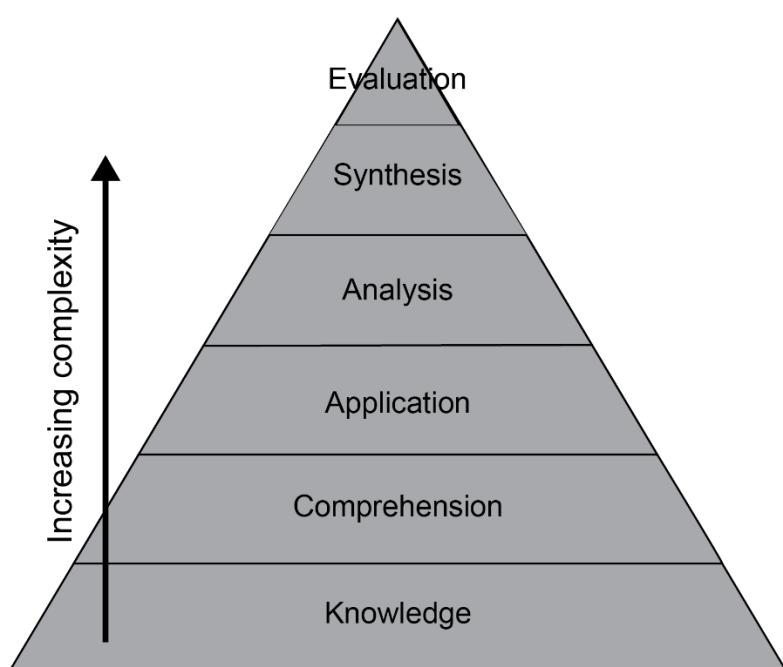


# Certified Information Systems Security Professional (CISSP) Exam Guide

## Introduction 1:

The screenshot shows the 'DASHBOARD' section of the Practice Resources website. At the top, there's a banner for the 'Certified Information Systems Security Professional (CISSP) Exam Guide' with the subtitle 'Master CISSP with hands-on bonus content and practical coverage of all eight exam domains'. Below the banner are four expandable sections: 'Mock Exams', 'Chapter Review Questions', 'Flashcards', and 'Exam Tips'. At the bottom of the dashboard, there's a link to 'BACK TO THE BOOK' which leads to the book's page.

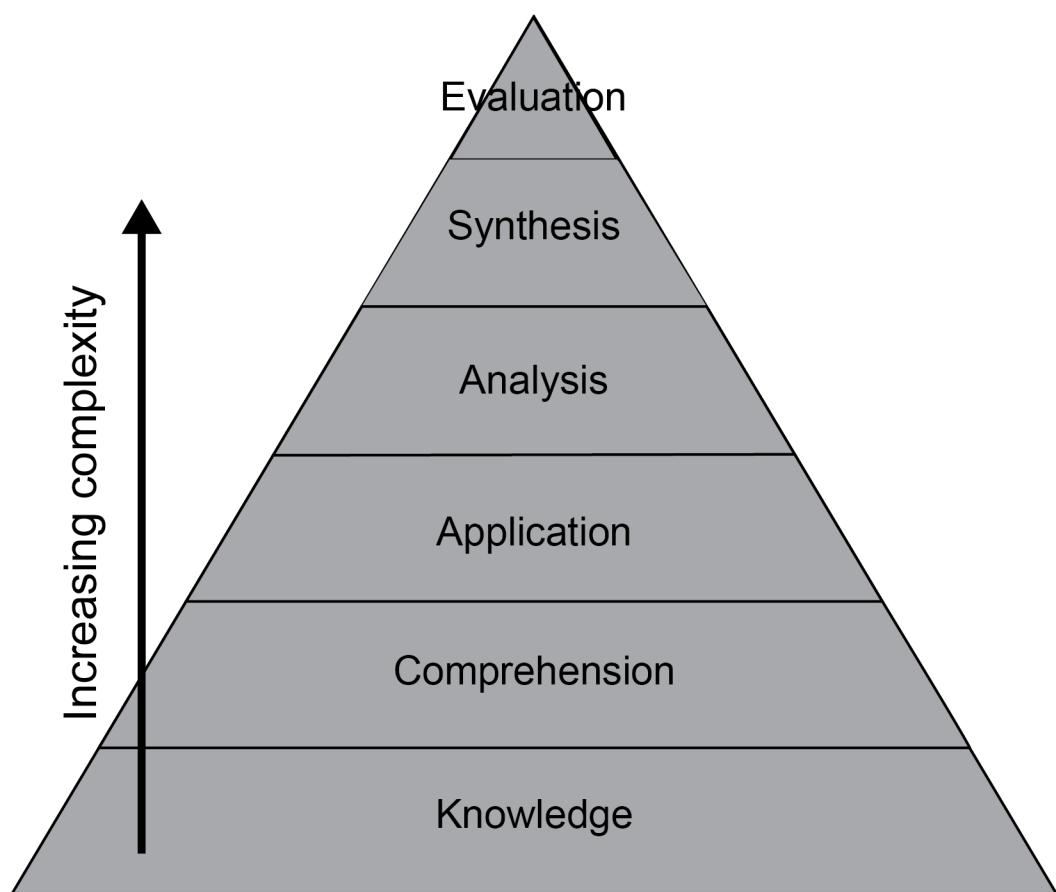




## Preface:

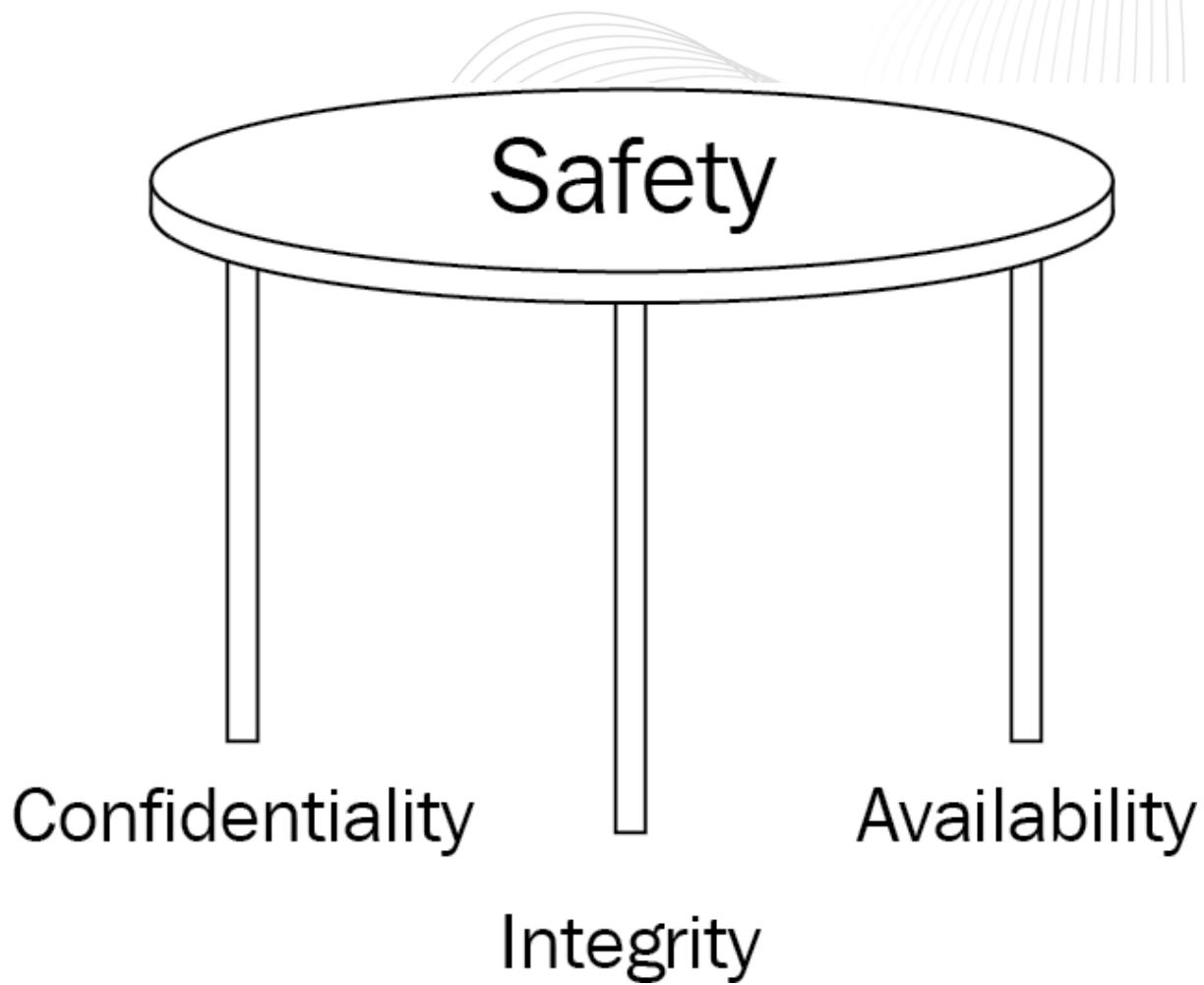
The screenshot shows the 'Practice Resources' interface for the CISSP Exam Guide. At the top, there's a navigation bar with a bell icon and a 'SHARE FEEDBACK' button. Below it is a 'DASHBOARD' section featuring a thumbnail of the book cover and the title 'Certified Information Systems Security Professional (CISSP) Exam Guide'. A subtitle below the title reads 'Become a certified CISSP professional with practical exam-oriented knowledge of all eight domains'. Below this are four expandable sections: 'Mock Exams', 'Chapter Review Questions', 'Flashcards', and 'Exam Tips', each with a corresponding icon. At the bottom left, there's a link to 'BACK TO THE BOOK'.

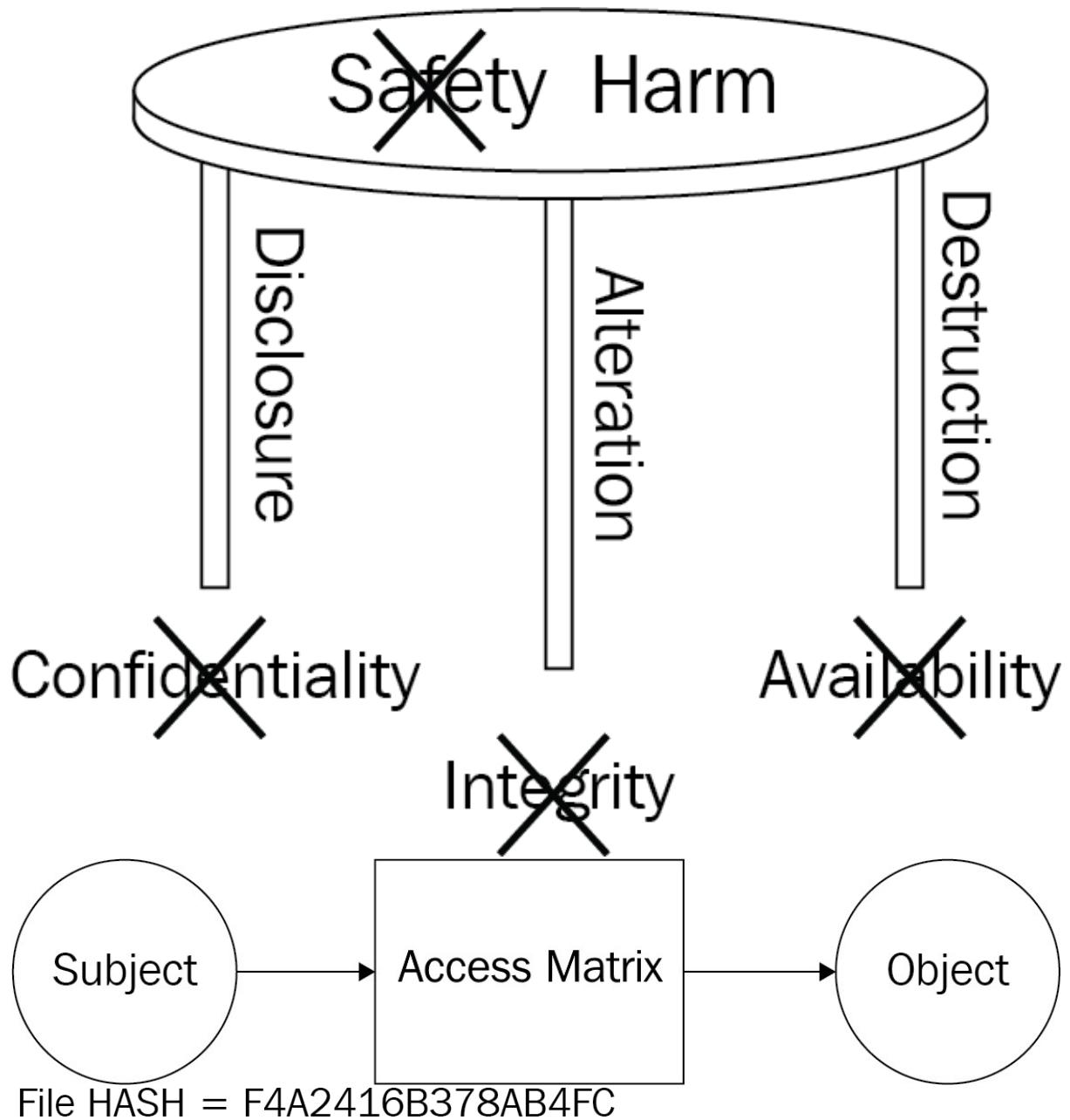
**Introduction 1:**

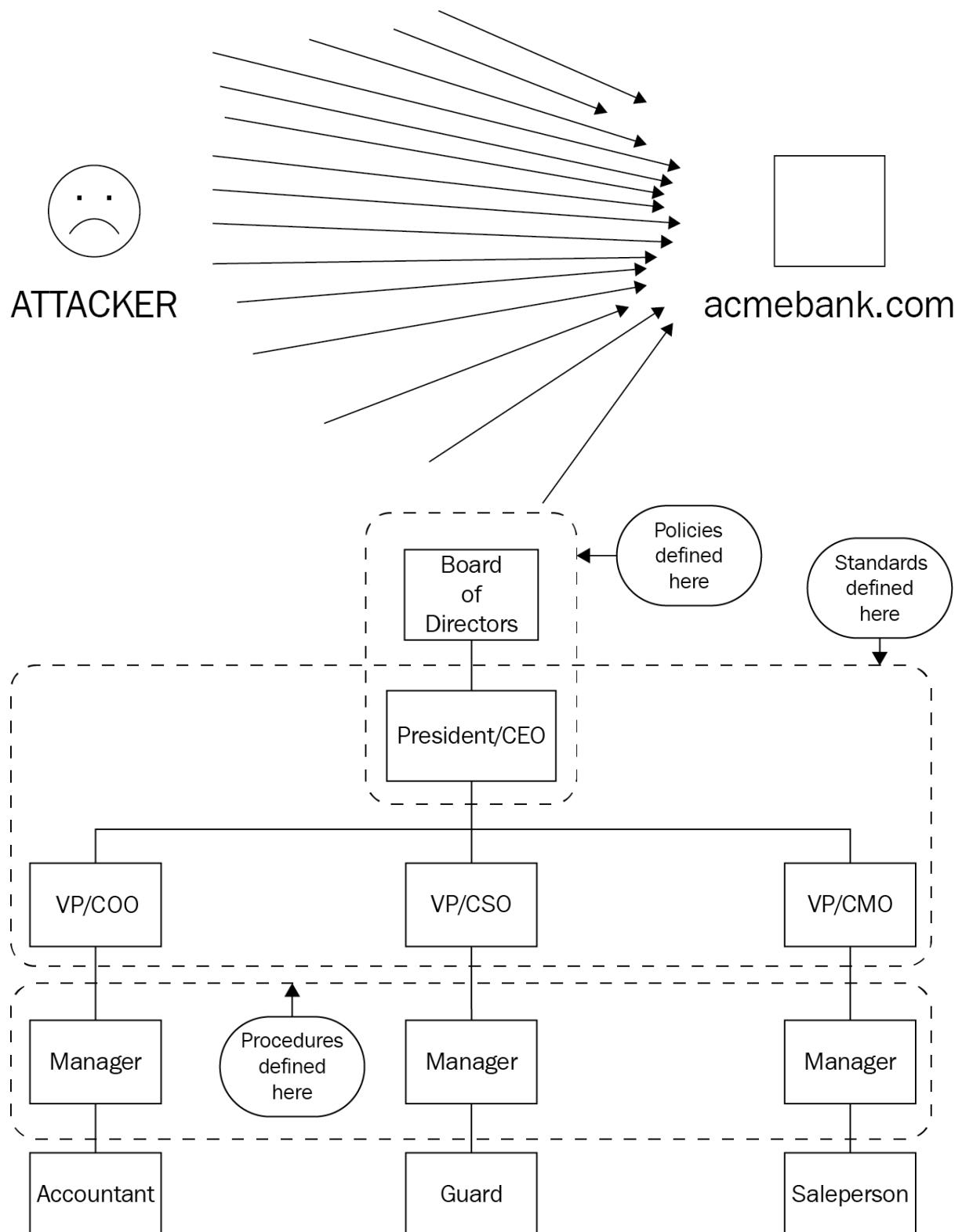


## Chapter 1: Ethics, Security Concepts, and Governance Principles

The screenshot shows the 'DASHBOARD' section of the CISSP Exam Guide Practice Resources. At the top, there's a header with a bell icon and a 'SHARE FEEDBACK' button. Below the header, a large callout box for the 'Certified Information Systems Security Professional (CISSP) Exam Guide' is displayed, featuring a book cover thumbnail and the text 'Become a certified CISSP professional with practical exam-oriented knowledge of all eight domains'. Below this, there are four expandable sections: 'Mock Exams', 'Chapter Review Questions', 'Flashcards', and 'Exam Tips'. At the bottom left, a link to 'BACK TO THE BOOK' is shown, accompanied by a small book icon.









