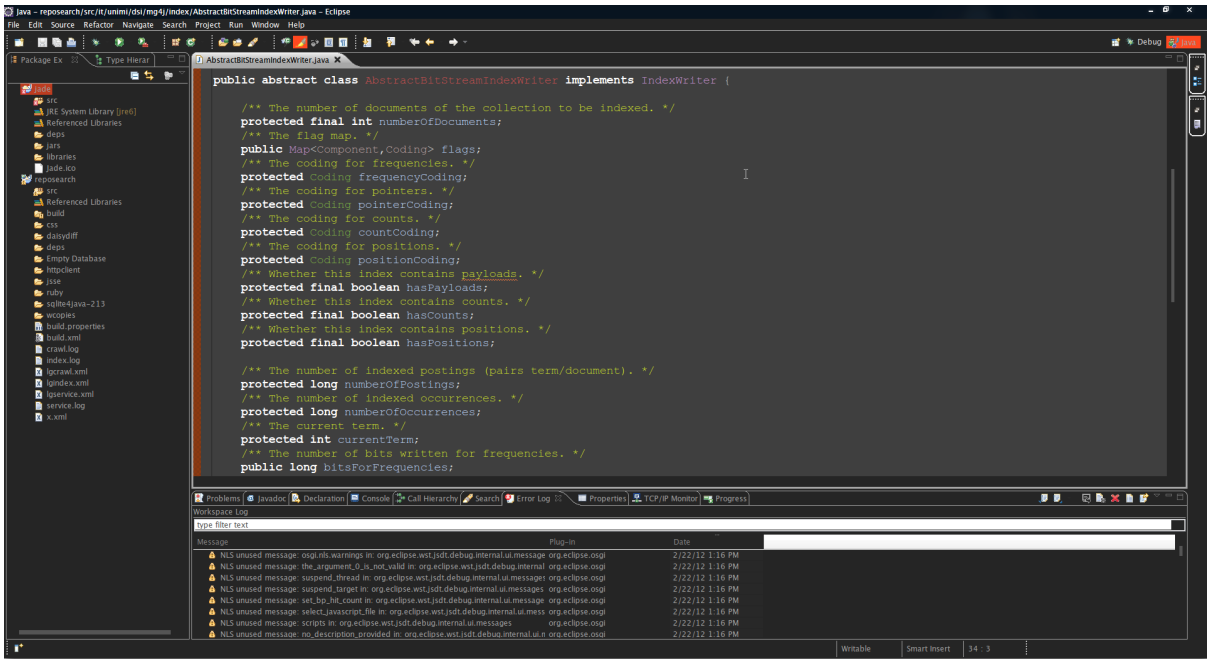
Chapter 20: ***Software Development Life Cycle Security***

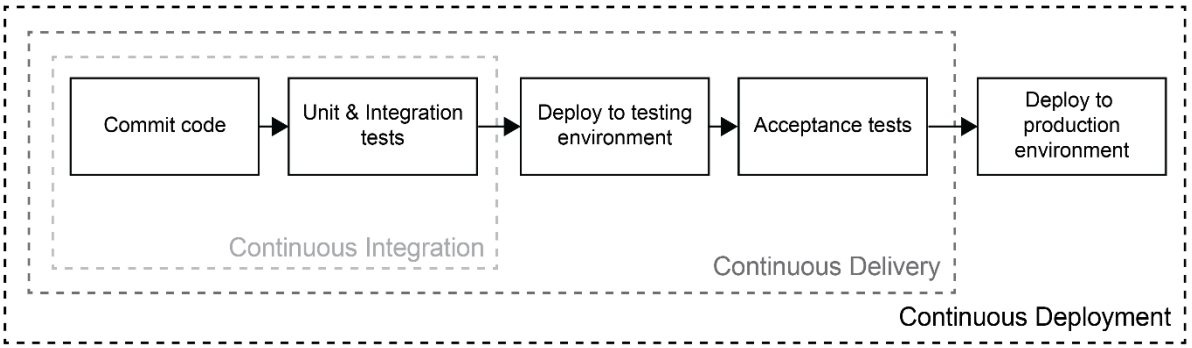






Chapter 21: *Software Development Security Controls*





Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 21

Software Development Security Controls

Summary

In this chapter, you explored various aspects of software development. Understanding the different levels of programming languages helps in analyzing the foundational principles of how code interacts with computer systems. Earlier-generation languages, which are closer to machine language and pure binary, provide more direct access to system resources, while later-generation languages are easier to read and more portable. The differing characteristics of these programming languages lead to different security concerns when considering secure coding practices. Additionally, you examined how the compilation process and runtime environments can introduce new security challenges.

