ExamLabs

CompTIA Cloud Essentials+

Study Guide

Exam CLO-002

CONTENTS

List of Tables

Chapter 1

Chapter 2

Chapter 4

Chapter 5

Chapter 6

List of Illustrations

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Table of Exercises

Introduction

Shortly after the Internet exploded in popularity, it was common to hear people joke that “maybe this isn’t just a fad.” Looking back, it’s hard to believe that anyone would have ever seriously thought that it was, given its omnipresence in our lives today. The same things can be said about the cloud. What might have seemed like a novelty in the late 2000s is now mainstream. Most of us use cloud-based services every day, whether we realize it or not.

It’s safe to say that the cloud has transformed our Internet experience as users. It’s also had a massive impact on the way that companies and other organizations conduct business. The cloud has the potential to save organizations money and time, but only if it’s implemented properly. Of course, that takes some technical expertise. But it also takes business knowledge. The intersection of business acumen and technical knowledge is where this book focuses.

Why Certify for Cloud Business Skills?

There is a major need in the market today for people who understand both the technical side and the business side of an organization. Indeed, all of the following are reasons to become certified in cloud business skills:

- The largest skills gap in IT workers is business acumen.
- IT employees are now expected to weigh in on business decisions.
- Certification empowers both technical and nontechnical employees to make data-driven cloud recommendations.
- Certification demonstrates readiness for promotional opportunities to management-level positions.
- Certification ensures understanding of personnel working for cloud product and services organizations.

The CompTIA Cloud Essentials+ exam is a great certification for a few reasons. First, it's job-focused and aligned with the needs of employers. Second, it's current with today's cloud environment—the technology and how it's used. Third, it's the only vendor-neutral cloud-specific business certification. It's a great stepping stone for IT and business professionals who want to become certified in specific cloud technologies such as Amazon AWS or Microsoft Azure.

Who Should Read This Book?

This book is a great resource as a primer to cloud technologies, with a practical focus. We don't get into too much deep technical theory. We want people who read this book to understand cloud terms and basic technologies and be able to apply that knowledge to business situations.

The Cloud Essentials+ cert, and therefore this book, is for IT and business professionals who:

- Want to move into management and leadership roles
- Work for cloud product and services companies
- Have a strong technical or data background, but do not have a business degree
- Have good general business acumen, but do not have validation of their competency in cloud-specific situations
- Are responsible for providing recommendations on cloud-related decisions
- Wish to understand why their company makes the cloud-related decisions they do
- Want to remain relevant to their employers by demonstrating professional growth, in an area of unmet need

If any of these apply to you, then this book can help you out!

What Does This Book Cover?

This book covers everything you need to know to pass the CompTIA Cloud Essentials+ exam. Official objectives are available here:

https://certification.comptia.org/certifications/cloud-essentials

Chapter 1: **Cloud Principles and Design**. This chapter introduces basic cloud principles. Included are service models, or what the cloud can deliver, deployment models, or how the cloud can be executed, and several characteristics that make the cloud valuable to a business.

Chapter 2: **Cloud Networking and Storage**. The cloud is perhaps best known for its storage capabilities, so this chapter covers different features of cloud storage such as compression, deduplication, and capacity on demand, as well as hot versus cold storage, storage types, and software-defined storage and content delivery networks.

Accessing the cloud is also of high importance, so this chapter also discusses cloud connectivity and access types and popular networking tools such as load balancers, DNS, and firewalls.

Chapter 3: **Assessing Cloud Needs**. Every organization has slightly different cloud needs. This chapter starts with assessing company needs to determine how the cloud will provide benefits. Then, it moves into looking into some specific types of benefits in detail, including access management, data analytics, digital marketing, the Internet of Things, blockchain, and more.

Chapter 4: **Engaging Cloud Vendors**. After an organization has analyzed the technical side and decided to move to the cloud, it's time to find the right cloud provider. This chapter looks at financial and business aspects of engaging cloud providers. We talk about types of expenditures, licensing models, requests for information, statements of work, service level agreements, evaluations, and contracts and billing.

Chapter 5: **Management and Technical Operations**. Continuing with some of the technical aspects of operating in the cloud, we discuss data management, availability, disposable resources, monitoring, and visibility. These are a precursor and are used when starting DevOps and a CICD pipeline. Testing and configuration management are critical aspects of DevOps, and we walk through a few examples. Finally, we discuss financials and reporting on usage when using resources in the cloud.