## 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 Heffema

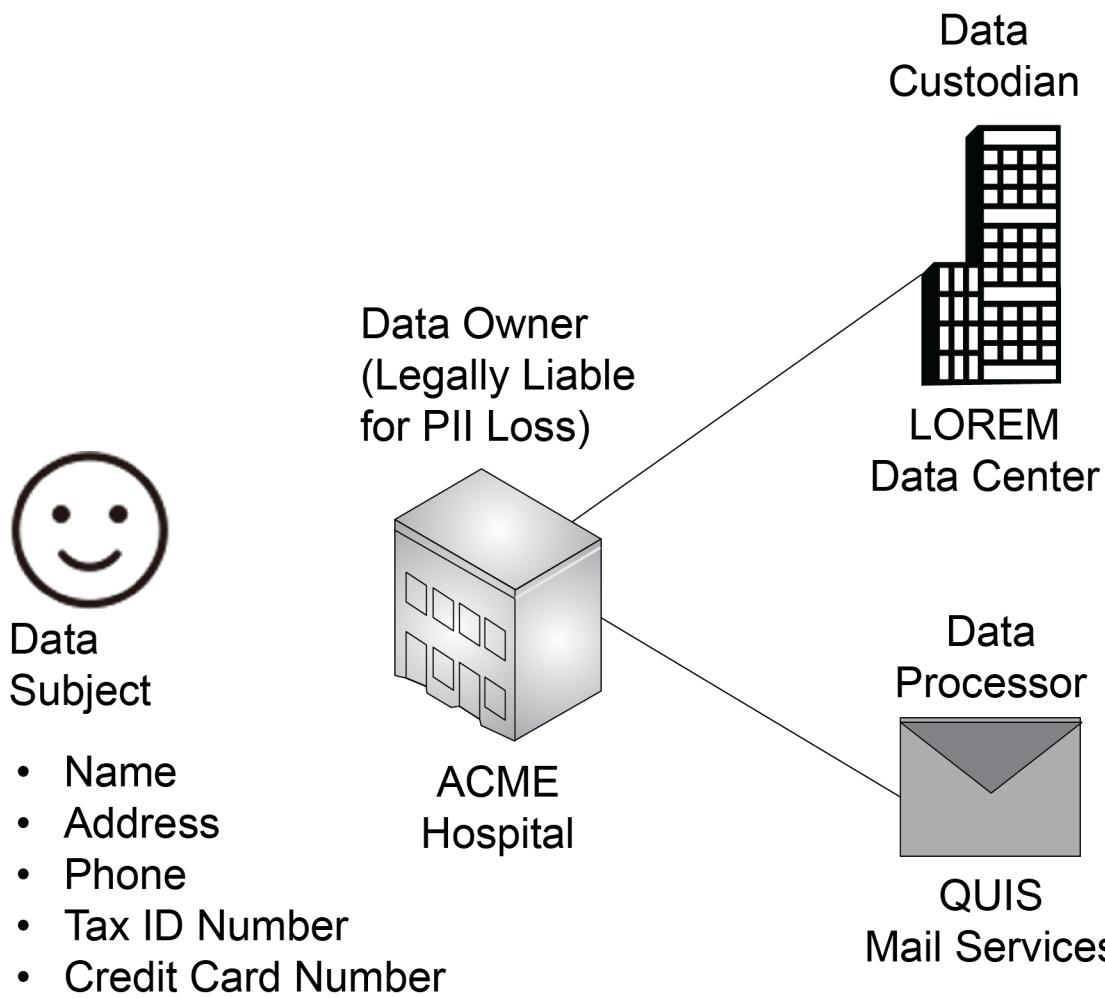
### Select Quiz

Quiz 1

[SHOW QUIZ DETAILS](#) ▾

START

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



**Practice Resources** SHARE FEEDBACK ▾

DASHBOARD > CHAPTER 2

**Compliance, Regulation, and Investigations**

**Summary**

This chapter covered compliance, regulation, investigations, and the importance of protecting a user's private information, such as their name, address, phone, and tax identification number. If such information is stolen during a breach, it exposes the individual to identification theft, which could cost them thousands of dollars in losses and inconvenience.

Laws and regulations are in place to protect citizens by making companies and businesses responsible for these losses, and information security professionals must be aware of the various laws and requirements. Some requirements come from contractual agreements such as PCI DSS, which requires businesses not to save the CVV code on the back of credit cards.

Federal institutions must abide by FISMA, stating that information security mitigations should be put in place to protect privacy records. ISO 27001 is an industry standard that provides similar requirements for businesses.

Companies doing business overseas may have to consider the GDPR, and medical institutions must follow HIPAA requirements to protect an individual's health records.

The chapter concluded by detailing the different investigation types and privacy terminology. The next chapter will cover how standards, procedures, and guidelines are developed from security policies created by management.

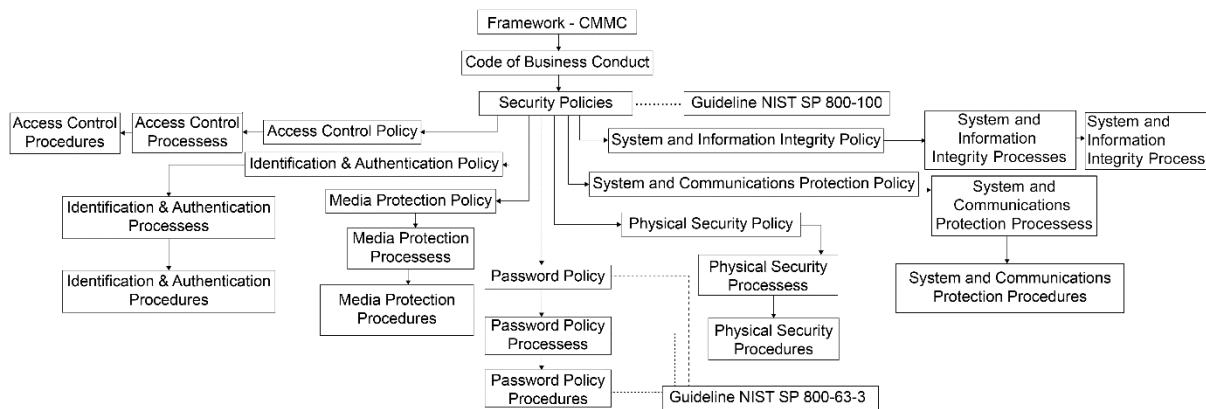
**Chapter Review Questions**

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 3: Security Policies and Business Continuity



Business Process	Potential Impacts	Max Tolerable Downtime	System Components	Recovery Time Objective
Process Invoice	Operations - more than Application 1,000 staff affected	80 hours	Application Server	40 hours
Prepare Report	Reputation - media outlets announce concerns	30 hours	Web Server	24 hours
Create Budget	Reputation - congressional insight	36 hours	Database Server	12 hours
Respond to Inquiries	Customer Service - over 500 customer complaints	36 hours	Desktop Computers	30 hours

Interdependencies

kp Practice Resources

DASHBOARD > CHAPTER 3
SHARE FEEDBACK
SHARE FEEDBACK

**Security Policies and Business Continuity**

**Summary**

This chapter covered security policies and BC. For security policies, you learned about their purpose, what makes a good policy, the information security policy life cycle, and personnel security policies and procedures. For BC, you looked at how to identify, analyze, and prioritize BC requirements. You reviewed the BIA process/report and its place in the overall BC effort. Lastly, you examined how to build a BCP. The next chapter will cover personnel policies, risk management, threat modeling, supply chain risk management (SCRM), as well as security awareness, education, and training programs.

**Chapter Review Questions**

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

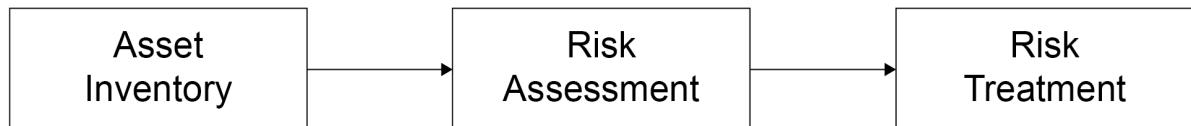
**Select Quiz**

Quiz 1 START

[SHOW QUIZ DETAILS](#)

## Chapter 4: Risk Management, Threat Modeling

$$\text{Threat} + \text{Vulnerability} + \text{Probability of Occurrence} = \text{Exposure}$$



**kp Practice Resources**

DASHBOARD > CHAPTER 4

**Risk Management, Threat Modeling, SCRM, and SETA**

Summary

This chapter concludes the first of the eight domains. Risk management, threat modeling, SCRM, and security awareness, education, and training – commonly referred to as SETA – were discussed in this chapter. For risk management, how to apply risk management concepts was covered. You also examined threat modeling concepts and methodologies, and SCRM concepts. Finally, you explored SETA programs. The next chapter will begin looking at the asset security domain – specifically, asset and privacy protection.

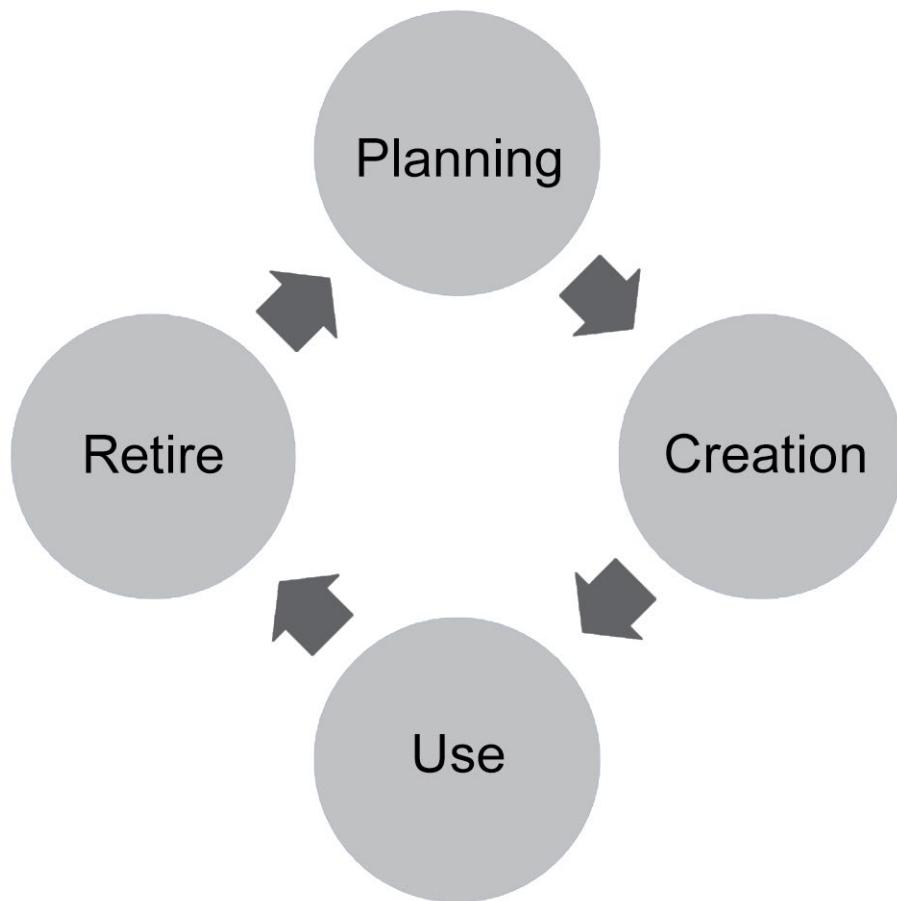
**Chapter Review Questions**

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 5: Asset and Privacy Protection



**Practice Resources**

DASHBOARD > CHAPTER 5

**Asset and Privacy Protection**

**Summary**

In this chapter, you reviewed asset security, specifically the identification and classification of assets and their provisioning and handling. Further, you reviewed the reasons for data and asset classification and the importance of determining asset ownership, as well as the difference between tangible and intangible assets. The next chapter will dig deeper into some of the specifics of asset management, such as data roles, the asset management life cycle, and the determination of appropriate controls for digital assets.

**Chapter Review Questions**

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

**Select Quiz**

Quiz 1 [SHOW QUIZ DETAILS](#) [START](#)

## Chapter 6: Information and Asset Handling

 Practice Resources

DASHBOARD > CHAPTER 6

### Information and Asset Handling

#### Summary

In this chapter, you completed your review of asset security—specifically, how to manage digital assets over the course of their life cycle. You reviewed some of the particulars in the usage and destruction phases of the data life cycle. You learned what information you need to collect and the questions you need to answer to properly oversee digital assets. Additionally, you explored the destruction phase and the criteria for when and how to carry out the destruction of a digital asset. Further, you examined the security controls and compliance requirements that influence how you should manage digital assets during their life cycle. Finally, you reviewed how to control/prevent DLP in traditional environments as well as cloud environments. In the next chapter, you will begin learning about *Domain 3, Security Architecture and Engineering*. Chapter 7 will focus on secure design principles and controls, being the first of three chapters covering *Domain 3*.

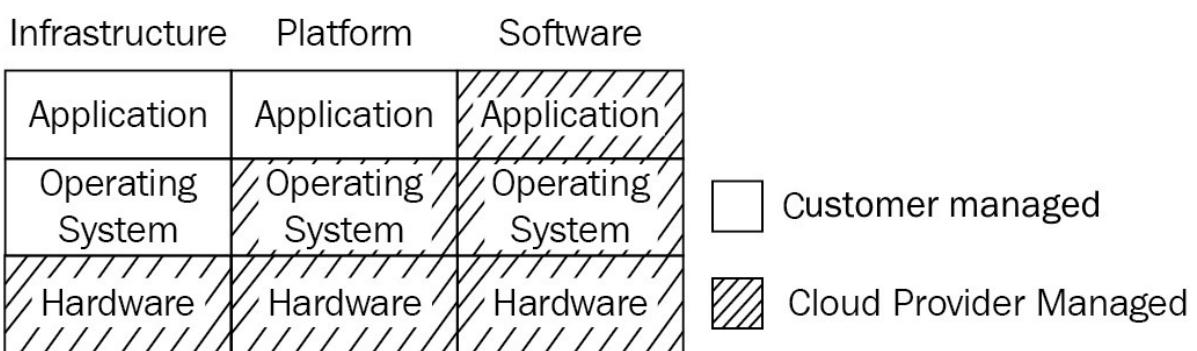
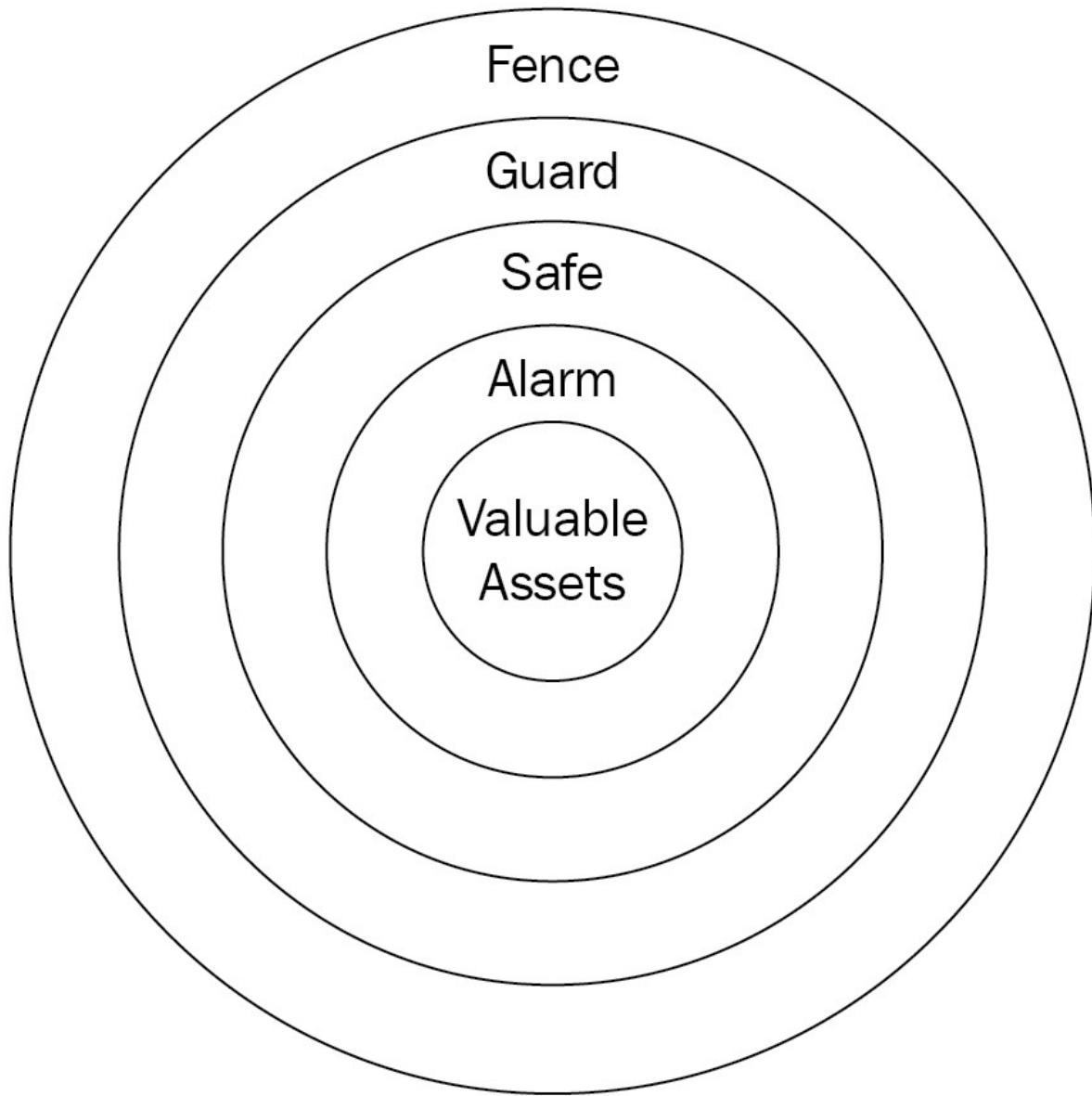
### Chapter Review Questions