You saw CI/CD security controls focus on integrating security checks into each stage of the software development life cycle. This includes using SAST tools to scan code for vulnerabilities, and DAST tools to scan running applications for weaknesses. Security analysts also use penetration testing to identify flaws.

Software security automation is the use of tools that automate security tasks throughout the SDLC. This includes automating the deployment of security controls, security tests, and remediation of vulnerabilities. The next chapter will cover securing software development.

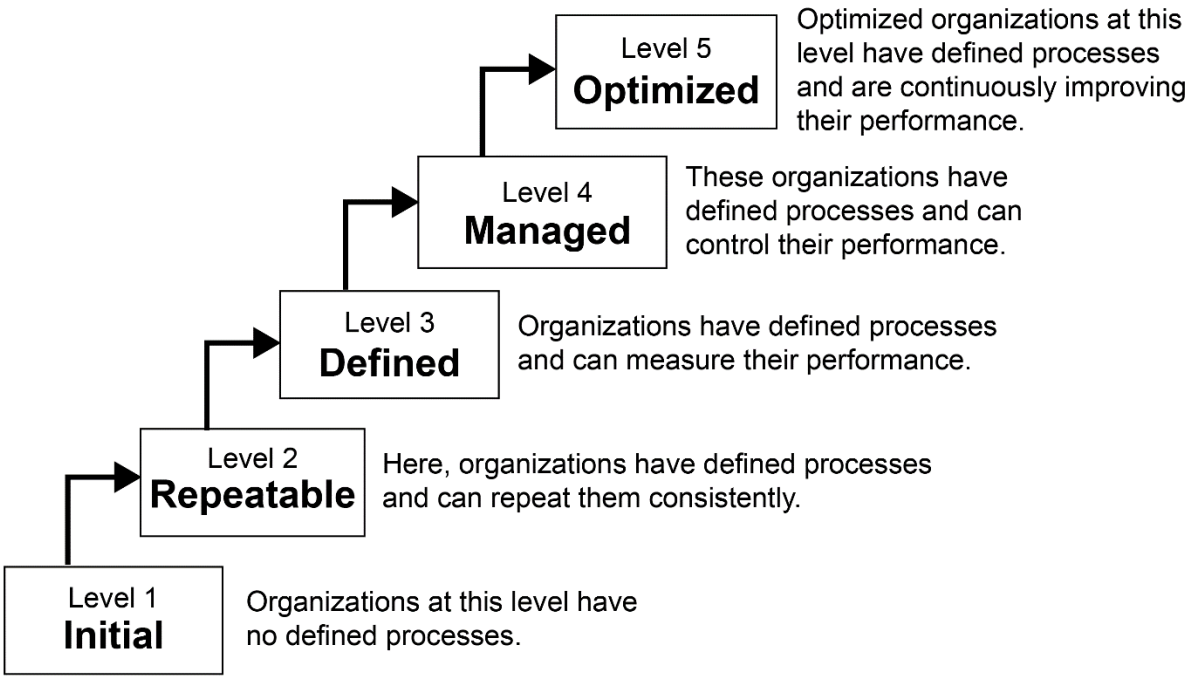
Chapter Review Questions

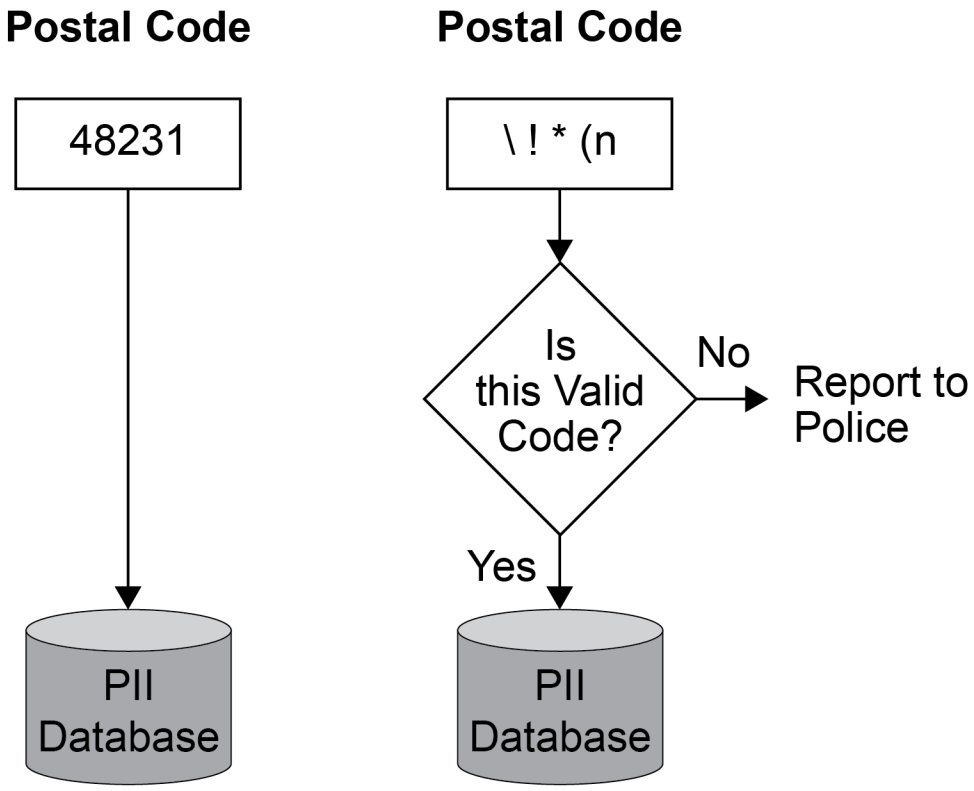
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

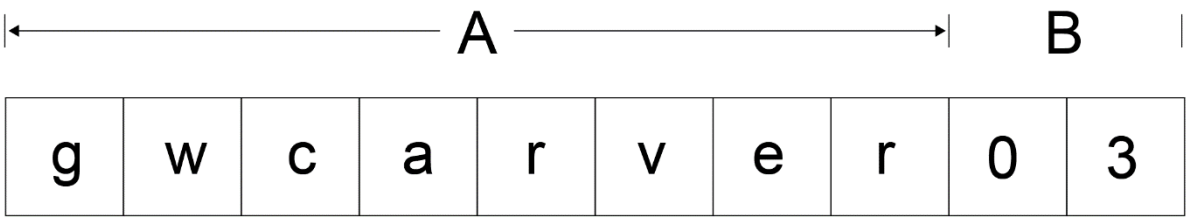
Select Quiz

Quiz 1 START

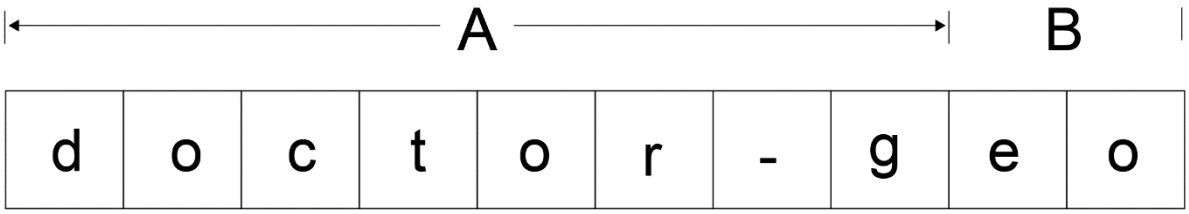
SHOW QUIZ DETAILS


Level 5
Optimized
Optimized organizations at this level have defined processes and are continuously improving their performance.
Level 4
Managed
These organizations have defined processes and can control their performance.
Level 3
Defined
Organizations have defined processes and can measure their performance.
Level 2
Repeatable
Here, organizations have defined processes and can repeat them consistently.
Level 1
Initial
Organizations at this level have no defined processes.


Postal Code
48231
PII Database
Postal Code
\ ! * (n
Is this Valid Code?
No
Report to Police
Yes
PII Database



doctor-geol → A



Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 22

Securing Software Development

Summary

This chapter started with a discussion about the effectiveness of software security. You examined how to audit software changes and the importance of logging software changes. When users write thousands of lines of code, errors are more likely.

