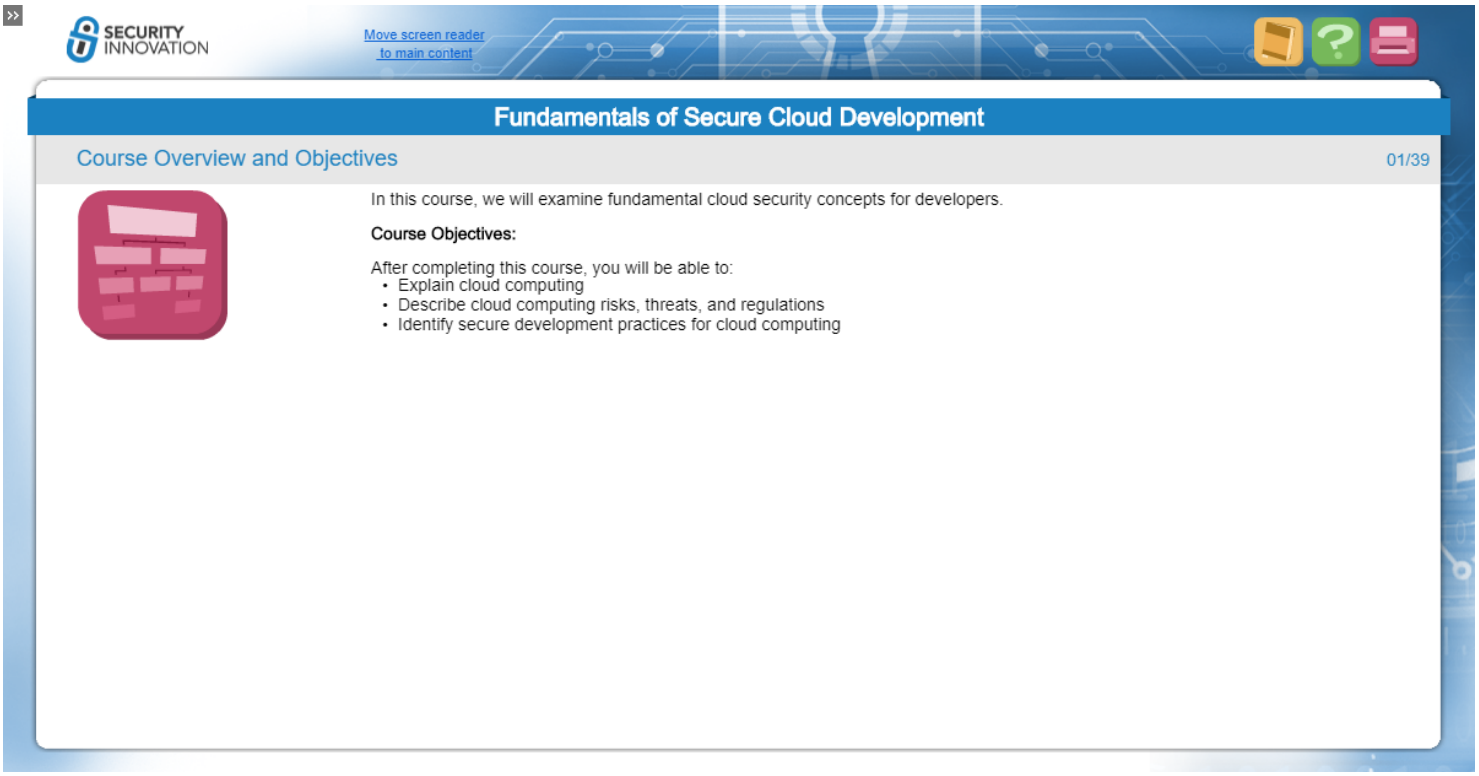
Course Overview and Objectives



Narration

In this course, we will examine fundamental cloud security concepts for developers.

First, we will examine the question, “What is the cloud?” The word cloud is very nebulous, and different people think of different things when they talk about the cloud.