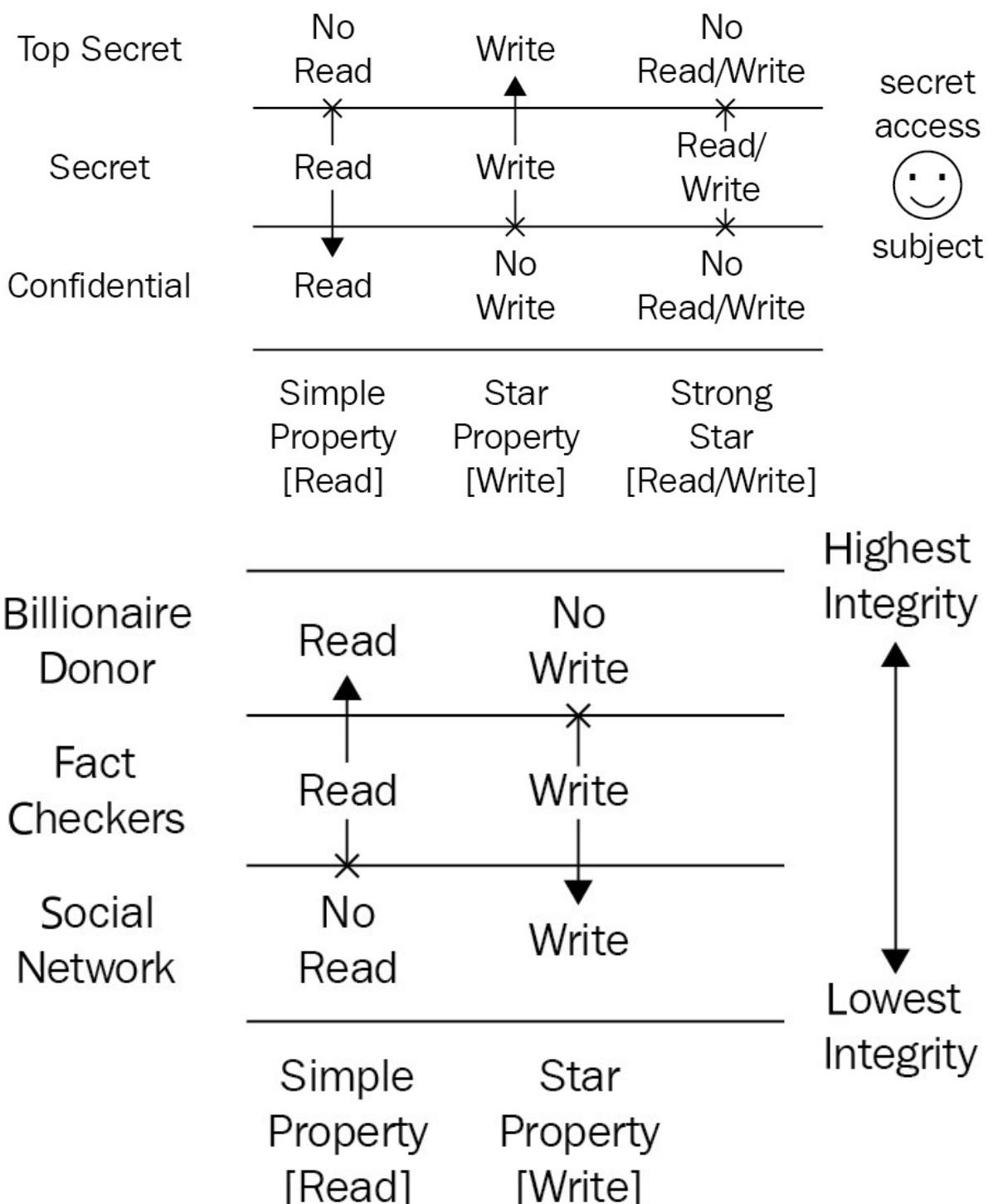
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

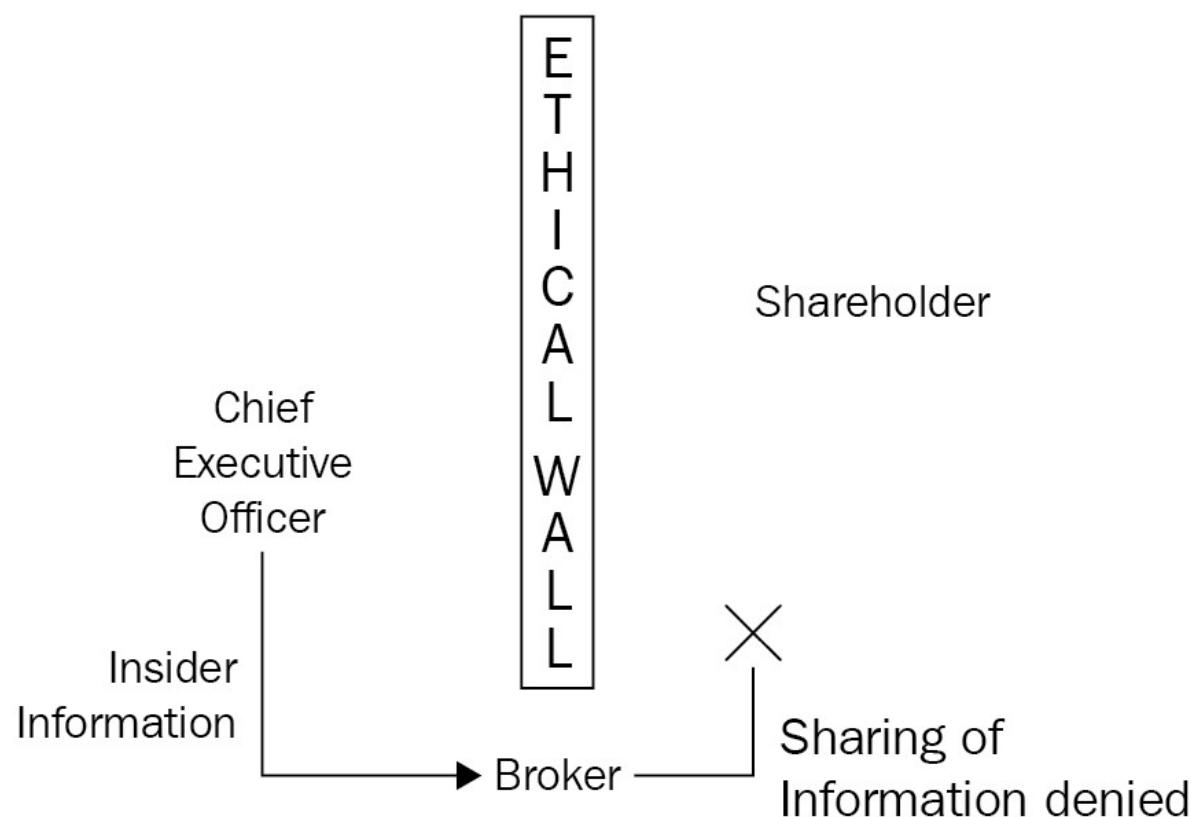
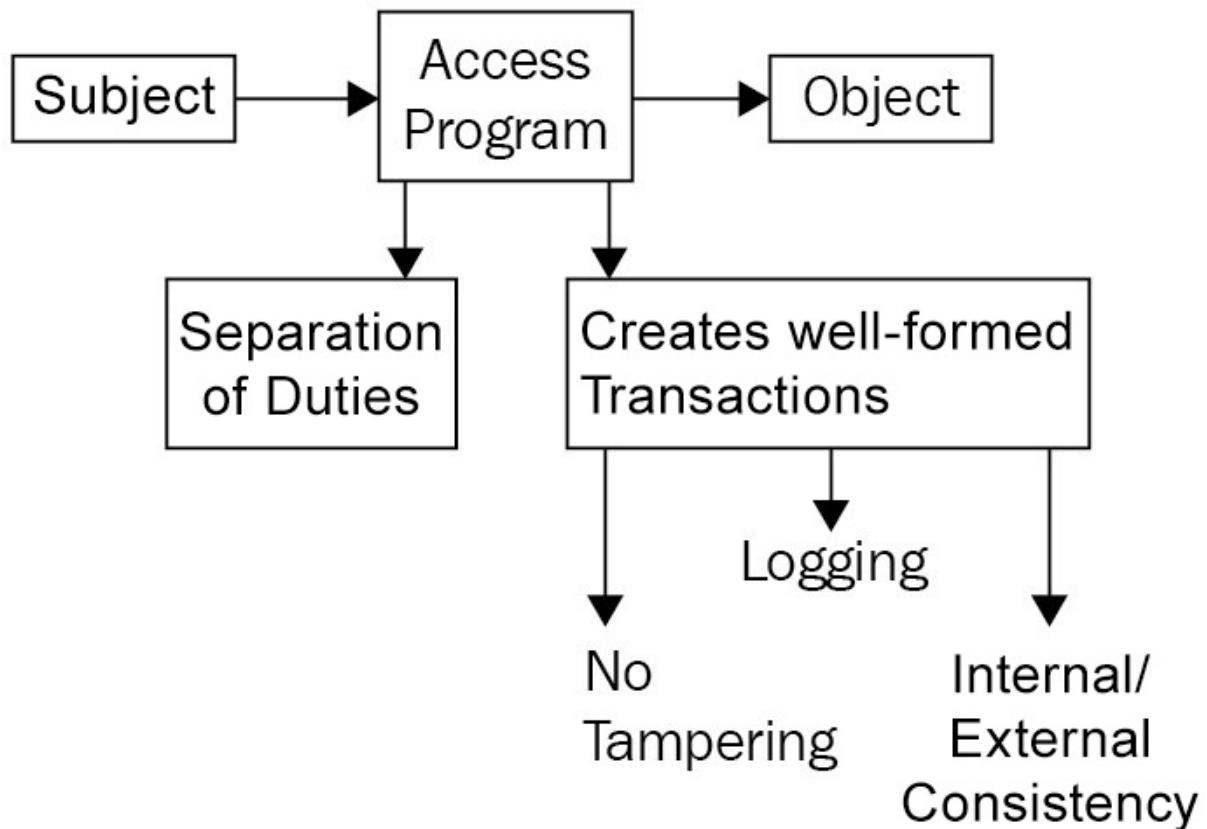
**Select Quiz**

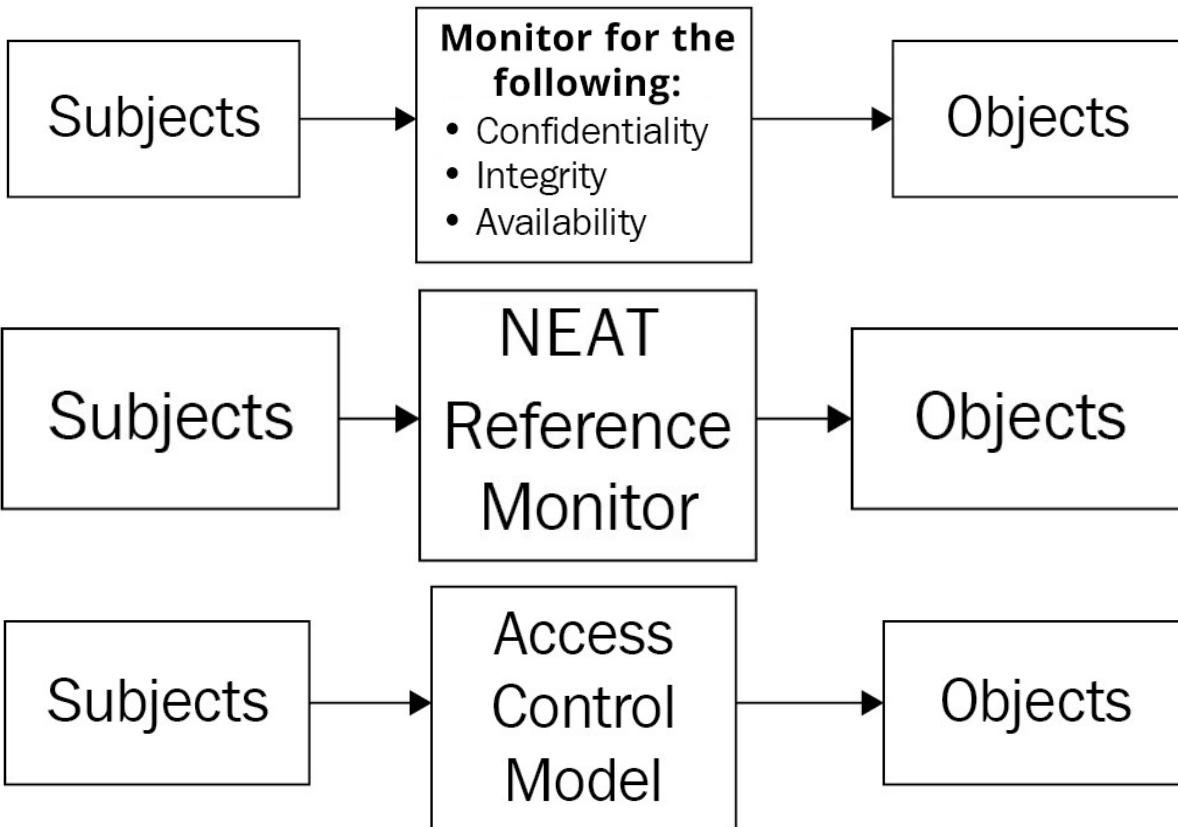
Quiz 1 [SHOW QUIZ DETAILS](#) 

**Chapter 7: Secure Design Principles and Controls**









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

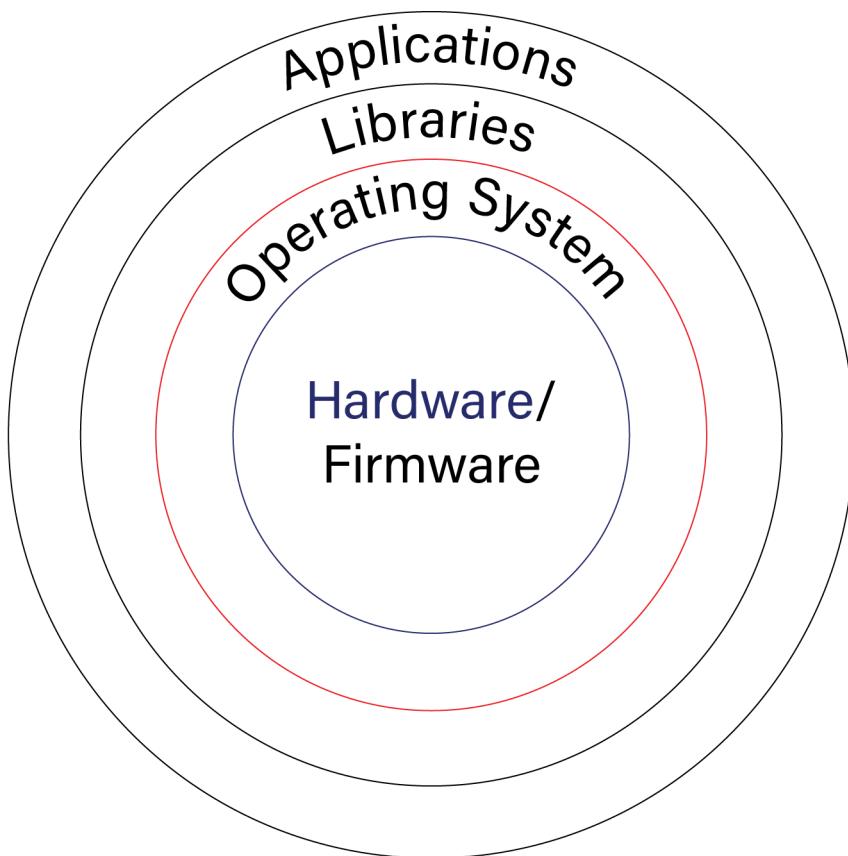
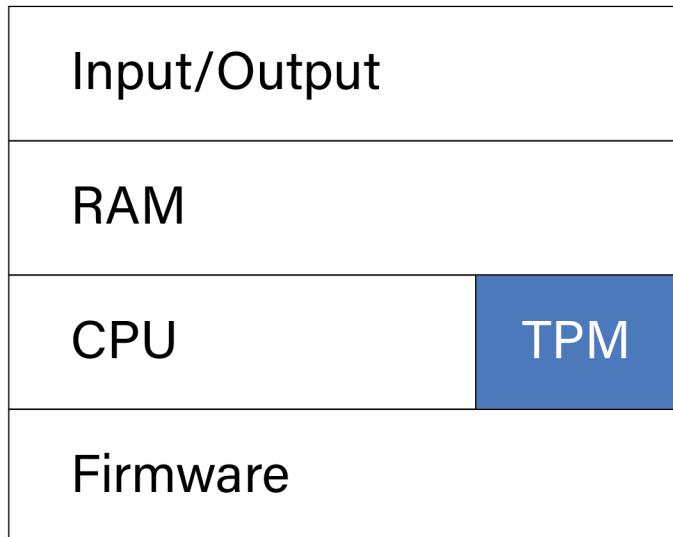
#### Select Quiz