Chapter 6: **Governance and Risk**. Organizations will have to manage risk whenever they use cloud resources. In this chapter we introduce the concept of risk and the responses. We discuss some risks that are different when using the cloud versus on-premises data centers. We introduce policies and procedures and some of the organization management needed for cloud initiatives. We finish with policies that are specific to security, access, and control.

Chapter 7: **Compliance and Security in the Cloud**. Cloud security will be a critical piece for any organization wanting to implement resources in the cloud. This chapter looks at regulations and standards that may be required for an organization to use the cloud. We take a deeper dive into data security and processes for securing the data. We give examples of security assessments that any organization should be performing. Finally, we discuss applications and infrastructure security.

What’s Included in This Book?

We’ve included the following study tools throughout the book:

Assessment Test. At the end of this introduction is an assessment test that you can use to check your readiness for the exam. Take this test before you start reading the book; it will help you determine the areas where you might need to brush up. The answers to the assessment test questions appear on a separate page after the last question of the test. Each answer includes an explanation and a note telling you the chapter in which the material appears.

Objective Map and Opening List of Objectives. Just before the assessment test, you’ll find a detailed exam objective map, showing you where each of the CompTIA exam objectives is covered in this book. In addition, each chapter opens with a list of the exam objectives it covers. Use these to see exactly where each of the exam topics is covered.

Exam Essentials. Each chapter, just after the summary, includes a number of exam essentials. These are the key topics that you should take from the chapter in terms of areas to focus on when preparing for the exam.

Written Labs. Each chapter includes a written lab to test your knowledge. These labs map to the exam objectives. You can find the answers to those questions in Appendix A.

Chapter Review Questions. To test your knowledge as you progress through the book, there are 20 review questions at the end of each chapter. As you finish each chapter, answer the review questions and then check your answers—the correct answers and explanations are in Appendix B. You can go back to reread the section that deals with each question you got wrong in order to ensure that you answer correctly the next time you’re tested on the material.

Cloud Essentials+ Study Guide Exam Objectives

This table provides the extent, by percentage, to which each domain is represented on the actual examination.

Domain	**% of Examination**
1.0 Cloud Concepts	24%
2.0 Business Principles of Cloud Environments	28%
3.0 Management and Technical Operations	26%
4.0 Governance, Risk, Compliance, and Security for the Cloud	22%
Total	100%

> NOTE .Exam objectives are subject to change at any time without prior notice .and at CompTIA’s sole discretion. Please visit CompTIA’s website .(www.comptia.org) for the most current listing of exam objectives.

Objective Map

Objective	Chapter
Domain 1.0: Cloud Concepts	
1.1 Explain cloud principles.	1
1.2 Identify cloud networking concepts.	2
1.3 Identify cloud storage technologies.	2
1.4 Summarize important aspects of cloud design.	1
Domain 2.0: Business Principles of Cloud Environments	
2.1 Given a scenario, use appropriate cloud assessments.	3
2.2 Summarize the financial aspects of engaging a cloud provider.	4
2.3 Identify the important business aspects of vendor relations in cloud adoptions.	4
2.4 Identify the benefits or solutions of utilizing cloud services.	3
2.5 Compare and contrast cloud migration approaches.	4
Domain 3.0: Management and Technical Operations	
3.1 Explain aspects of operating within the cloud.	5
3.2 Explain DevOps in cloud environments.	5
3.3 Given a scenario, review and report on the financial expenditures related to cloud resources.	5
Domain 4.0: Governance, Risk, Compliance, and Security for the Cloud	
4.1 Recognize risk management concepts related to cloud services.	6
4.2 Explain policies or procedures.	6
4.3 Identify the importance and impacts of compliance in	6

the cloud.	
4.4 Explain security concerns, measures, or concepts of cloud operations.	7

Assessment Test

1. In the shared responsibility model, who is responsible for the security of compute and storage resources?

    A. CSP

    B. Client

    C. CSP and client

    D. All clients together

2. Gmail is an example of which type of cloud service?

    A. SaaS

    B. IaaS

    C. XaaS

    D. PaaS

3. Microsoft Azure is an example of which type of cloud deployment model?

    A. Commercial

    B. Public

    C. Private

    D. Hybrid

4. Your CTO wants to ensure that company users in Asia, Europe, and South America have access to cloud resources. Which cloud characteristic should be considered to meet the business need?