We will also look at a definition and framework for cloud security so that when we examine security frameworks, we can easily compare and contrast them. Then, we will look at cloud computing risks, threats, and regulations. Finally, we will examine cloud computing secure development practices.

After completing this course, you will be able to Explain cloud computing; Describe cloud computing risks, threats, and regulations; Identify secure development practices for cloud computing.

On Screen Text

Course Overview and Objectives

In this course, we will examine fundamental cloud security concepts for developers.

Course Objectives:

After completing this course, you will be able to:

- Explain cloud computing
- Describe cloud computing risks, threats, and regulations
- Identify secure development practices for cloud computing

Module Overview and Objectives

Narration

This module provides an overview of cloud computing.

After completing this module, you will be able to understand cloud computing characteristics, service models, deployment models, and regulatory requirements.

On Screen Text

Module Overview and Objectives

This module provides an overview of cloud computing.

Module Objectives:
After completing this module, you will be able to:

- Understand cloud computing characteristics, service models, deployment models, and regulatory requirements

What Is the Cloud?

Narration

Cloud computing is a service offered by a cloud service provider (CSP) that can reduce or eliminate your organization's need for certain resources. Instead of designing, ordering, procuring, and supporting their own infrastructure as capital investments, companies can use a cloud service.

Traditionally, organizations have to build storage area networks and network file servers, and manage equipment, capacity, and server redundancy to ensure high availability. With cloud computing, when a server or network router fails, the cloud service provider can simply initialize a server, virtual machine, or router, and move the workload. In some cases, they can prevent failures and overloads using automated failure recovery and resource allocation. Cloud vendors also manage, monitor, patch, and upgrade the cloud infrastructure.

Cloud services can help prevent data loss, reduce costs related to data center redundancy, and help prevent monetary loss due to equipment failure.

However, the cloud does pose new risks. Entrusting sensitive corporate data to a third party raises privacy and regulatory concerns about protecting sensitive corporate, healthcare, and financial data, and protecting personally identifiable information. Keep in mind that, regardless of where data is stored, the ultimate responsibility for data security resides with the data's owner, be it an individual, organization, or enterprise.

According to the National Institute of Standards and Technology (NIST), the cloud consists of five essential characteristics, three service models, and four deployment models.

We will examine each of these concepts in a bit more detail on the next few screens.