One system that helps to measure the software development process for developers is the CMMI model. The closer the development team gets to the top of the scale, or 5, the better that developer's processes are. Then you learned about software vulnerabilities; the top 3 have to do with poor authentication, broken encryption, and injection attacks. Other vulnerabilities are SQL injection and buffer overflow attacks.

Next, you learned about working with software developers and COTS software. In most cases, you're not going to be able to see the source code, so it's important to make sure that these developers have strong software development processes and secure policies; again, the CMMI model can help find the best developer.

Finally, the chapter concluded with an overview of managed software providers and a review of the SOC 3 or SOC 2 report to make sure they follow software security policies. To confirm that developers have security controls in place and that they are effective, you need to view the SOC 2 Type II report. The SOC 2 Type I report only confirms that the vendor has security controls in place.

You will read about secure coding practices and issues around artificial intelligence and security in the next chapter.

Chapter Review Questions

The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

Select Quiz

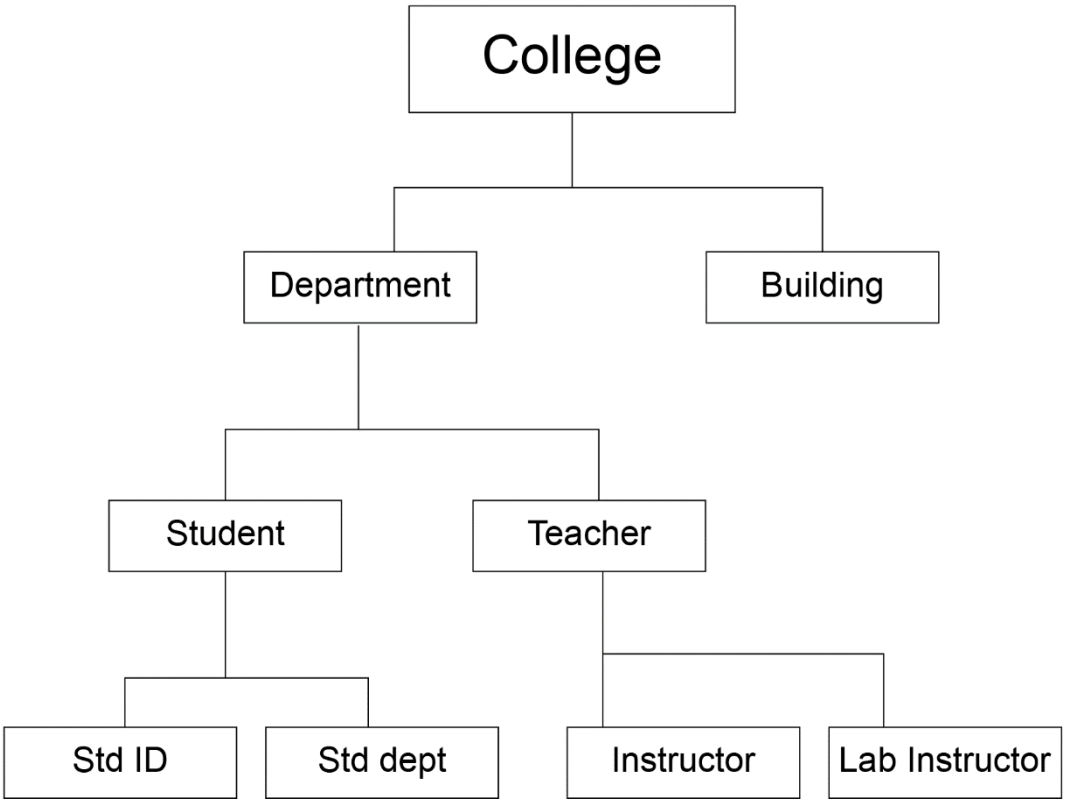
Quiz 1

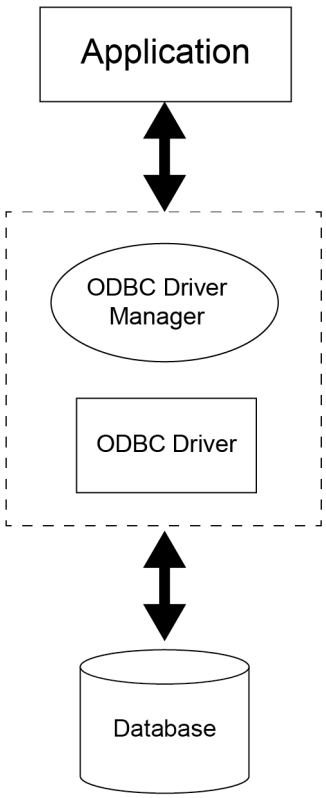
START

SHOW QUIZ DETAILS

```
bosko@pnap:~$ telnet google.com 22
Trying 142.251.39.78...
Trying 2a00:1450:400d:80e::200e...
telnet: Unable to connect to remote host: Network is unreachable
```

```
bosko@pnap:~$ telnet google.com 80
Trying 142.251.39.78...
Connected to google.com.
Escape character is '^]'.
```