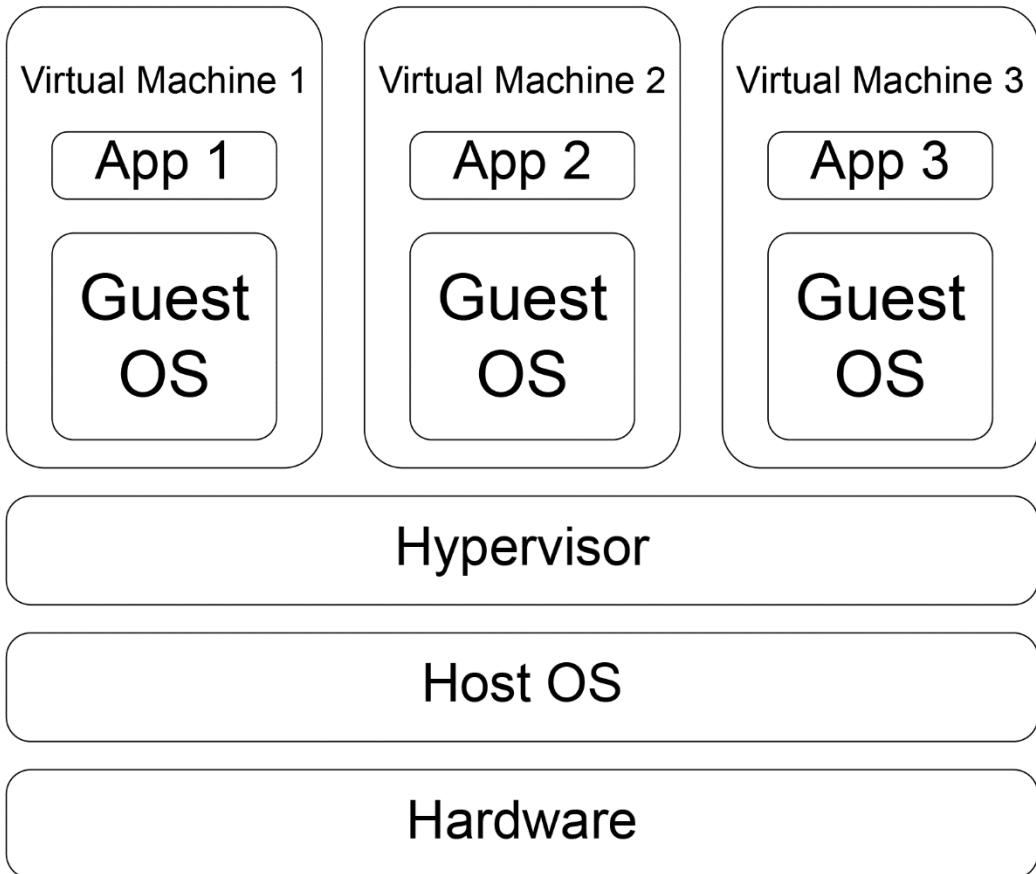
Quiz 1

[SHOW QUIZ DETAILS ▾](#)

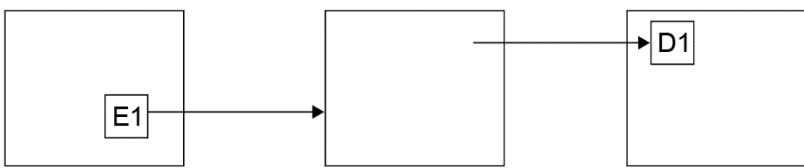
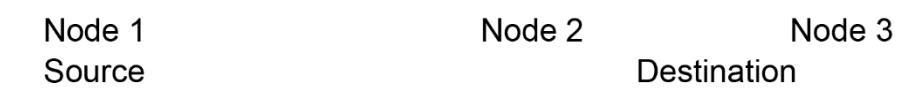
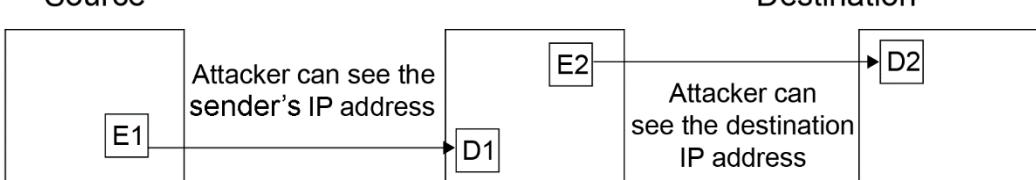
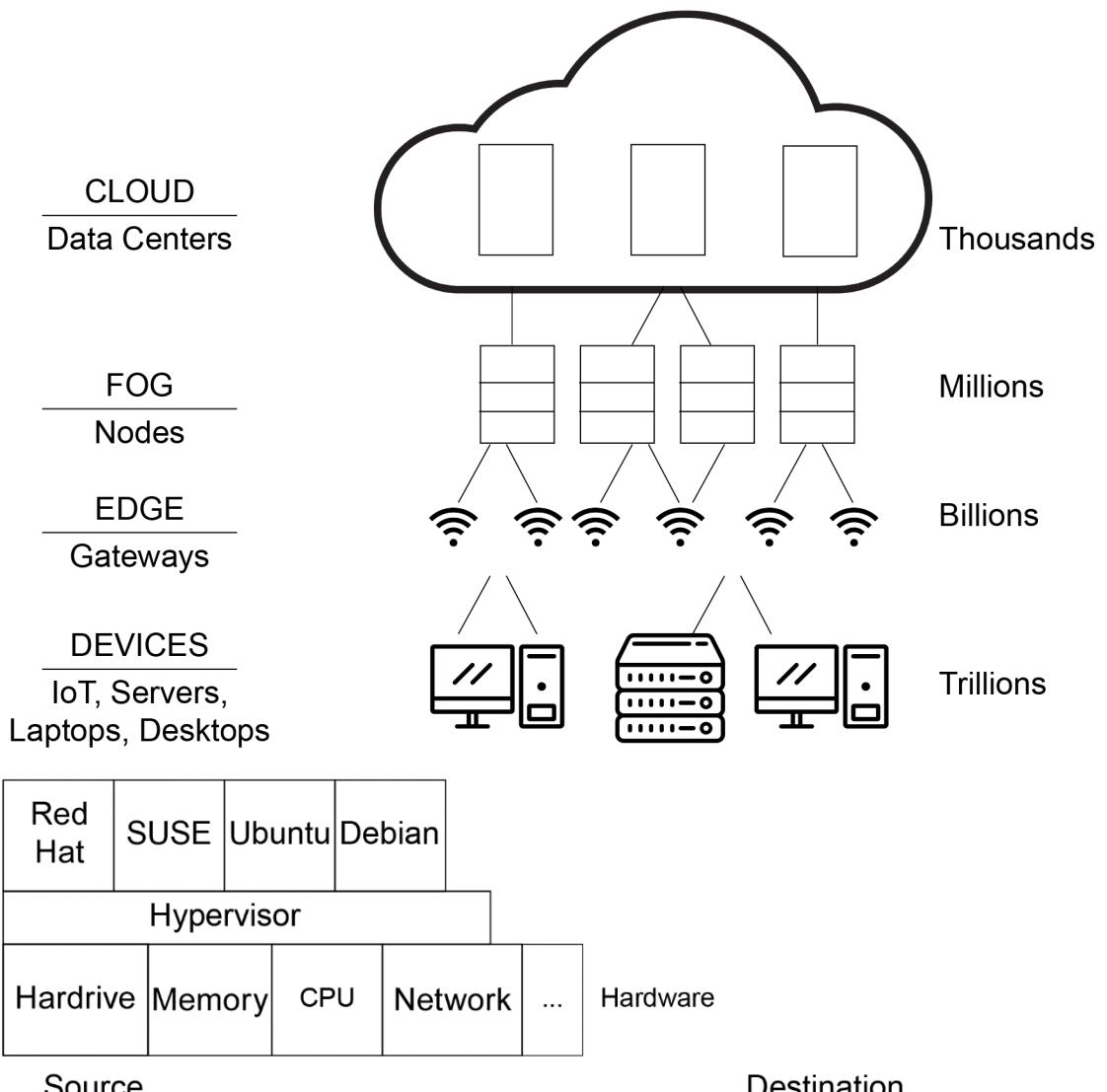
START

**Chapter 8: Architecture Vulnerabilities and Cryptography**





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



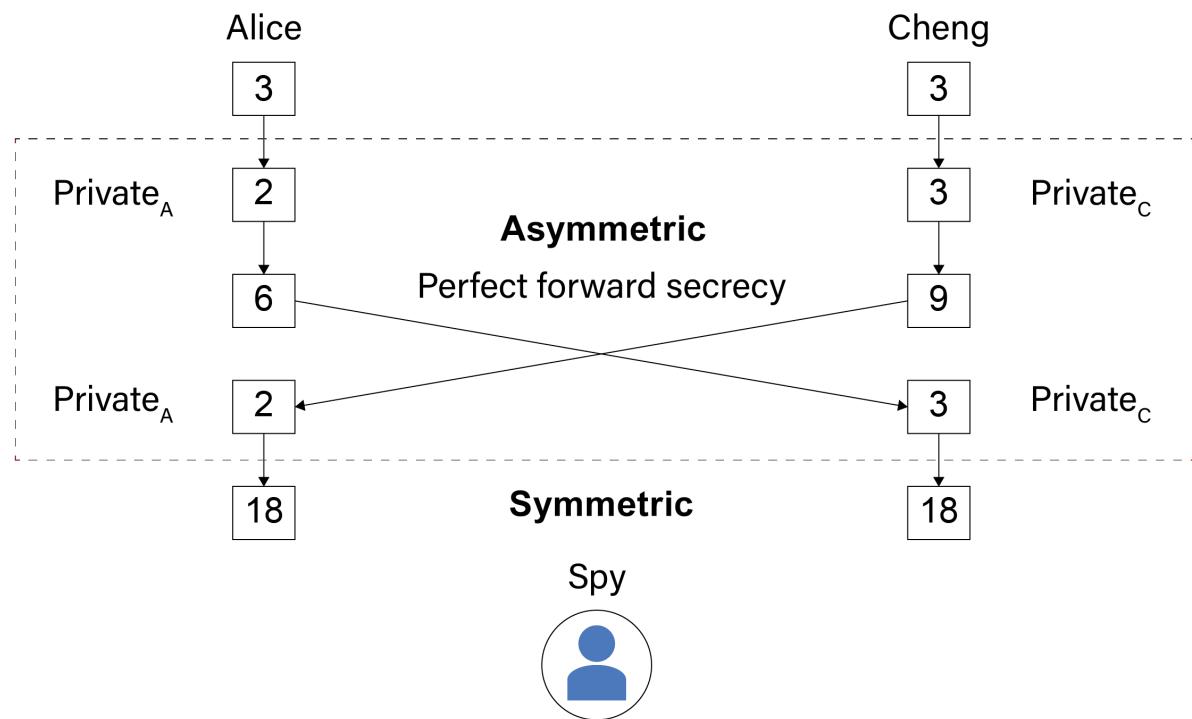
Original image



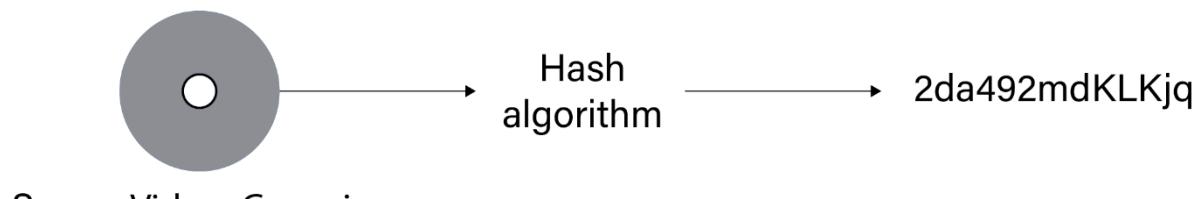
Original image plus hidden data

	<b>Sender has</b> 	<b>Recipient has</b> 
 <b>Signing</b>	 Sender private key	 Sender public key
 <b>Encrypting</b>	 Recipient public key	 Recipient private key

## Diffie - Hellman



s



Super\_Video\_Game.iso

## Client Server

3. The client verifies the SSL certificate information



1. Client sends hello, cipher suite, client random
2. Server respond back by sending the server random and SSL certificate (private key)
4. Pre-master key generated using the public key
6. Pre-master key decrypted 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