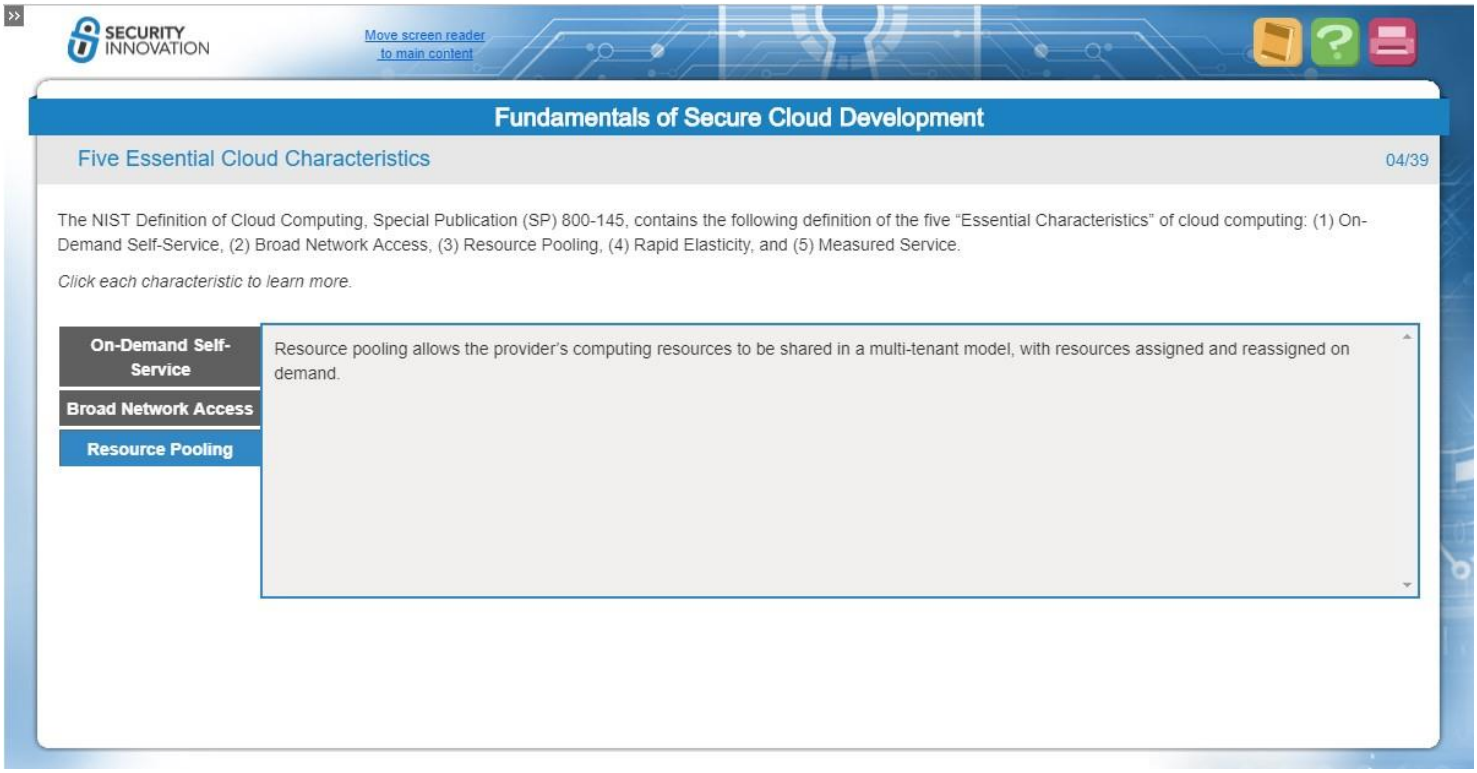
On Screen Text

What Is the Cloud?

As per the National Institute of Standards and Technology (NIST), the cloud consists of:

- Five essential characteristics
- Three service models
- Four deployment models

Five Essential Cloud Characteristics



Narration

Cloud computing can be applied to incorporate all aspects of computing technology into a shared pool of configurable cloud computing resources.

The NIST Definition of Cloud Computing, Special Publication (SP) 800-145, contains the definition of the following five "Essential Characteristics" of cloud computing—on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Click each characteristic to learn more.

On Screen Text

Five Essential Cloud Characteristics

The NIST Definition of Cloud Computing, Special Publication (SP) 800-145, contains the following definition of the five “Essential Characteristics” of cloud computing: (1) On-Demand Self-Service, (2) Broad Network Access, (3) Resource Pooling, (4) Rapid Elasticity, and (5) Measured Service.

Click each characteristic to learn more.

On-Demand Self-Service

On-demand self-service is a service available to the consumer without the intervention of the provider.

The “consumer” is the individual or organization that purchases the cloud service. Most of the examples in this course assume that an organization is the consumer.