    A. Self-service

    B. Broad network access

    C. Scalability

    D. Shared responsibility

5. You are negotiating the SLA with a CSP. Which of the following high availability guarantees is likely to cost you the most?
   A. Three nines
   B. Four nines
   C. Five nines
   D. None—they should all be the same price
6. You are negotiating an SLA with a CSP. Who is responsible for defining the RPO and RTO?
   A. The client.
   B. The CSP.
   C. The client defines the RPO, and the CSP defines the RTO.
   D. The client defines the RTO, and the CSP defines the RPO.
7. Which of the following cloud technologies reduces the amount of storage space needed by removing redundant copies of stored files?
   A. Capacity on demand
   B. Compression
   C. Deduplication
   D. Block storage
8. You are setting up a cloud solution for your company, and it needs to be optimized for unstructured data. Which storage type is appropriate?
   A. Block
   B. File
   C. Cold
   D. Object
9. What is SSH used for within the cloud environment?
   A. To remotely manage a Windows server

B. To remotely manage a Linux server

C. To remotely access cloud storage

D. To remotely deliver content to clients

10. You are setting up cloud services and need space to store email archives. Which of the following will be the least expensive solution?

A. Hot storage

B. Cold storage

C. Object storage

D. Block storage

11. You are obtaining cloud-based networking for your company. The CIO insists that the cloud resources be as safe as possible from potential hackers. Which service will help with this?

A. Load balancing

B. DNS

C. SDN

D. Firewall

12. Which of the following services within a cloud is responsible for resolving host names to IP addresses?

A. DNS

B. SDN

C. CDN

D. SDS

13. You are consulting for Company A, and they ask you to run a cloud assessment. In which order should you perform the following tasks as part of this assessment? (List the steps in order.)

A. Compare benchmarks

B. Perform a feasibility study

C. Run a baseline

D. Gather current and future requirements

14. An engineer on your team says that the company should use new technology to enter a new stream of business. He says that you should sell and monitor linked home appliances and smart thermostats. Which technology is he talking about using?

A. VDI

B. IoT

C. SSO

D. AI

15. You are beginning a cloud assessment for your company and need to contact key stakeholders. Who in the following list is NOT an example of a key stakeholder for the cloud assessment?

A. CEO

B. CISO

C. CSP

D. Department manager

16. Which of the following cloud services uses probabilities to make predictions about input?

A. Artificial intelligence

B. Autonomous environments

C. Microservices

D. Machine learning

17. Which of the following is NOT a key operating principle of blockchain?

A. Anonymity

B. Transparency

C. Immutability

D. Decentralization

18. You are implementing multiple levels of security for new cloud resources. Which of the following is NOT a method of cloud-based identity access management?

A. SSO

B. MFA

C. VDI

D. Federation

19. You are searching for the right cloud vendor for your organization. Which of the following should be your first step?

A. Pilot

B. RFP

C. RFQ

D. RFI

20. Your current cloud contract is expiring, and you need to quickly move to a different provider. Which type of migration is best in this situation?

A. Rip and replace

B. Lift and shift

C. Hybrid

D. Phased

21. You want to test a solution from a CSP to show that a new technology works properly. Which type of evaluation should you perform?

A. PoC

B. PoV

C. Managed

D. Pilot

22. Internal IT employees need to learn to use a new cloud-based software interface to manage corporate services. What should you request from the CSP?

    A. Support

    B. Managed services

    C. Training

    D. Professional development

23. The finance department wants you to convert the IT infrastructure capital expenditures to operating expenditures. Which of the following would do this?

    A. Switch to BYOL licensing

    B. Negotiate billing terms for new IT hardware

    C. Switch to a pay-as-you-go model

    D. Depreciate the IT assets on a shorter time horizon

24. A company hires contractors for six-month projects. After six months, a new team of contractors will be brought in. Which type of software licensing allows the licenses to be transferred from the first group to the second group?

    A. Pilot

    B. PoC

    C. Subscription

    D. BYOL

25. You have migrated to the cloud, and users have access to cloud-based productivity software. There are 10 users in the finance group. Each user has a laptop, tablet, and smartphone that can access the productivity software. Using a subscription model, how many software licenses will you need to purchase for the finance department?

    A. 1

B. 10

C. 20

D. 30

26. In the Continuous Integration Continuous Delivery (CI/CD) pipeline the four steps are separated into _________ from each other, and the CI/CD attempts to remove them.