## SSL Server

5. The server verifies the client certificate (if required)



 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

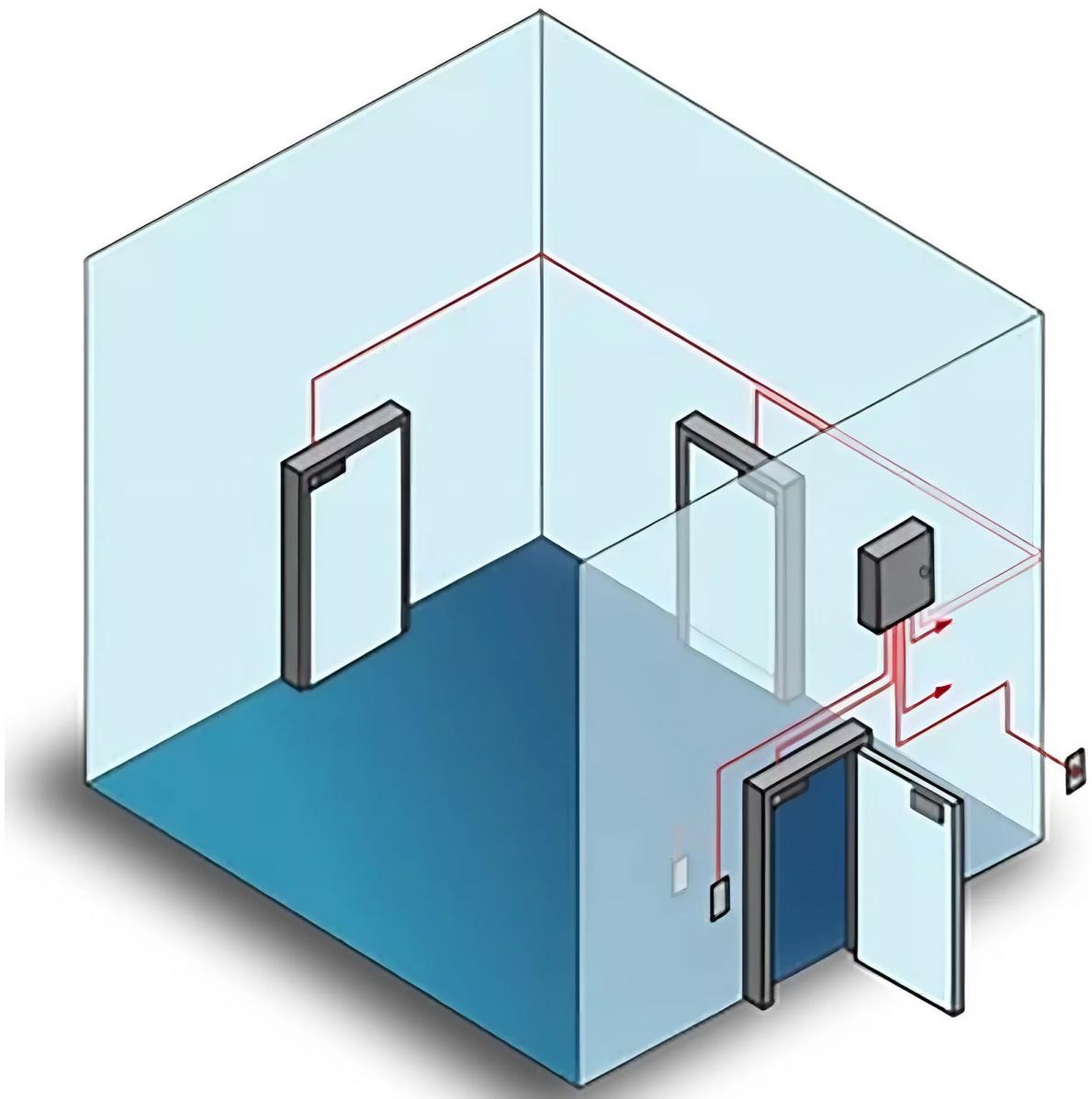
[SHOW QUIZ DETAILS](#) ▾

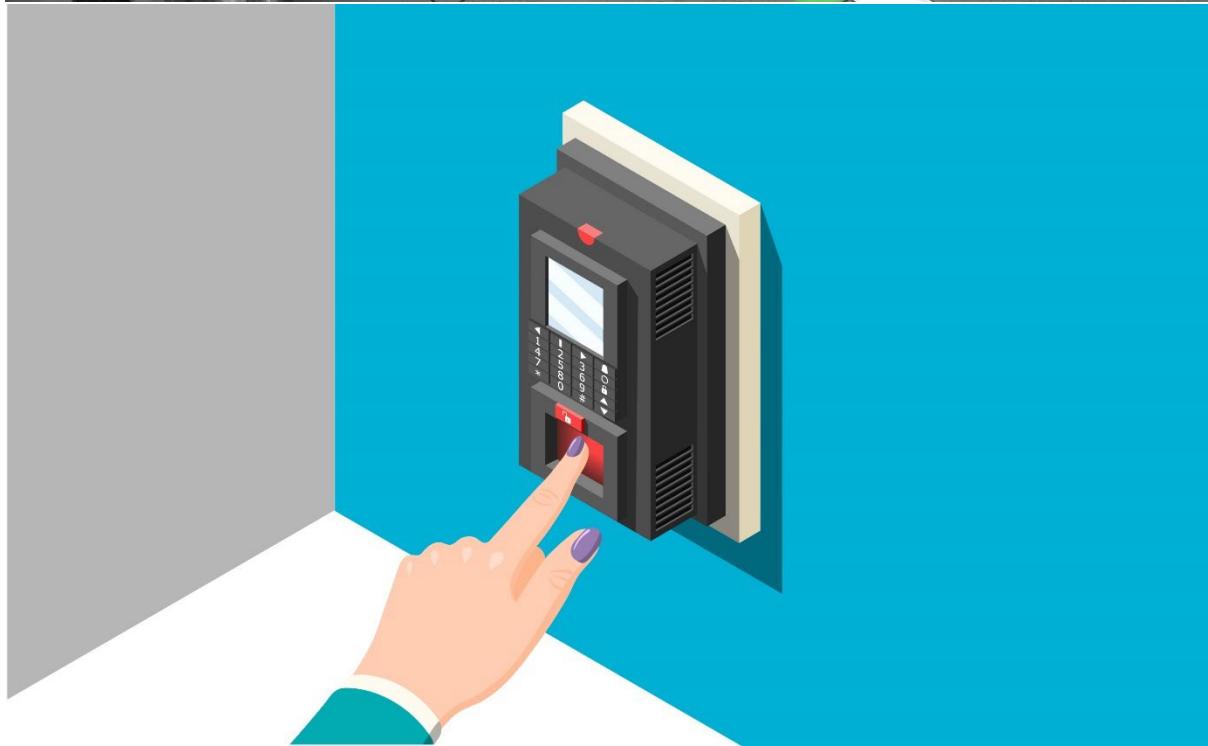
START

## **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

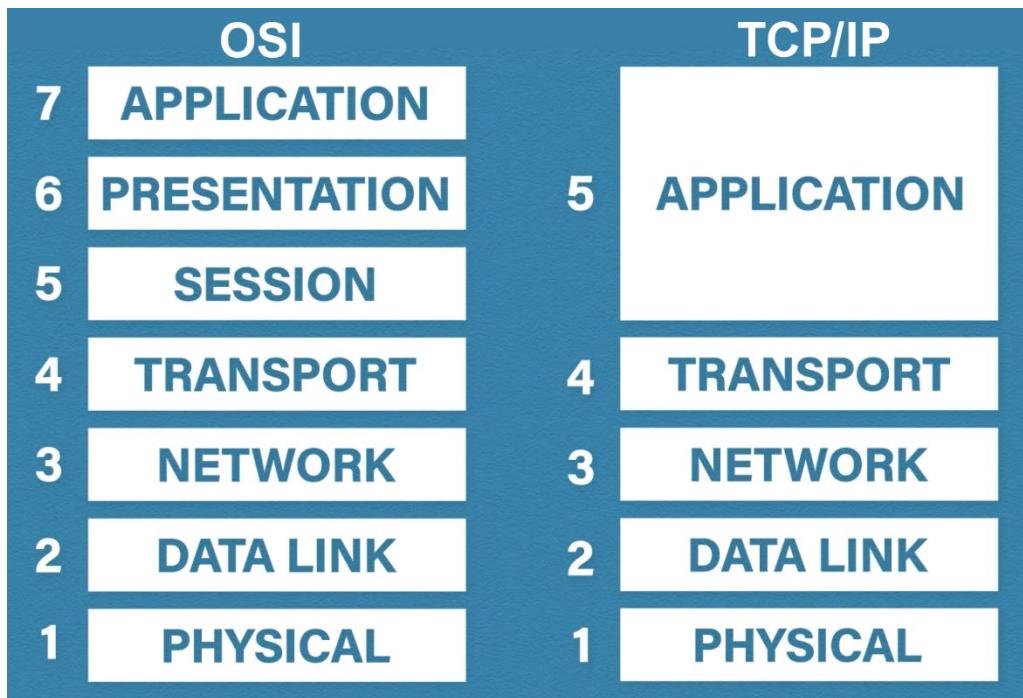
### Select Quiz

Quiz 1

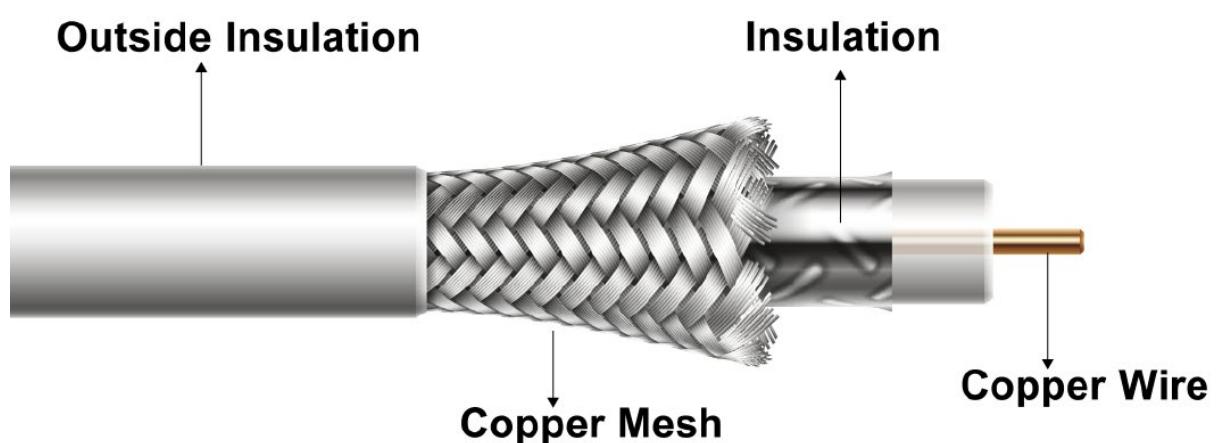
[SHOW QUIZ DETAILS](#) ▾

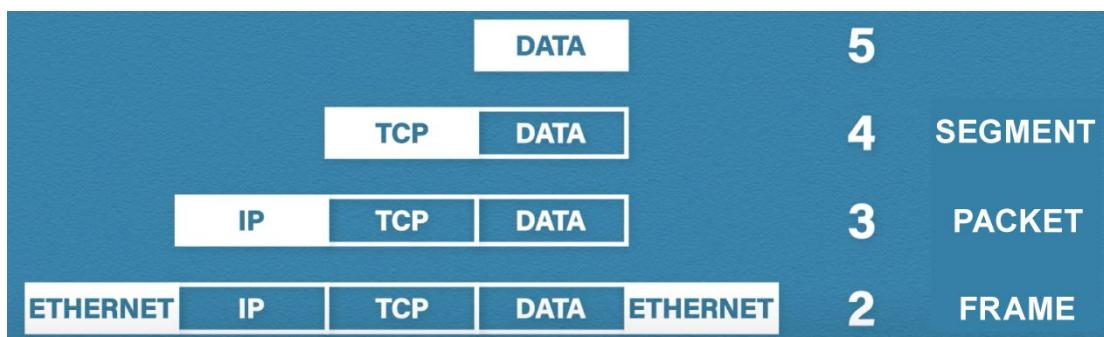
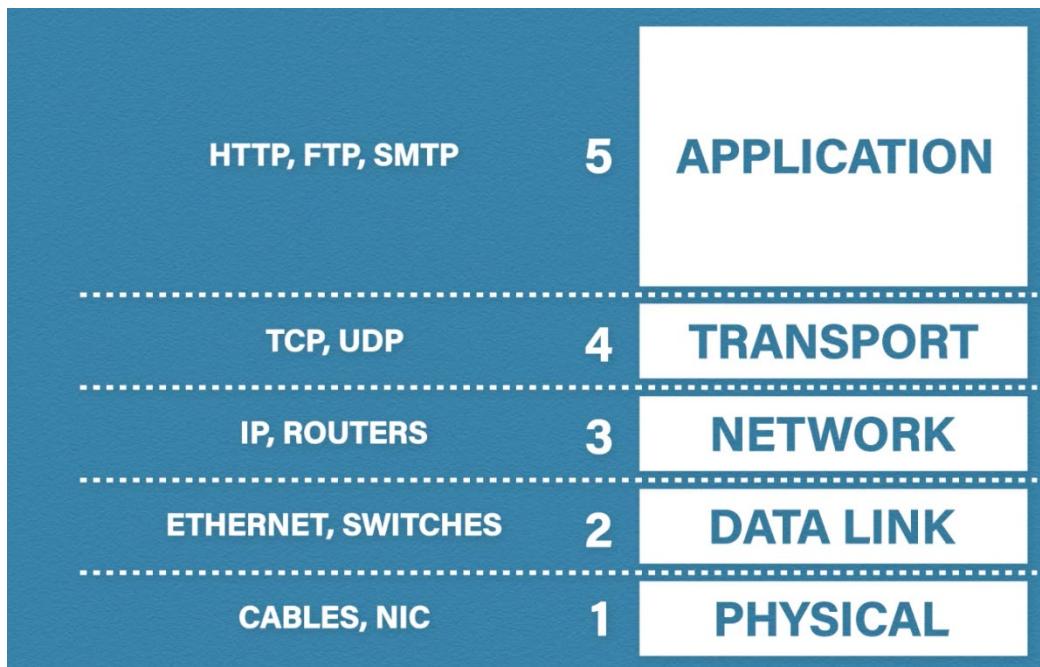
START

**Chapter 10: Network Architecture Security**



## Coaxial cable





**cp Practice Resources**

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.

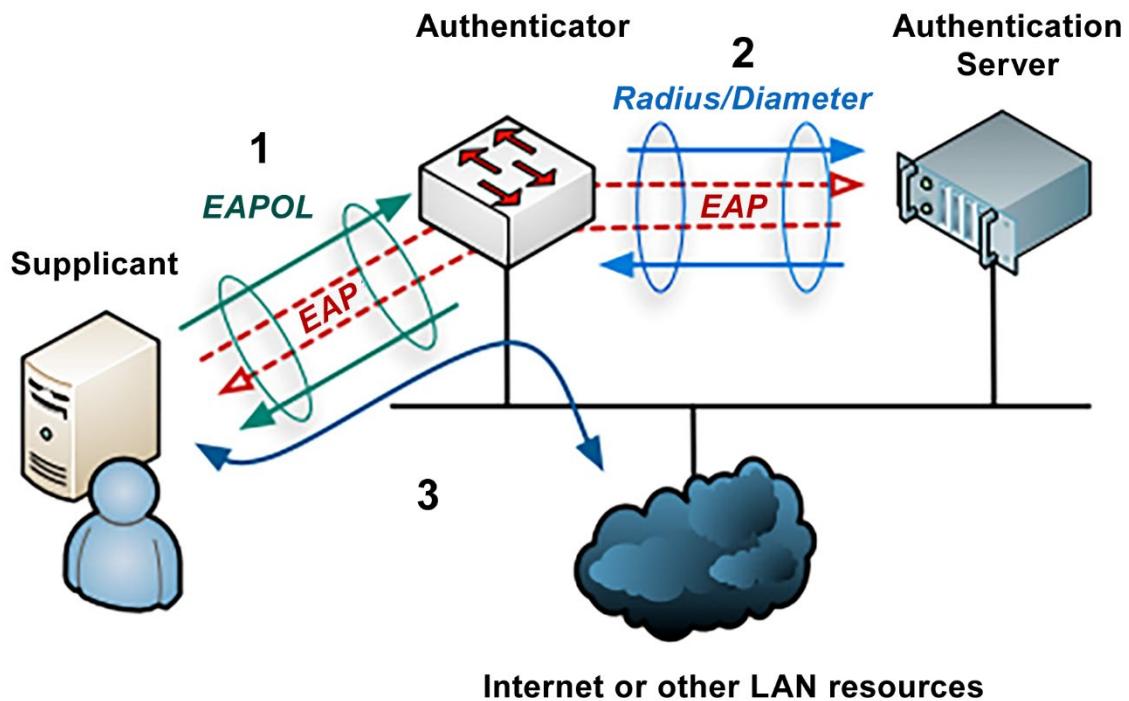
**Chapter Review Questions**

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

**Select Quiz**

Quiz 1      SHOW QUIZ DETAILS ▾      START

## Chapter 11: Securing Communication Channels



**kp 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 communication 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

```
Activities Terminal Thu 15:31
student@debian: ~
File Edit View Search Terminal Help
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
apt:x:104:65534::/nonexistent:/bin/false
rtkit:x:105:110:RealtimeKit,,,:/proc:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:107:111:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
geoclue:x:110:116::/var/lib/geoclue:/bin/false
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
:
```





## kp Practice Resources

[SHARE FEEDBACK](#)[DASHBOARD](#) > [CHAPTER 12](#)

### 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 CISO 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

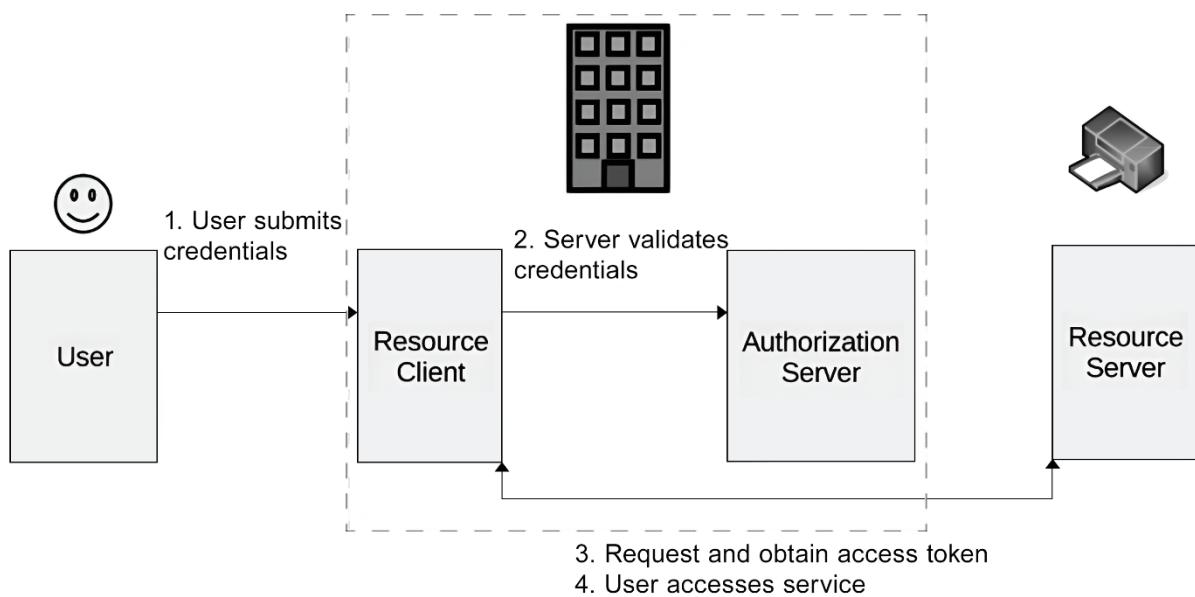
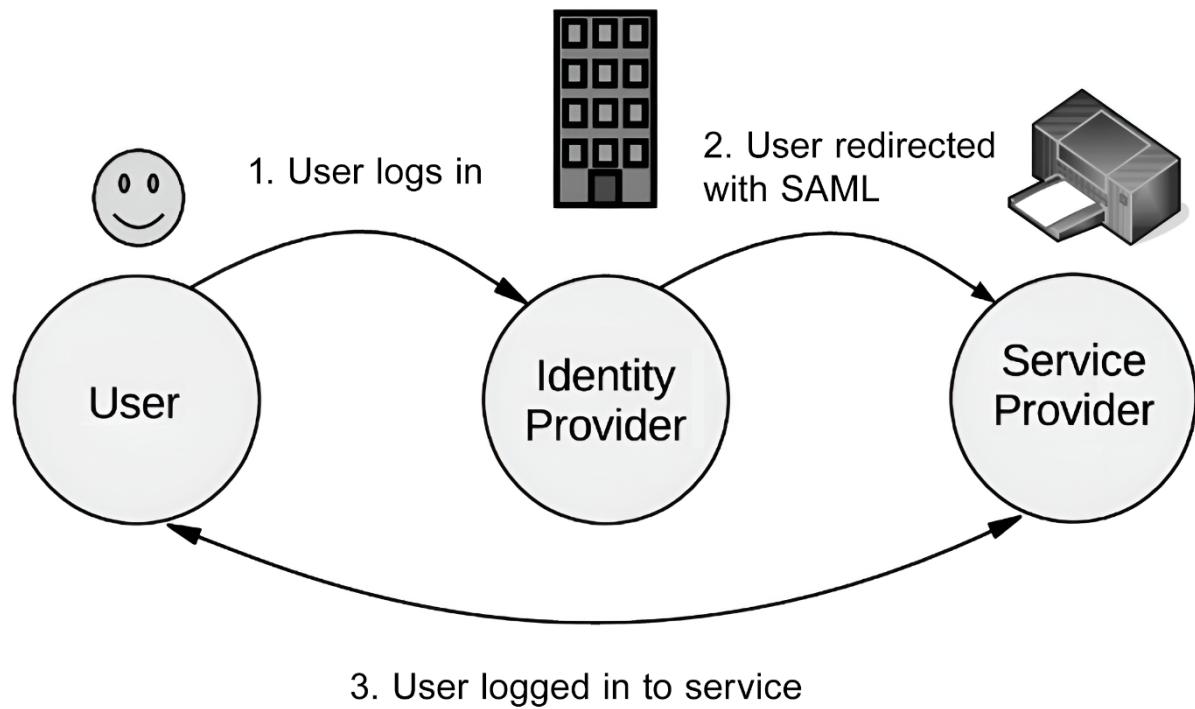
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Heftema