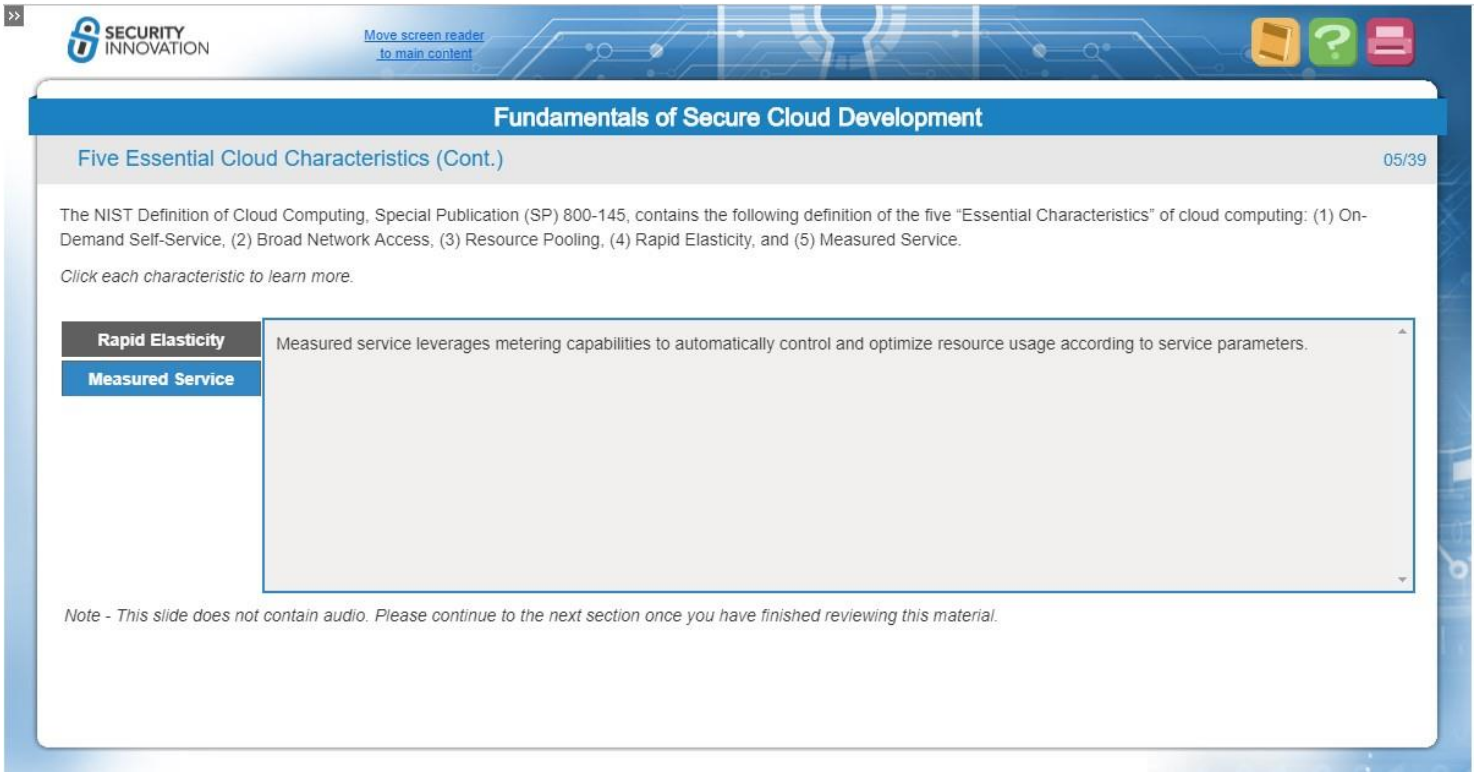
Broad Network Access

Broad network access goes beyond the Internet to include a wide range of client platforms.

Resource Pooling

Resource pooling allows the provider’s computing resources to be shared in a multi-tenant model, with resources assigned and reassigned on demand.

Five Essential Cloud Characteristics (Cont.)



Narration

On Screen Text

Five Essential Cloud Characteristics (Cont.)

The NIST Definition of Cloud Computing, Special Publication (SP) 800-145, contains the following definition of the five "Essential Characteristics" of cloud computing: (1) On-Demand Self-Service, (2) Broad Network Access, (3) Resource Pooling, (4) Rapid Elasticity, and (5) Measured Service.

Click each characteristic to learn more.