Practice Resources

SHARE FEEDBACK

DASHBOARD > CHAPTER 23

Secure Coding Guidelines, Third-Party Software, and Databases

Summary

This chapter covered secure coding guidelines around working with suppliers and other third-party vendors. Whether you are developing applications on your own or have outsourced the work, it is important to design applications with security built in from the requirements stage of the SDLC. There are some risks of having third parties develop applications for you. One important risk is the possibility of the firm going out of business. Processes such as third-party trust and code escrow can mitigate the risks of you losing your entire project should the worst happen to your supplier. Most applications work with some type of database, so securing these database systems is important. You learned how ACID secures database transactions and data. Finally, you learned about the differences between expert systems, machine learning, and neural networks, and how these can secure applications.

Security is an ongoing process. It is the recommended best practice to integrate security measures throughout the entire SDLC, from the planning and development phases to the deployment and maintenance ones. By prioritizing application security, you can safeguard your organization's most valuable asset.

Chapter Review Questions

The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

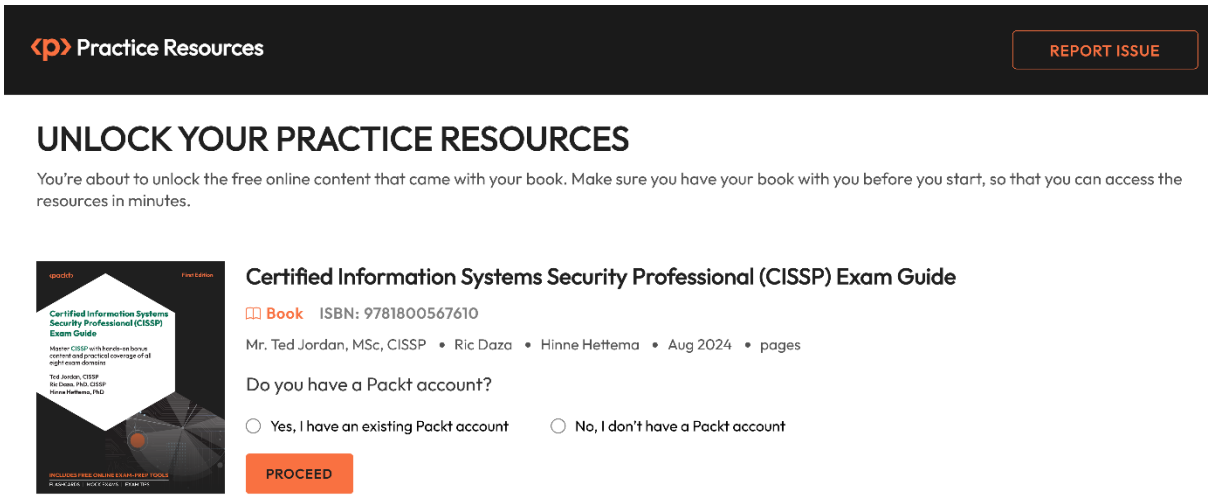
Select Quiz

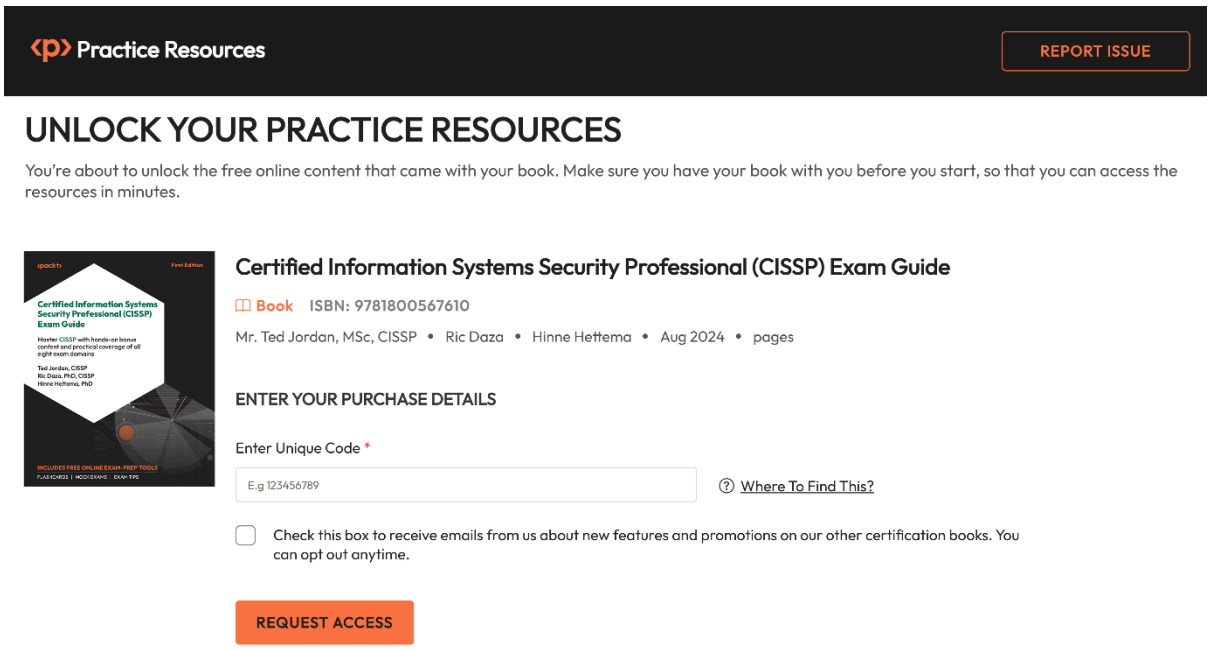
Quiz 1

SHOW QUIZ DETAILS

START

Chapter 24: *Accessing the Online Practice Resources*

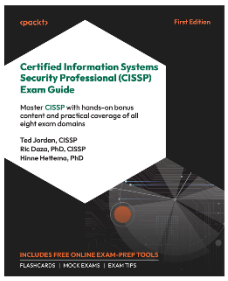




Practice Resources

REPORT ISSUE

You've just unlocked the free online content that came with your book.



Certified Information Systems Security Professional (CISSP) Exam Guide

Book ISBN: 9781800567610

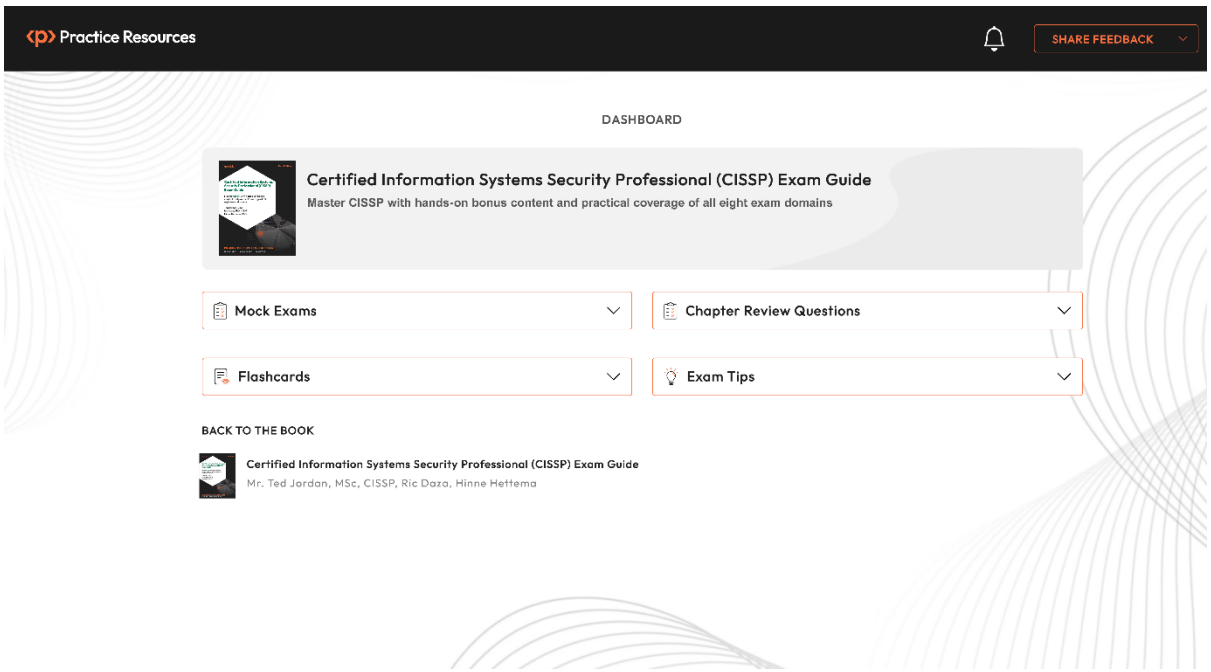
Mr. Ted Jordan, MSc, CISSP • Ric Daza • Hinne Hettema • Aug 2024 • pages