A. Regions

B. Zones

C. Silos

D. Networks

27. The latency between data and the end user is determined for the most part by the property:

A. Locality

B. Provisioned

C. Replication

D. Data availability

28. Linux as an operating system utilizes which license type?

A. Free for use

B. Pay for use

C. Rent for use

D. Lease for use

29. Which replication type keeps data synced between two or more locations in real time?

A. Asynchronous

B. Autoscaling

C. Synchronous

D. Reserved

30. Copying snapshots of instances to different locations in order to protect against data loss or corruption is an example of:

    A. Geo-redundancy

    B. Replication

    C. Backups

    D. Object storage

31. Immutable infrastructure contains resources that:

    A. Are unchangeable

    B. Are destructable

    C. Are ephemeral

    D. Are changeable

32. Analysis that is dependent on the quality or perceived value of an asset is known as:

    A. Perceptive

    B. Qualititative

    C. Quantitative

    D. Valuative

33. Analysis that is dependent on the monetary value or quantity of an asset is known as:

    A. Qualititative

    B. Perceptive

    C. Valuative

    D. Quantitative

34. The three main components of risk are?

    A. Employees, health, happiness

    B. Servers, network, attack

    C. Assets, threat, probability

D. Money, stocks, failure

35. __________ and __________ owner are the individuals of an organization who own and manage risk. (Choose two.)

A. CEO

B. Risk

C. President

D. Asset

36. __________ is a risk response where an organization decides to initiate actions to prevent any risk from taking place.

A. Transfer

B. Avoidance

C. Mitigation

D. Acceptance

37. __________ are directions, guidance, and provide goals for an organization.

A. Procedures

B. Policies

C. Agendas

D. Manuals

38. With new advancements in CSP technologies, you don't need to worry about storing sensitive data in the cloud. Without any configuration on your part, a CSP's tools will be .sufficient for what?

A. Application scanning

B. Reulatory requirements

C. Confidentiality

D. Integrity

39. An organization that does business internationally needs to take

into consideration data sovereignty laws on data stored in: (Choose all that apply.)

A. The nation where the data is stored

B. The nationality of the user the data is about

C. The language that the data is stored in

D. The location of the organization that stores the data

40. In the event of competing local, state, federal, and international regulatory requirements, which regulations should an organization follow?

A. Local

B. State

C. Federal

D. International

41. Your organization is in negotiations with a federal contractor that also deals with sensitive information from the federal government. Which federal regulation will apply in this scenario?

A. FERPA

B. MPAA

C. FISMA

D. NIST

42. You have been tasked with designing an FIPS 140-2 compliant application. Which technology are you most concerned with?

A. User identity and passwords

B. Encryption

C. Mac versus PC

D. Authorization

43. HIPAA, GLBA, PCI DSS, and FINRA are all examples of __________ based standards.

A. Organizational

B. Federal

C. Industry

D. International

Answers to Assessment Test

1. C. In the shared responsibility model, the CSP is responsible for security of the cloud, which includes services and infrastructure such as compute and storage resources. Clients are responsible for security in the cloud, such as operating systems, access management, and customer data. See Chapter 1 for more information.
2. A. The software as a service (SaaS) model provides software applications, including apps such as Google Docs, Microsoft Office 365, and Gmail. Infrastructure as a service (IaaS) offers hardware for compute, storage, and networking functionality.

   Anything as a service (XaaS) is too broad and can mean a combination of multiple services. Platform as a service (PaaS) provides development platforms for software developers. See Chapter 1 for more information.
3. B. Microsoft Azure, Amazon Web Services, and Google Cloud are all examples of public clouds. There is no commercial cloud deployment model. Private clouds are owned and used by one company and not sold to others. A hybrid cloud is both public and private. See Chapter 1 for more information.
4. C. Scalability can refer to the ability for cloud services to be scaled geographically. Users from multiple global locations can access resources. Self-service means the ability to add resources without supplier intervention. Broad network access means that various client devices with different operating systems can access resources. Shared responsibility is a model that defines and enhances cloud security. See Chapter 1 for more information.
5. C. High availability models are specified in terms of nines. More nines guarantee more uptime but also cost more. Therefore, five nines will cost more than four nines, which will cost more than three nines. See Chapter 1 for more information.