Rapid Elasticity

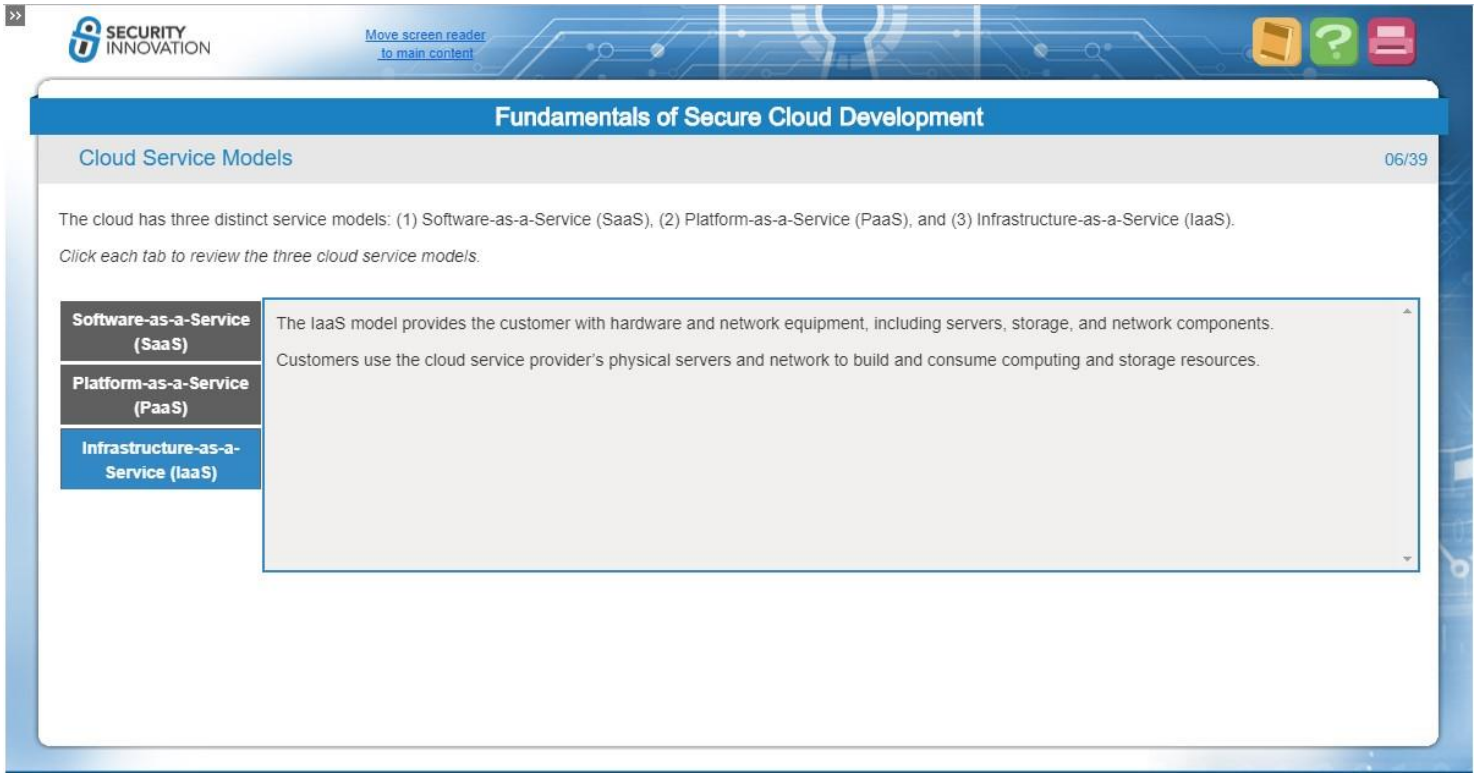
Rapid elasticity allows resources to be rapidly and flexibly provisioned and scaled out and in. This provisioning and scaling is performed manually or, in the best case, automatically, either from set parameters or from application logic.