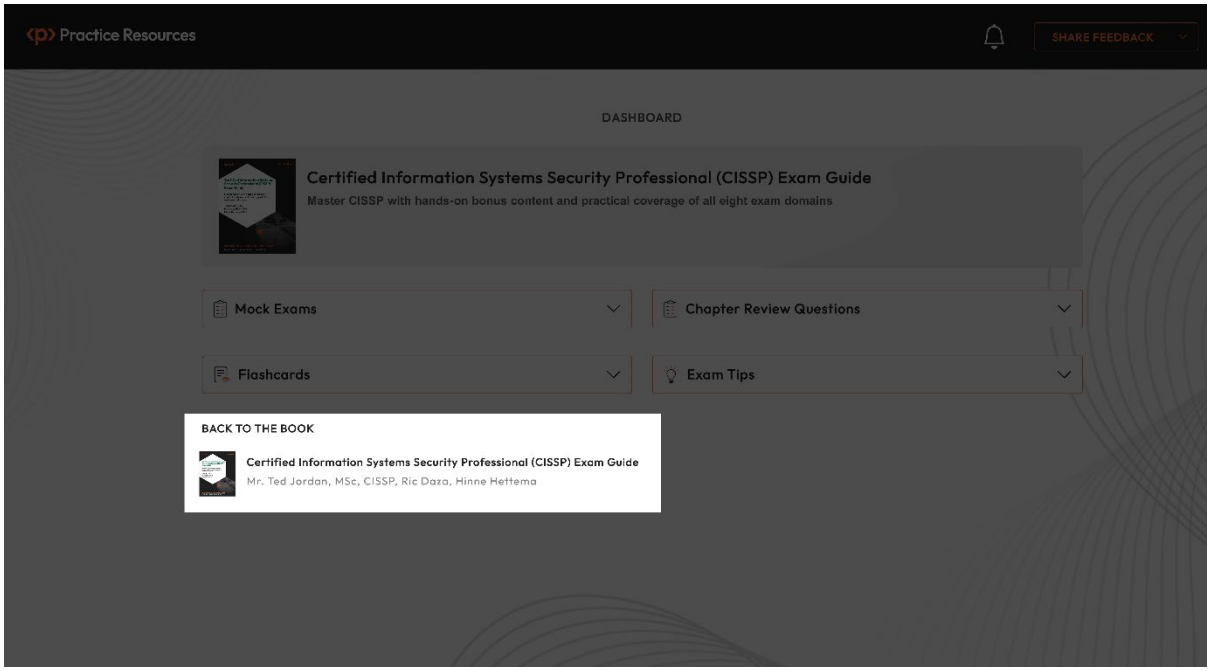
Unlock Successful

Click the following link to access your practice resources at any time.

Pro Tip: You can switch seamlessly between the ebook version of the book and the practice resources. You'll find the ebook version of this title in your Owned Content

OPEN PRACTICE RESOURCES




Practice Resources
SHARE FEEDBACK
DASHBOARD
Certified Information Systems Security Professional (CISSP) Exam Guide
Master CISSP with hands-on bonus content and practical coverage of all eight exam domains
Mock Exams
Chapter Review Questions
Flashcards
Exam Tips
BACK TO THE BOOK
Certified Information Systems Security Professional (CISSP) Exam Guide
Mr. Ted Jordan, MSc, CISSP, Ric Daza, Hinne Hettema