6. A..The client is responsible for defining the recovery point objective (RPO), which is the maximum age of files that must be recovered from backups in order to restore normal operations, and the recovery time objective (RTO), which is how long the CSP has to get everything operational, including network access and data restoration, in the event of a disaster. See Chapter 1 for more information.
7. C..Deduplication saves storage space by removing redundant copies of files. Compression also saves space but does it by removing redundancy within a file. Capacity on demand is when a client can get more storage space instantaneously. Block storage is a storage type. While it's more efficient than file storage, it doesn't remove redundant files or data. See Chapter 2 for more information.
8. D..Object storage is the best option for unstructured data. Block storage is good for databases, storage area networks, and virtual machines. File storage is used on common PC operating systems such as Windows and macOS. Cold storage means the data is offline. See Chapter 2 for more information.
9. B..Secure Shell (SSH) is used to remotely manage Linux-based servers. The Remote Desktop Protocol is used to remotely manage Windows-based servers. See Chapter 2 for more information.
10. B..Cold storage will always be less expensive than hot storage. Object and block storage are ways to store files, but either can be hot or cold. See Chapter 2 for more information.
11. D..A firewall is a network- or host-based security device. It can help protect a network or individual computers from malicious network traffic. Load balancing means spreading work across multiple servers. Domain Name System (DNS) resolves host names to IP addresses. Software-defined networking (SDN) makes networks more agile and flexible by separating the forwarding of network packets (the infrastructure layer) from the logical decision-making process (the control layer). See Chapter 2 for more information.

12. A. Domain Name System (DNS) resolves host names to IP addresses. SDN abstracts network hardware in the cloud. A content delivery network does load balancing for websites. Software-defined storage (SDS) allows for the virtualization of cloud storage solutions. See Chapter 2 for more information.

13. D, C, B, A. The first step in a cloud assessment is to determine current and future requirements. Then, run a baseline, followed by a feasibility study, then gap analysis, then use reporting, and then compare to benchmarks. Finally, create documentation and diagrams. See Chapter 3 for more information.

14. B. Linked home appliances and smart thermostats are examples of technologies that rely upon the Internet of Things (IoT). Virtual desktop infrastructure (VDI) creates virtual user desktops. Single sign-on (SSO) is a security mechanism for computer logins. Artificial intelligence is when computers perform complex, human-like tasks. See Chapter 3 for more information.

15. C. Key stakeholders are important people with a vested interest in something. In this case, the chief executive officer (CEO), chief information security officer (CISO), and department manager could all be key stakeholders. The cloud service provider (CSP) is not a key stakeholder who should have input on which cloud services you need. They can make suggestions, but their role is to sell you services. See Chapter 3 for more information.

16. D. Machine learning (ML), which is a general form of artificial intelligence (AI), uses probabilities to make predictions about classifying new input based on previous input it received. Autonomous environments are when machines perform complex, human-like actions without human intervention. Microservices is a way to speed up app development and lower costs. See Chapter 3 for more information.

17. A. Blockchain operates on three key principles: decentralization, transparency, and immutability. No one organization owns the blockchain, and the information is stored on all participating nodes. Therefore, there is decentralization and transparency. The data is also hard to hack, which gives it immutability. While the

user IDs are securely hashed in blockchain, there is no anonymity. See Chapter 3 for more information.

18. C. Virtual desktop infrastructure (VDI) is for creating virtual user desktops on a server. It is not related to identity access management (IAM). Single sign-on (SSO), multifactor authentication, and federation are all IAM services. See Chapter 3 for more information.

19. D. The first step is to gather information about a vendor's capabilities, and that is done through a request for information (RFI). After the RFI stage, you might request a bid for standard services with a request for quotation (RFQ) or request for proposal (RFP). A pilot is a small-scale evaluation deployment in the production environment. You would not do that before an RFI. See Chapter 4 for more information.

20. B. Lift and shift, where data and applications are picked up as is and moved to another location, is the quickest and cheapest migration option. In a rip and replace, software needs to be redeveloped to take advantage of cloud services. A hybrid is a combination of the two, or a migration where some items stay in the original location. Phased migrations happen over time. See Chapter 4 for more information.

21. A. A PoC is an evaluation used to prove that a technology works as it should. A proof of value (PoV) is run to see whether cost savings can be realized. Managed services are professional services used to support cloud installations. A pilot is a small-scale initial rollout of a solution into the production environment. See Chapter 4 for more information.

22. C. Training is a short-term activity that focuses on acquiring a specific skillset to perform a job. Support and managed services are professional services that you might buy to help support the cloud. Professional development refers to a long-term educational process focused on employee growth. See Chapter 4 for more information.