Measured Service

Measured service leverages metering capabilities to automatically control and optimize resource usage according to service parameters.

Note - This slide does not contain audio. Please continue to the next section once you have finished reviewing this material.

Cloud Service Models



Narration

As described by the Cloud Security Alliance, the cloud has three distinct service models—Software-asa-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). The three cloud service models provide different sets of resources to the customer.

The SaaS model provides customers with a cloud-hosted software and development environment. The PaaS model provides customers with a virtual infrastructure, which runs on top of the CSP's physical infrastructure and Virtual Machine Manager (VMM), to build, process, and store data. And, in the IaaS model, customers use the provider's physical servers and network to build and consume computing and storage resources.

Click each tab to review the three cloud service models.

On Screen Text

Cloud Service Models

The cloud has three distinct service models: (1) Software-as-a-Service (SaaS), (2) Platform-as-aService (PaaS), and (3) Infrastructure-as-a-Service (IaaS).Click each tab to review the three cloud service models.

Software-as-a-Service (SaaS)

The SaaS model gives customers access to the provider's cloud-hosted software and development environment.

Customers configure the application and load data.

Platform-as-a-Service (PaaS)

The PaaS model provides the operating system virtual machine management, libraries, services, and tools required to support applications in the cloud.

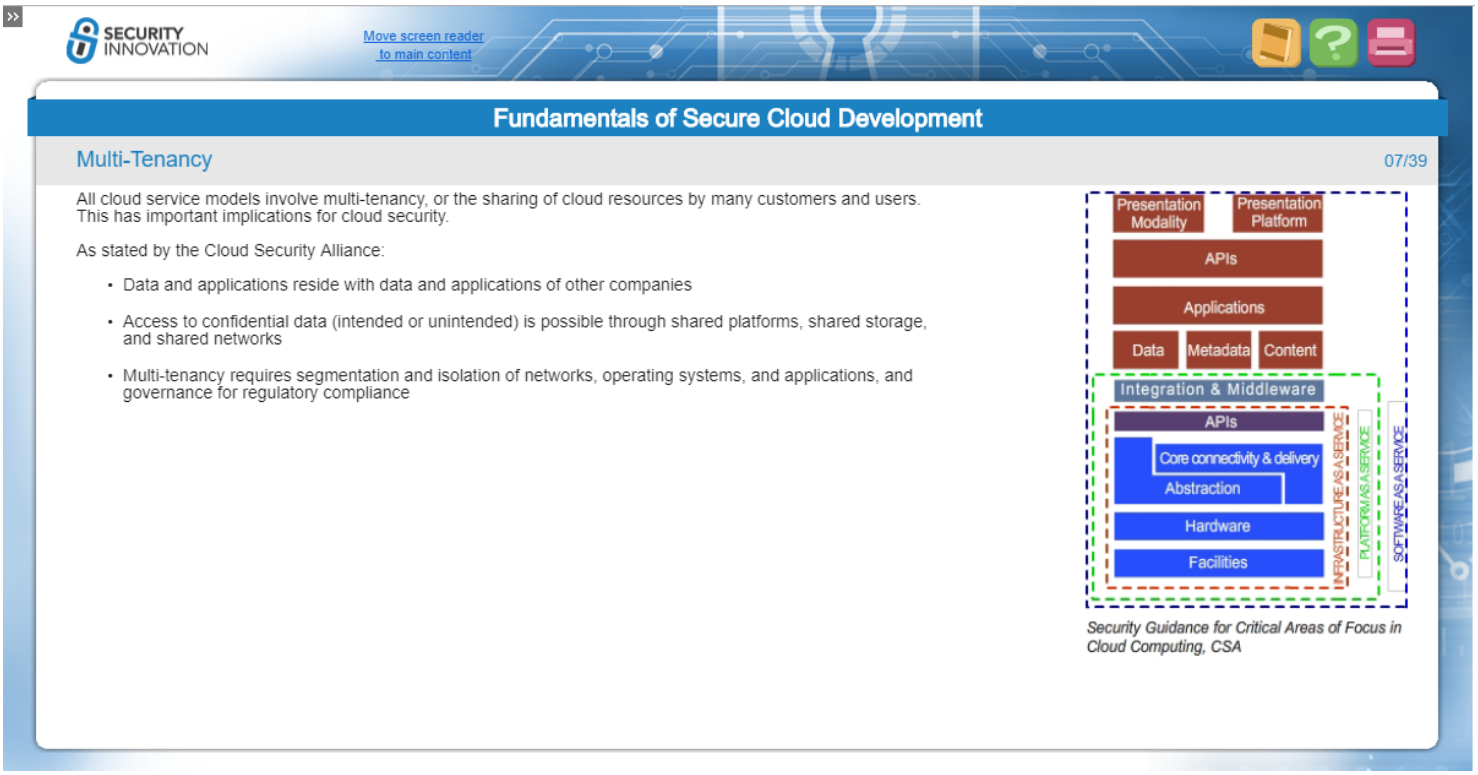
Customers use a virtual infrastructure, which runs on top of the CSP's physical infrastructure and Virtual Machine Manager (VMM), to build, process, and store data.