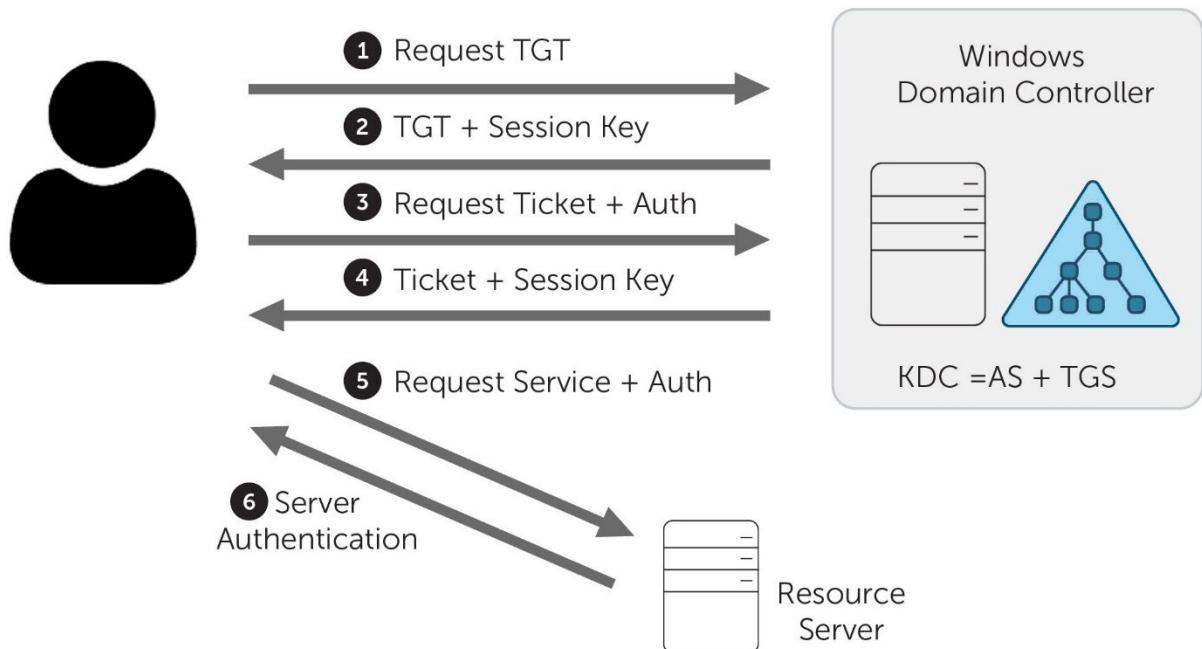
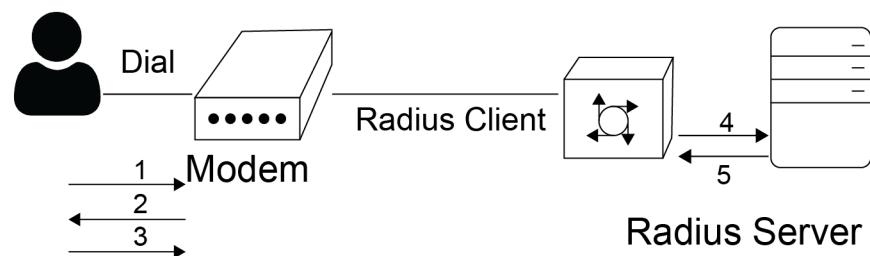
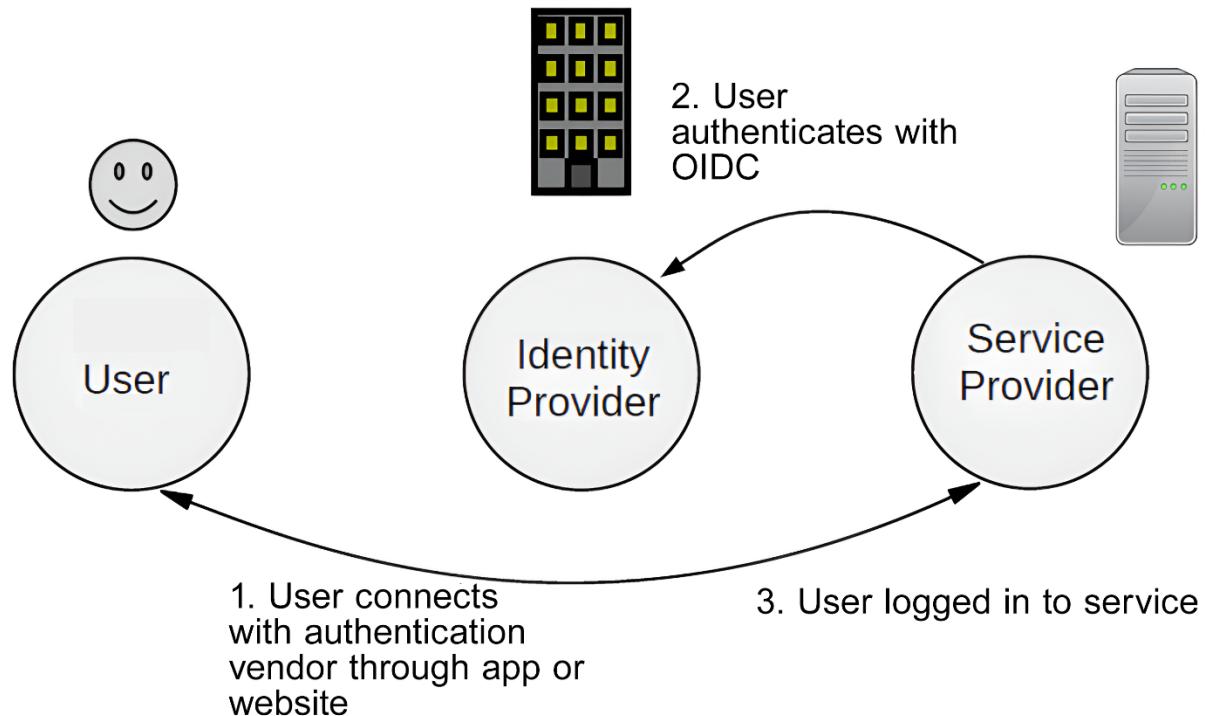
#### Select Quiz

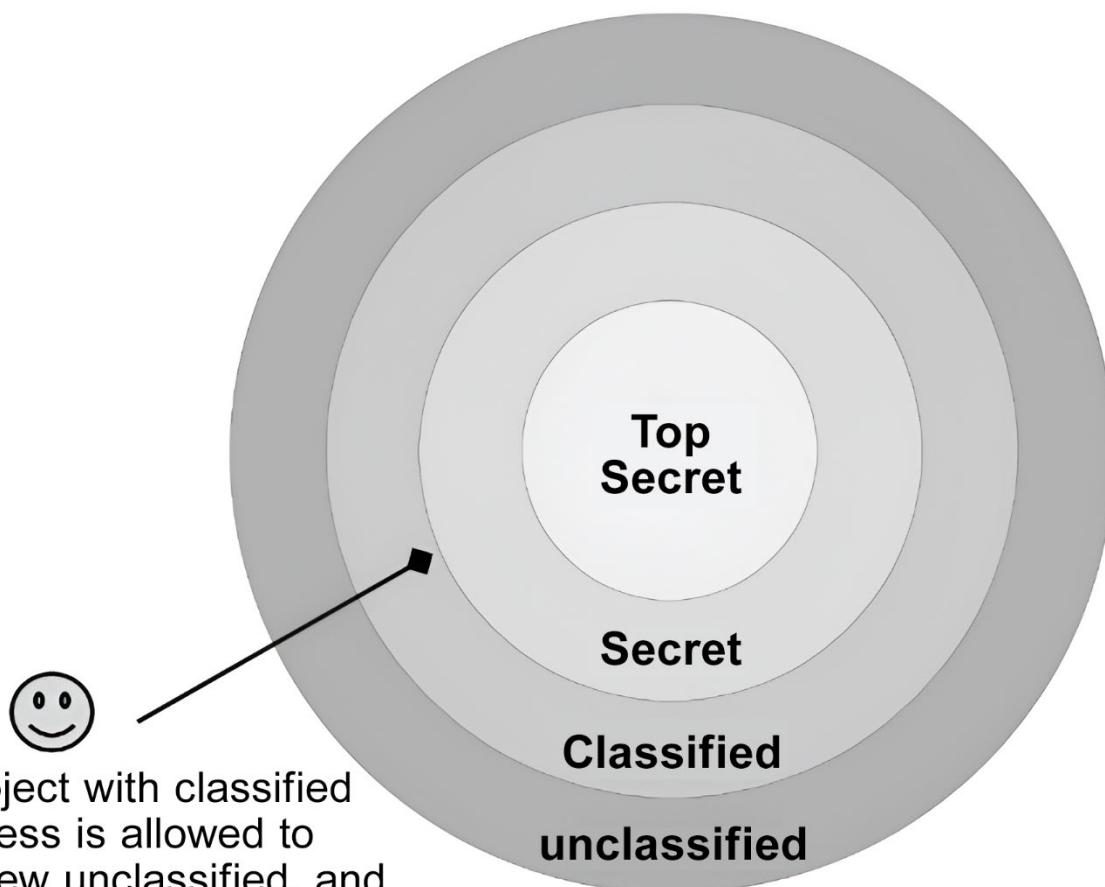
Quiz 1

[SHOW QUIZ DETAILS](#)[START](#)

Chapter 13: *Identity Management Implementation*







 Practice Resources

DASHBOARD > CHAPTER 13

SHARE FEEDBACK 

## 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, Hime Heffema

### Select Quiz

Quiz 1  

## Chapter 14: Designing and Conducting Security Assessments

The screenshot shows a dark-themed user interface for 'Practice Resources'. At the top left is the 'Practice Resources' logo. On the right are a bell icon and a 'SHARE FEEDBACK' button with a dropdown arrow. Below the header, a breadcrumb navigation shows 'DASHBOARD > CHAPTER 14'. The main content area has a title 'Designing and Conducting Security Assessments' and a 'Summary' section. The summary text discusses the importance of security control testing for ensuring system integrity and identifies key components like risk understanding, testing methodology, and plan adaptation. To the right, a sidebar titled 'Chapter Review Questions' lists the book 'The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema'. It features a 'Select Quiz' section with 'Quiz 1' and a 'START' button, along with a 'SHOW QUIZ DETAILS' link.

DASHBOARD > CHAPTER 14

### Designing and Conducting Security Assessments

#### Summary

In this chapter, we covered how effective assessment, test, and audit strategies are essential for ensuring the security and integrity of any organization's systems and data. Regular security control testing is a critical component of any security program and enables organizations to validate that security controls are working as intended and to detect any vulnerabilities that need to be addressed.

To conduct security control testing effectively, organizations must have a comprehensive understanding of their security risks and a robust testing methodology. This includes identifying the types of security controls to be tested, selecting appropriate testing techniques, and defining test objectives and success criteria. Organizations should also have a plan for addressing any issues or vulnerabilities that are identified during testing and should be prepared to adapt their security controls and procedures as needed.

Assessment, test, and audit strategies are crucial for maintaining a strong security posture, and regular vulnerability scans, penetration testing, and log analysis are essential parts of this. By implementing effective compliance strategies, organizations can ensure that their systems and data remain secure and protected from potential threats. The next chapter will look at designing and conducting security testing.

### 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 15: Designing and Conducting Security Testing

 Practice Resources



SHARE FEEDBACK ▾

DASHBOARD > CHAPTER 15

### Design and Conduct Security Testing

#### Summary

This chapter covered the process of collecting security data during a security assessment. Planning your assessment and getting the right data is key, as well as ensuring that your organization follows security processes and that they're verified and validated. This planning should be done systematically with the full involvement of management. The important parts of this assessment include ensuring that the right people have the right accounts with the right permissions, as well as checking for any accounts that are orphaned or not in use. Also important is checking that training is effective, with gamification such as phishing attacks, as well as ensuring that backups are done properly. Key performance and risk indicators provide a way to ensure that we're properly following our audit plan.

KPIs are also important in disaster recovery and business continuity, giving data on an organization's and department's tolerance for downtime and data loss, as well as targets for recovery. We looked at the differences between RPO, RTO, WRT, and MTD and why these are critical metrics if there is a major incident, such as a flood or earthquake.

Finally, the chapter discussed post-audit procedures, including remediation, and the differences between internal, external, and third-party audits. You saw what to do when exceptions were raised in the process of auditing. We emphasized the importance of addressing high-impact vulnerabilities and ensuring that audit recommendations are implemented. The next chapter, Planning for Security Operations, will cover what needs to be done to prepare for security incidents, and subsequent investigations.

### Chapter Review Questions

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

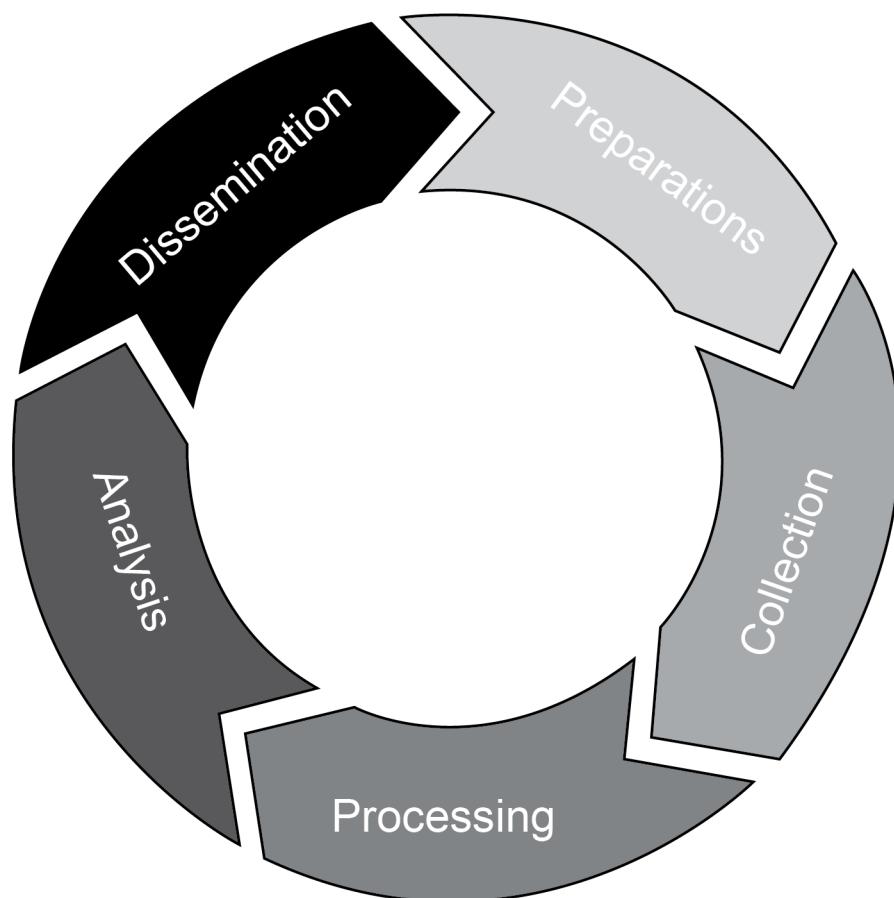
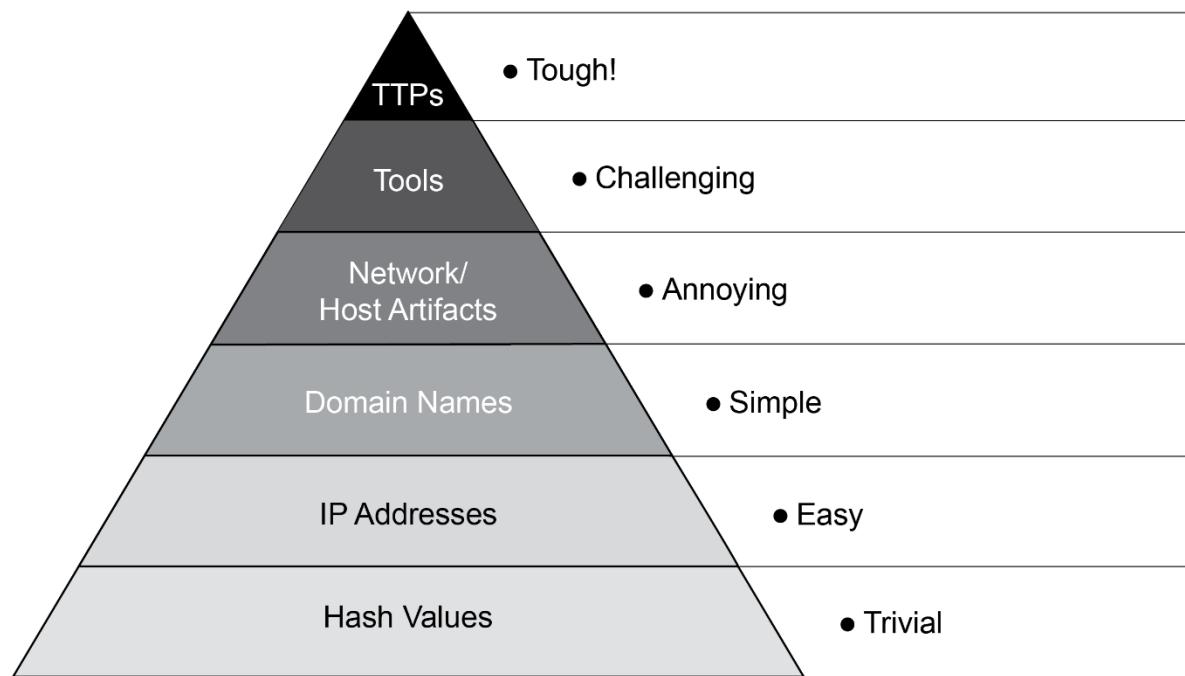
#### Select Quiz