23. C. Purchasing IT hardware or other tangible assets is a capital

expenditure. Switching to a cloud-based IT infrastructure model with pay-as-you-go pricing means less (or no) need to purchase hardware and therefore no new capital expenditures. BYOL licenses can be permanent or subscription-based. Depreciation timelines are for capital expenditures only. See Chapter 4 for more information.

24. D. Bring your own license (BYOL) is when software can be transferred from one user to another or from one system to another. Subscriptions might or might not qualify as BYOL. Pilots and proof of concepts (PoCs) are types of evaluations. See Chapter 4 for more information.

25. B. Under a subscription-based model, users should have device flexibility, meaning that only one license per user is required. Therefore, you need 10 licenses. See Chapter 4 for more information.

26. C. The four teams involved in the CICD pipeline do not communicate or collaborate with each other. Regions, zones, and networks are terms that are not specific to the CICD pipeline. See Chapter 5 for more information.

27. A. Locality is the measure of the distance between data and the end user. This distance directly impacts the latency between the two. Provisioned is a state of an instance. Replication can affect latency but does not determine it. Data availability is a property of data and the availability. See Chapter 5 for more information.

28. A. The Linux kernel is licensed under the GPL, which is a free-for-use license. Pay for use is a license type, but the Linux kernel is free. C and D are not license types. See Chapter 5 for more information.

29. C. Synchronous replication keeps data synced in real time. Asynchronous replication eventually keeps data consistent. Autoscaling and Reserved are not types of replication. See Chapter 5 for more information.

30. C. Backups are the copying of data to a different location in the event of data loss or corruption. Replication does not copy

snapshots. Geo-redundancy does copy data, but the source can still be lost or corrupted. Object storage is where backups are usually copied to. See Chapter 5 for more information.

31. A.,Immutable means that the data cannot be modified or changed. B, C, and D are all properties that are changeable. See Chapter 5 for more information.

32. B.,Qualitative analysis is the analysis of a value of an asset based on its perceived value. In ,contrast, quantitative analysis is the analysis of the monetary value of an asset based on monetary value. See Chapter 6 for more information.

33. D.,Quantitative analysis is the analysis on of a value of an asset based on monetary value or its quantity. In contrast, qualitative analysis is the analysis of the value of an asset based on its perceived value. See Chapter 6 for more information.

34. C.,While the other choices may be assets and potential threats, they are all specific. Risk is the probability or likelihood of a threat against an asset. See Chapter 6 for more information.

35. B, D.,While a company's CEO and president maybe the top-level risk owners, they are not all of them. The two identified owners are the risk and asset owners. See Chapter 6 for more information.

36. C.,Mitigation is the risk response where an organization lowers or reduces the chance of risk but does not prevent all risk from occurring. Avoidance is the risk response where all risk is removed. See Chapter 6 for more information.

37. B.,Policies are general guidelines for an organization. Procedures are specific steps or actions. Agendas and manuals are where the guidelines are either documented or noted. See Chapter 6 for more information.

38. B.,CSPs do offer tools that can meet most if not all the regulatory requirements your organization may require. However, compliance is similar to the shared responsibility model. You will need to take some ownership of compliance. See Chapter 7 for more information.

39. A, B, D.‚Organizations that do business internationally and store data about users and transactions that originate around the globe must consider three criteria: Where the data is physically stored. The nationality of the users for whom the organization is storing data. The location in which the organization is doing business. See Chapter 7 for more information.

40. C.‚Particularly in the US, federal laws preempt all other regulations. However, most nation states have similar rules due to sovereignty laws. See Chapter 7 for more information.

41. C.‚The Federal Information Security Management Act (FISMA) is the federal regulation that deals with sensitive information security for federal agencies. FERPA is a federal law that protects the privacy of student education records. Motion Picture Association of America (MPAA) is the association that provides best practices guidance and control frameworks to help major studio partners and vendors design infrastructure and solutions to ensure the security of digital film assets. National Institute of Standards and Technology (NIST) is a part of the US Commerce Department that maintains and promotes guidelines and measurement standards. See Chapter 7 for more information.

42. B.‚FIPS is a cryptographic standard for encryption. The other answers may use encryption in some fashion, but they are not rated for FIPS compliance. See Chapter 7 for more information.

43. C.‚All the examples are standards that are industry specific. HIPAA is healthcare, GLBA is financial, PCI DSS is credit care, and FINRA is financial. See Chapter 7 for more information.