Infrastructure-as-a-Service (IaaS)

The IaaS model provides the customer with hardware and network equipment, including servers, storage, and network components.

Customers use the cloud service provider's physical servers and network to build and consume computing and storage resources.

Multi-Tenancy



Narration

Multi-tenancy, the sharing of cloud resources by many separate organizations and many separate users within those organizations, is characteristic of all cloud services, and affects cloud security.

As stated by the Cloud Security Alliance, multi-tenancy means that your data and applications reside with the data and applications of other companies. Access to confidential data, whether intended or unintended, is possible through shared platforms, shared storage, and shared networks.

Multi-tenancy requires enforced segmentation and isolation of network, operating system, and applications, as well as governance for regulatory compliance.

On Screen Text

Multi-Tenancy

All cloud service models involve multi-tenancy, or the sharing of cloud resources by many customers and users. This has important implications for cloud security.

As stated by the Cloud Security Alliance:

- Data and applications reside with data and applications of other companies
- Access to confidential data (intended or unintended) is possible through shared platforms, shared storage, and shared networks

- Multi-tenancy requires segmentation and isolation of networks, operating systems, and applications, and governance for regulatory compliance

Cloud Deployment Models

Narration

Let's look at the cloud deployment models, which include private, community, public, and hybrid.

NIST defines a private cloud infrastructure as one that is provisioned for exclusive use by a single organization, comprising multiple consumers—for example, business units. It can be owned, managed, and operated by the organization, a third party, or some combination of them, and it can exist on or off premises.

A community cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. For example, they may share a mission, security requirements, policies, or compliance considerations. A community cloud infrastructure can be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it can exist on or off premises.

A public cloud infrastructure is provisioned for open use by the public. It can be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Finally, a hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures that remain unique entities. These clouds are bound together by standardized or proprietary technology that enables data and application portability—for example, cloud bursting for load balancing between clouds. Cloud bursting is when an application that normally runs in one type of cloud environment, such as a private cloud, pulls resources from another cloud (including public ones) during periods of peak resource demand.

On Screen Text

Cloud Deployment Models

Let’s look at the cloud deployment models, which include: (1) Private, (2) Community, (3) Public, and (4) Hybrid.

Click each tab to learn more about the models.