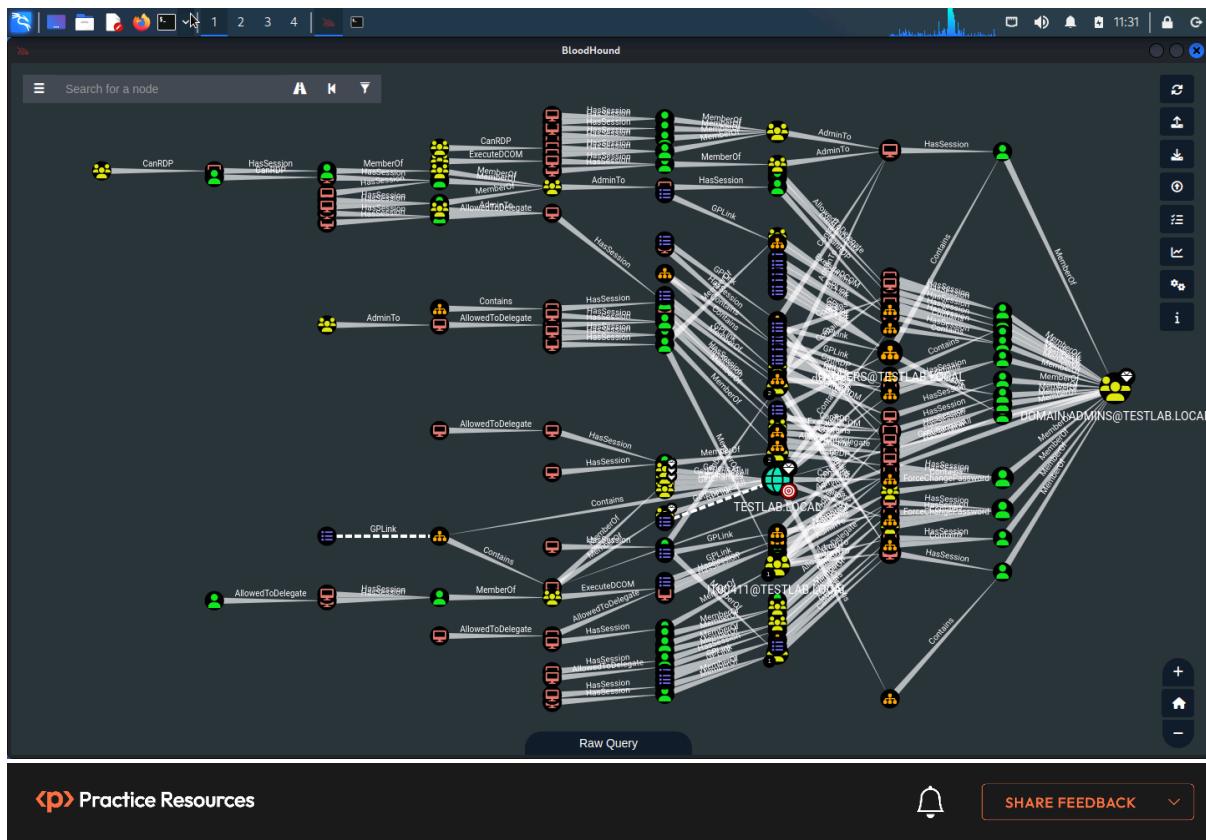
Quiz 1

[SHOW QUIZ DETAILS ▾](#)

START

**Chapter 16: Planning for Security Operations**





**< p Practice Resources**



**SHARE FEEDBACK**

DASHBOARD > CHAPTER 16

## 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

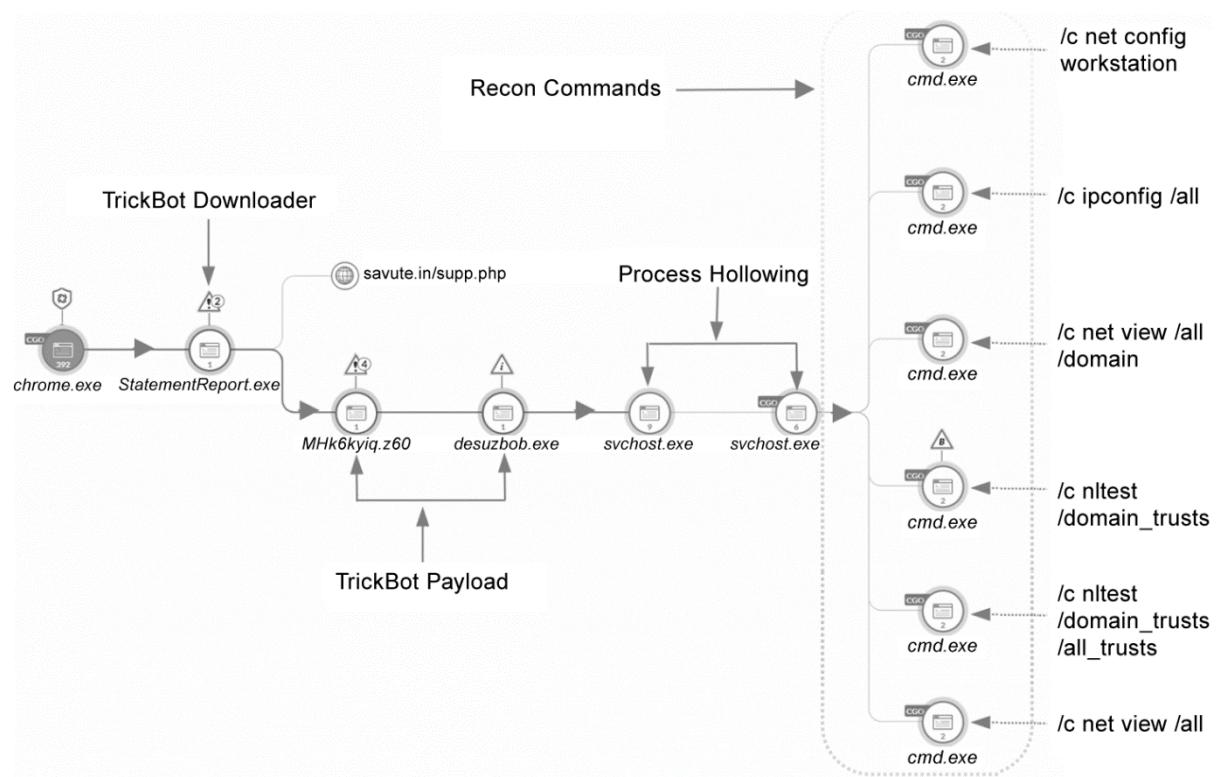
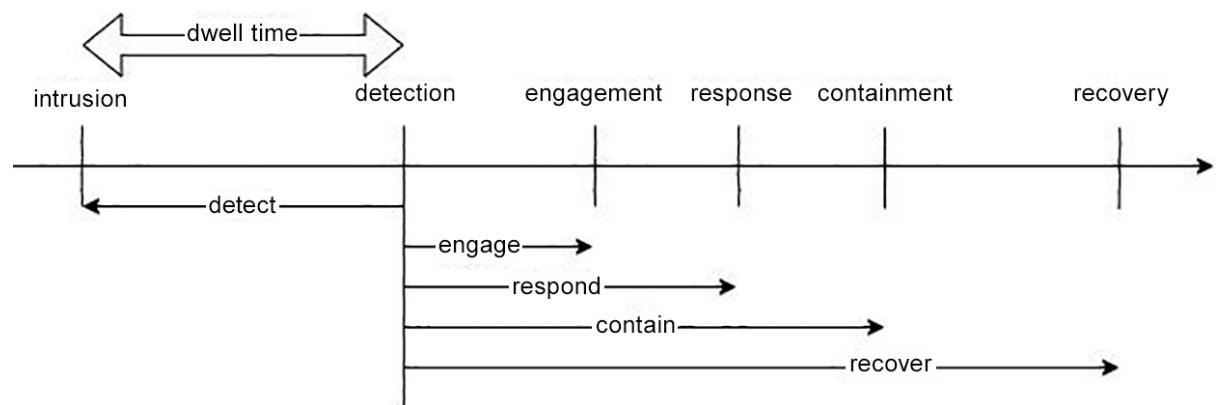
### Select Quiz

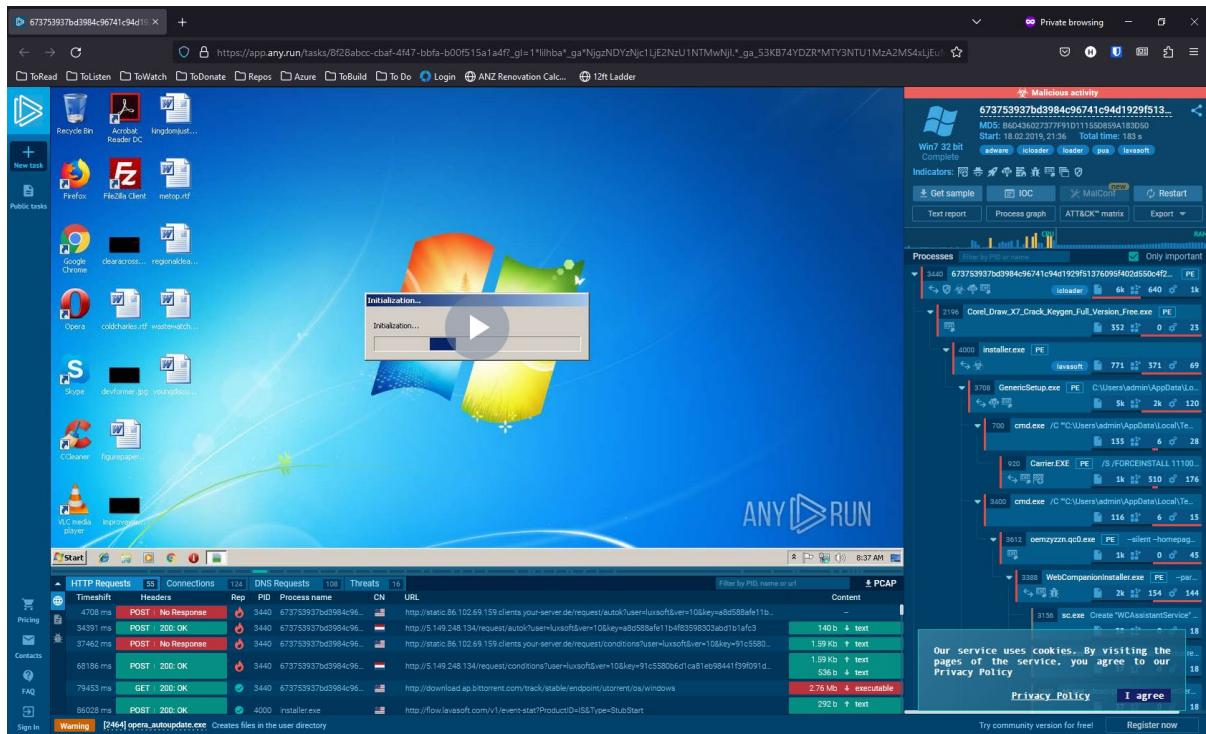
Quiz 1

[SHOW QUIZ DETAILS](#) ▾

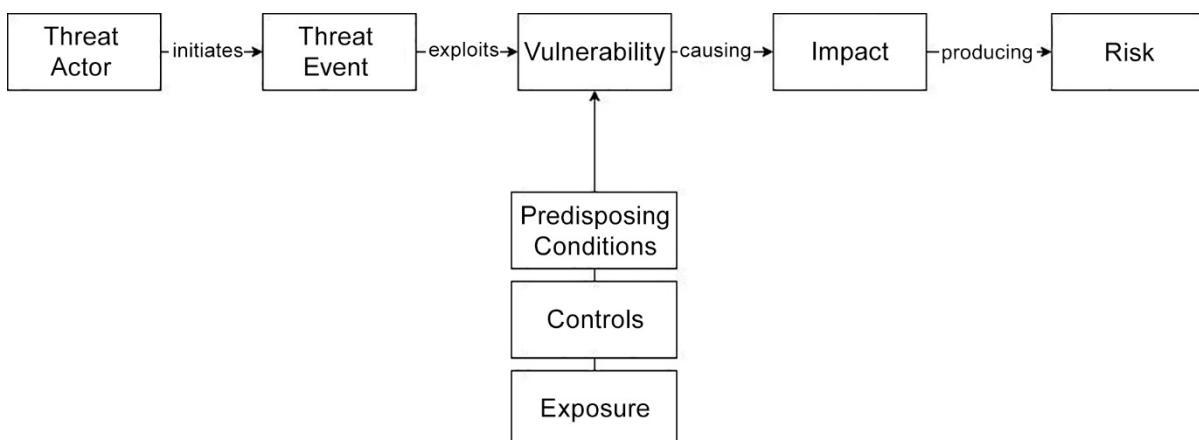
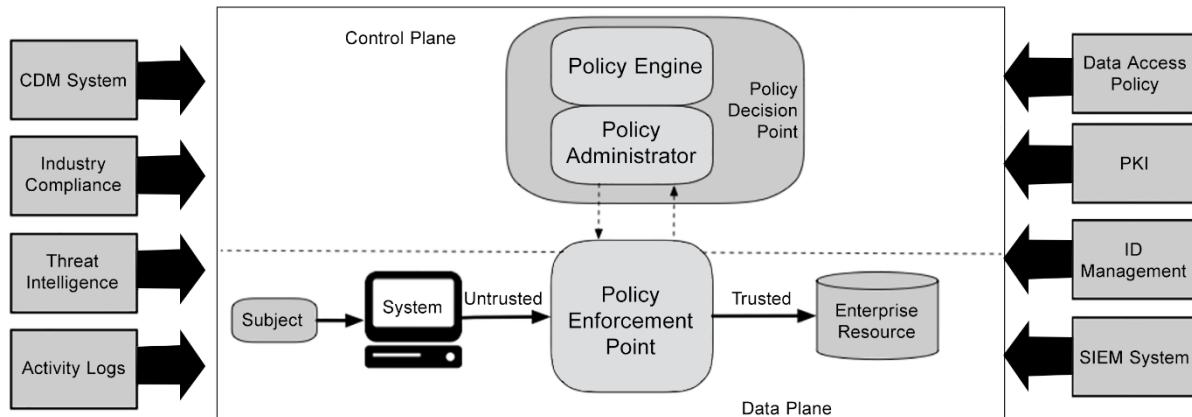
**START**

## Chapter 17: Security Operations





S





## 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 Heftema

### Select Quiz

Quiz 1

[SHOW QUIZ DETAILS](#) ▾

START

## Chapter 18: Disaster Recovery

**kp Practice Resources**

DASHBOARD > CHAPTER 18

### Disaster Recovery

#### Summary

This chapter discussed the important aspects to consider when designing and implementing disaster recovery. Disaster recovery is usually run by the operations side of the business, not by security. However, availability is one of the components of the Confidentiality, Integrity, and Availability (CIA) triad, as well as the increasing prevalence of ransomware, leading to security being involved in the design and principles of disaster recovery planning in business.

You looked at the various approaches that organizations can take to implement disaster recovery, their advantages and disadvantages, and the operative principles that help an organization decide which approach is suitable for a given scenario and risk tolerance. You also saw how these approaches are carried out and documented, but it is also important that plans are tested to ensure that they will work as well as possible during an incident.

The topic of disaster recovery and resilience is large and depends critically on an interplay between processes and available technologies. There are also many technical options available to deliver resilience and disaster recovery capabilities. When studying for the exam, a good strategy is to consider which of these are currently in use in the place where you work, and how they work together to deliver an overall approach to resiliency and disaster recovery. A lot of this process depends on the context of the business that you are in, and what constitutes a *disaster* or *failure* in that context.

The next chapter will discuss business continuity, and some aspects of personnel and physical security that you need to be aware of.

**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 19: Business Continuity

 Practice Resources

DASHBOARD > CHAPTER 19

### Business Continuity, Personnel, and Physical Security

#### Summary

This chapter addressed some areas of physical and safety that affect the operation of cyber security teams such as business continuity, personnel safety, and the resilience of security monitoring systems, as well as the security aspects of systems used in protecting physical security.

Most of these topics involve developing and maintaining contact with various areas of the business outside of IT: finance, human resources, corporate travel, and physical security.

The topics of business continuity, physical safety, and travel often involve a very specific context, such as what the line of business of the organization is, what its legal obligations are, whether it owns or leases buildings, or how much data it is prepared to lose. For this reason, it is hard to come up with best-practice solutions to these items. Instead, the common recommendation is that teams develop and maintain relationships with the other departments in the business that are responsible for them and see what the common problems are, and how IT security may be able to assist.

Security leadership has to make a determined and genuine effort to foster and develop these relations and maintain fruitful conversations between the security team and the rest of the business. In the next chapter, you will read about the importance of security in the software development lifecycle.

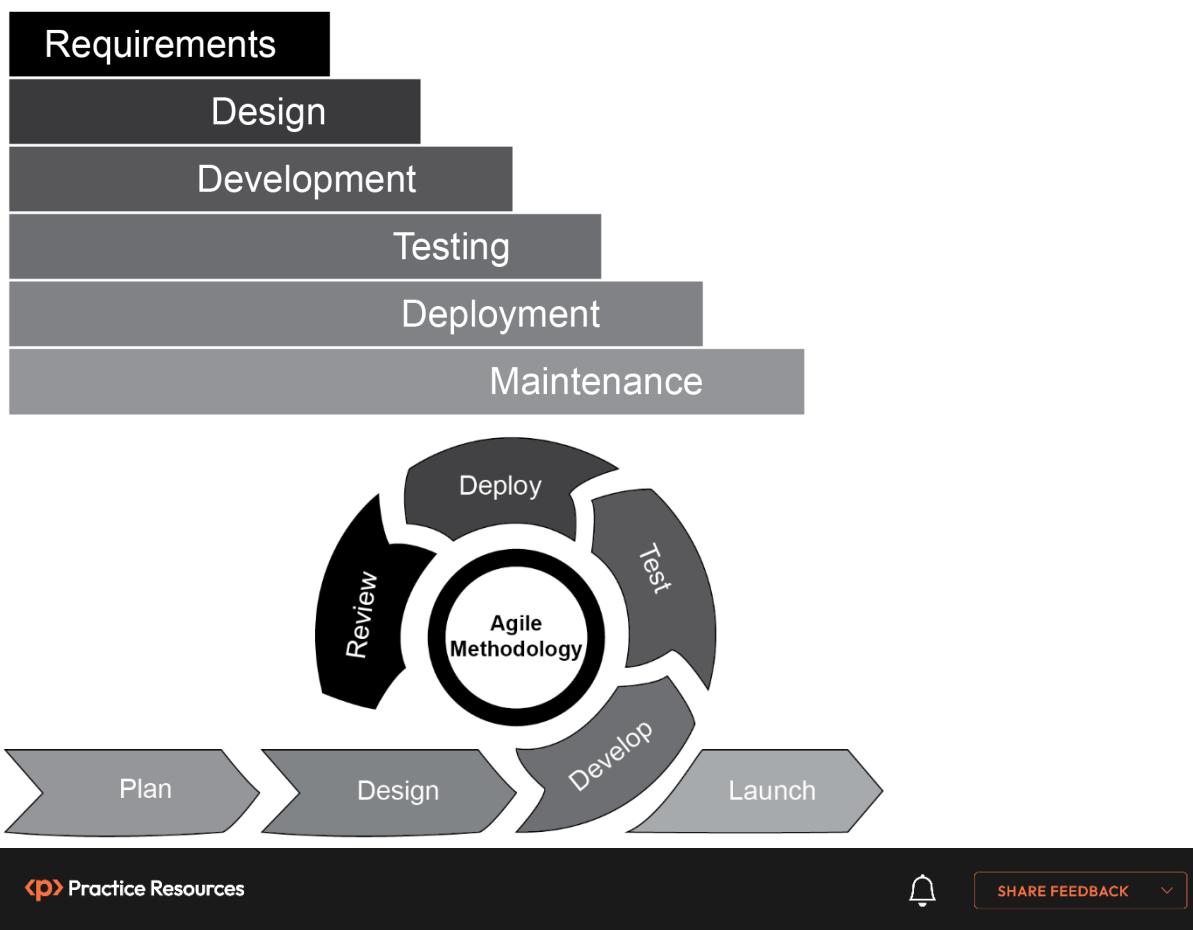
#### Chapter Review Questions

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

Select Quiz

Quiz 1 [SHOW QUIZ DETAILS](#) 

## Chapter 20: Software Development Life Cycle Security



### Practice Resources



SHARE FEEDBACK ▾

DASHBOARD > CHAPTER 20

### Software Development Life Cycle Security

#### Summary

In this chapter, you learned about the several frameworks used for creating applications, including Waterfall, Agile, and DevOps. Each of these has a suite of tools that work along with them to help teams create secure operating systems, programs, and websites.

You also learned about the importance of ensuring that suppliers meet minimal security levels and have application security policies in place. These can be measured with maturity models such as CMMI and SAMM.

Operations and maintenance are essential considerations. Once an application is released, it's important to determine whether patches will need to be created or whether the application will be updated with new features. You learned that applications are not static and must be changed for various reasons. Changes are planned and designed as part of the SDLC.

Finally, you learned how changes need to be tracked and managed, and that as you improve applications, you should make sure that changes are secure. You learned how IPTs help you by making sure applications meet the needs of the customer, vendors, suppliers, and other working teams in the organization. The next chapter will cover software development security controls.

#### Chapter Review Questions

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

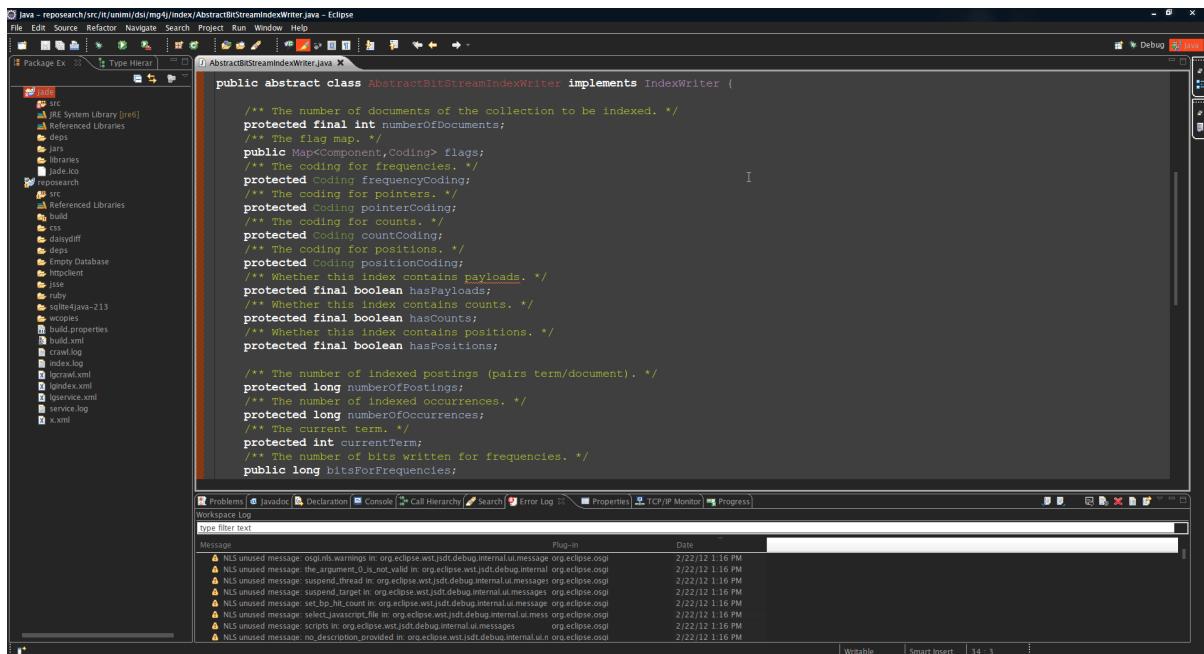
##### Select Quiz

Quiz 1

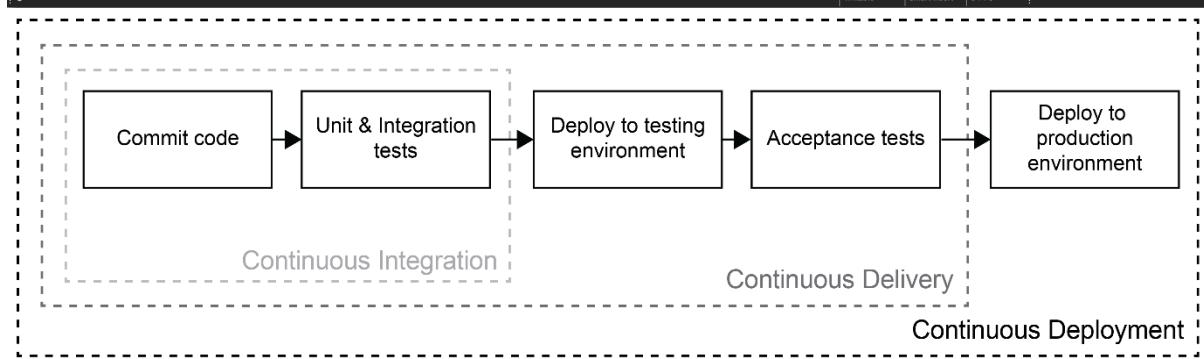
[SHOW QUIZ DETAILS ▾](#)

START

## Chapter 21: Software Development Security Controls



A screenshot of the Eclipse IDE interface. The top window shows the code for `AbstractBitStreamIndexWriter.java`. The code is an abstract class that implements `IndexWriter`. It contains various protected fields and methods related to indexing documents, frequencies, and positions. Below the code editor is the Eclipse error log window, which displays several log messages from the org.eclipse.wst.jsdt.debug internal plugin, indicating unused messages and warnings.



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

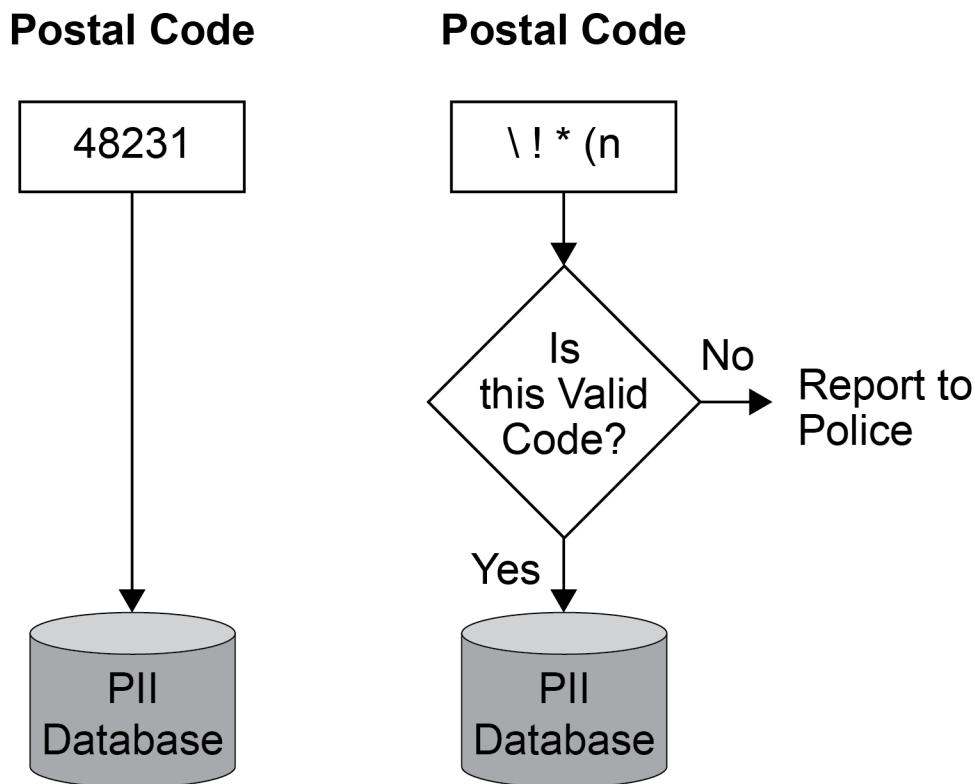
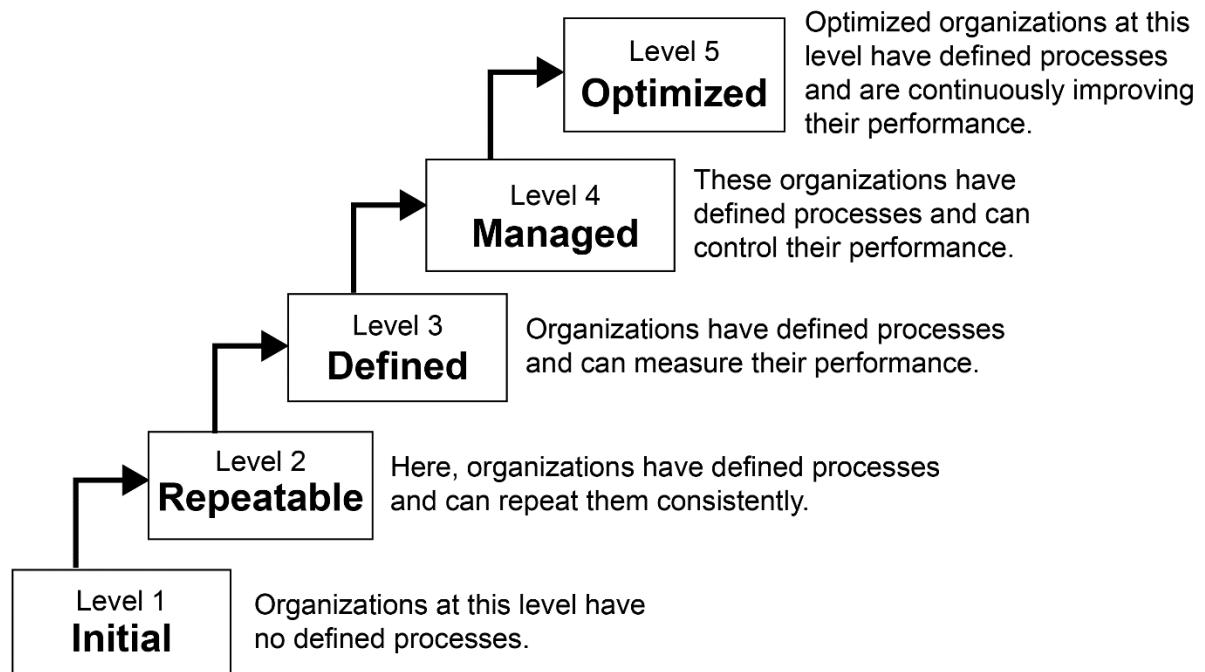
The Certified Information Systems Security Professional (CISSP) Exam Guide by Ted Jordan, Ric Daza, Hinne Hettema

#### Select Quiz

Quiz 1  
[SHOW QUIZ DETAILS](#)

START

## Chapter 22: Securing Software Development



A → B

g	w	c	a	r	v	e	r	o	3
---	---	---	---	---	---	---	---	---	---

doctor-geol → A

A → B

d	o	c	t	o	r	-	g	e	o
---	---	---	---	---	---	---	---	---	---

◀p 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 Heffema

#### Select Quiz

Quiz 1

[SHOW QUIZ DETAILS ▾](#)

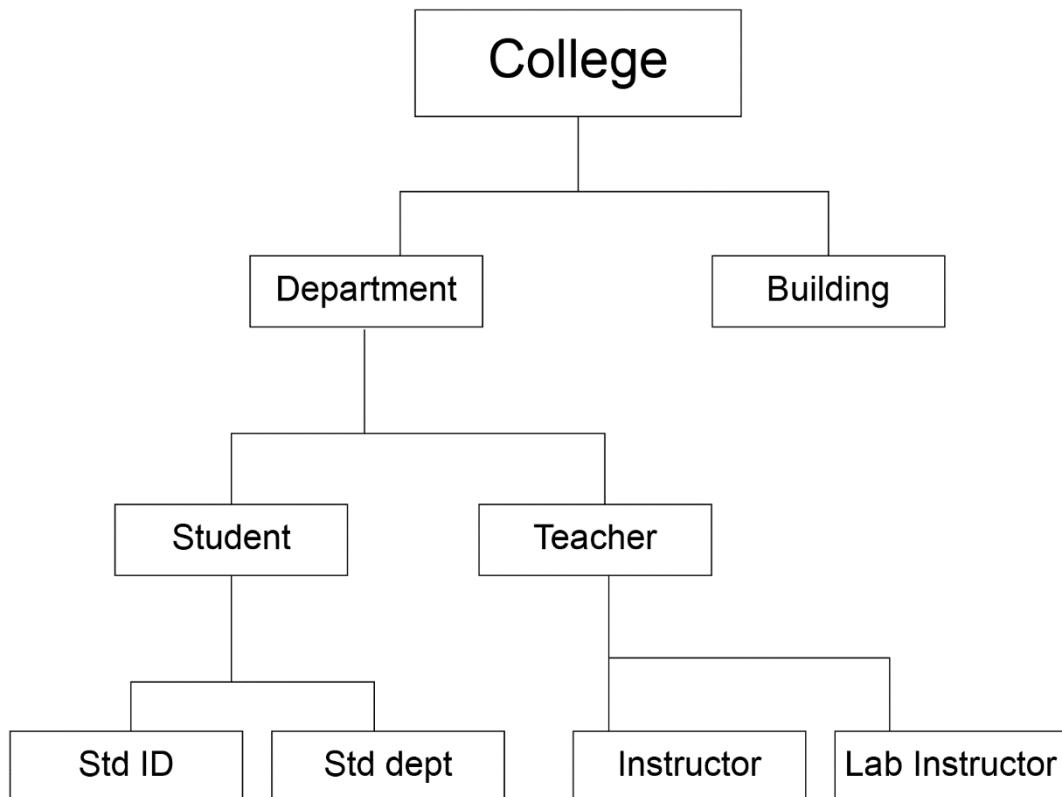
START

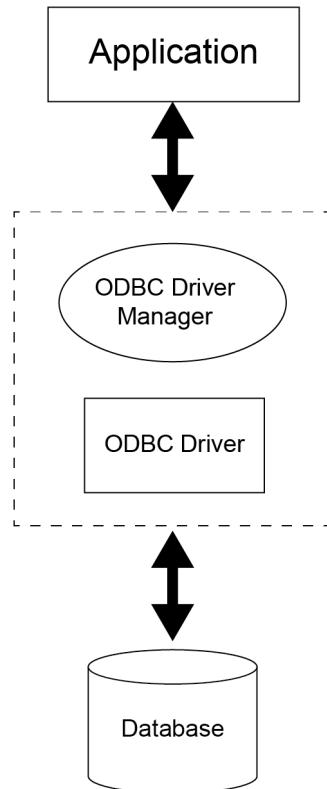
Chapter 23: Secure Coding Guidelines, Third-Party Software, and Databases

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

```





**Practice Resources**

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 Heittema

Select Quiz

Quiz1 [SHOW QUIZ DETAILS](#) ▾ [START](#)

## Chapter 24: Accessing the Online Practice Resources

**<P> Practice Resources**

**REPORT ISSUE**

### UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.



#### Certified Information Systems Security Professional (CISSP) Exam Guide

Book ISBN: 9781800567610  
Mr. Ted Jordan, MSc, CISSP • Ric Daza • Hinne Hettema • Aug 2024 • pages

Do you have a Packt account?

Yes, I have an existing Packt account  No, I don't have a Packt account

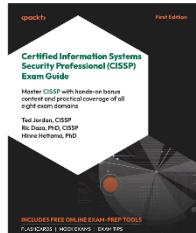
**PROCEED**

**<P> Practice Resources**

**REPORT ISSUE**

### UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.



#### Certified Information Systems Security Professional (CISSP) Exam Guide

Book ISBN: 9781800567610  
Mr. Ted Jordan, MSc, CISSP • Ric Daza • Hinne Hettema • Aug 2024 • pages

#### ENTER YOUR PURCHASE DETAILS

Enter Unique Code \*

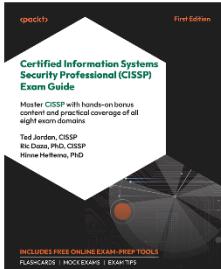
E.g. 123456789

[Where To Find This?](#)

Check this box to receive emails from us about new features and promotions on our other certification books. You can opt out anytime.

**REQUEST ACCESS**

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](#) 

### 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



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