Private Cloud

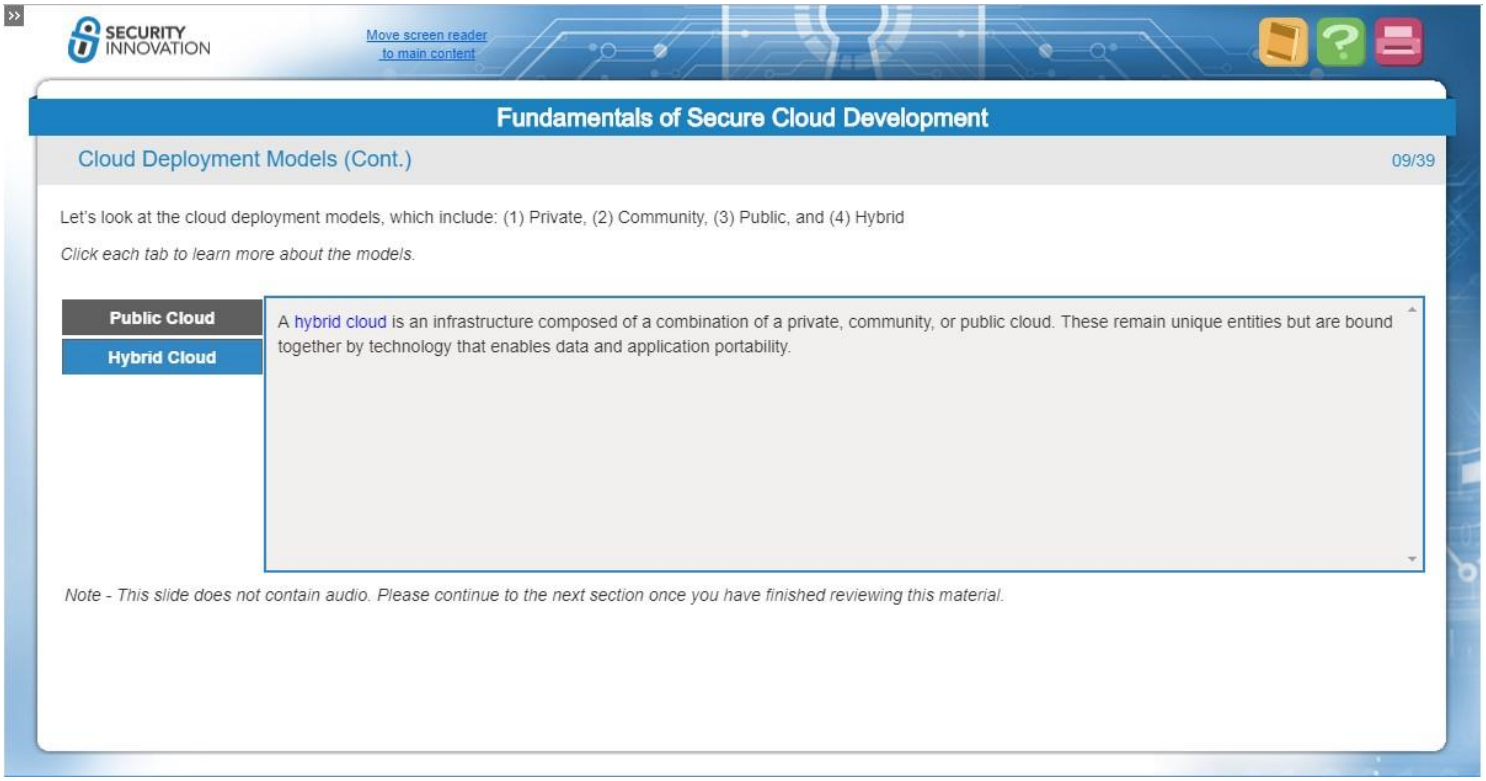
A private cloud is provisioned for exclusive use by a single organization comprising multiple consumers—for example, business units.

It can be owned, managed, and operated by the organization, a third party, or some combination of them, and it can exist on or off premises.

Community Cloud

A community cloud is an infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns.

Cloud Deployment Models (Cont.)



Narration

On Screen Text

Cloud Deployment Models (Cont.)

Let's look at the cloud deployment models, which include: (1) Private, (2) Community, (3) Public, and (4) Hybrid.

Click each tab to learn more about the models.

Public Cloud

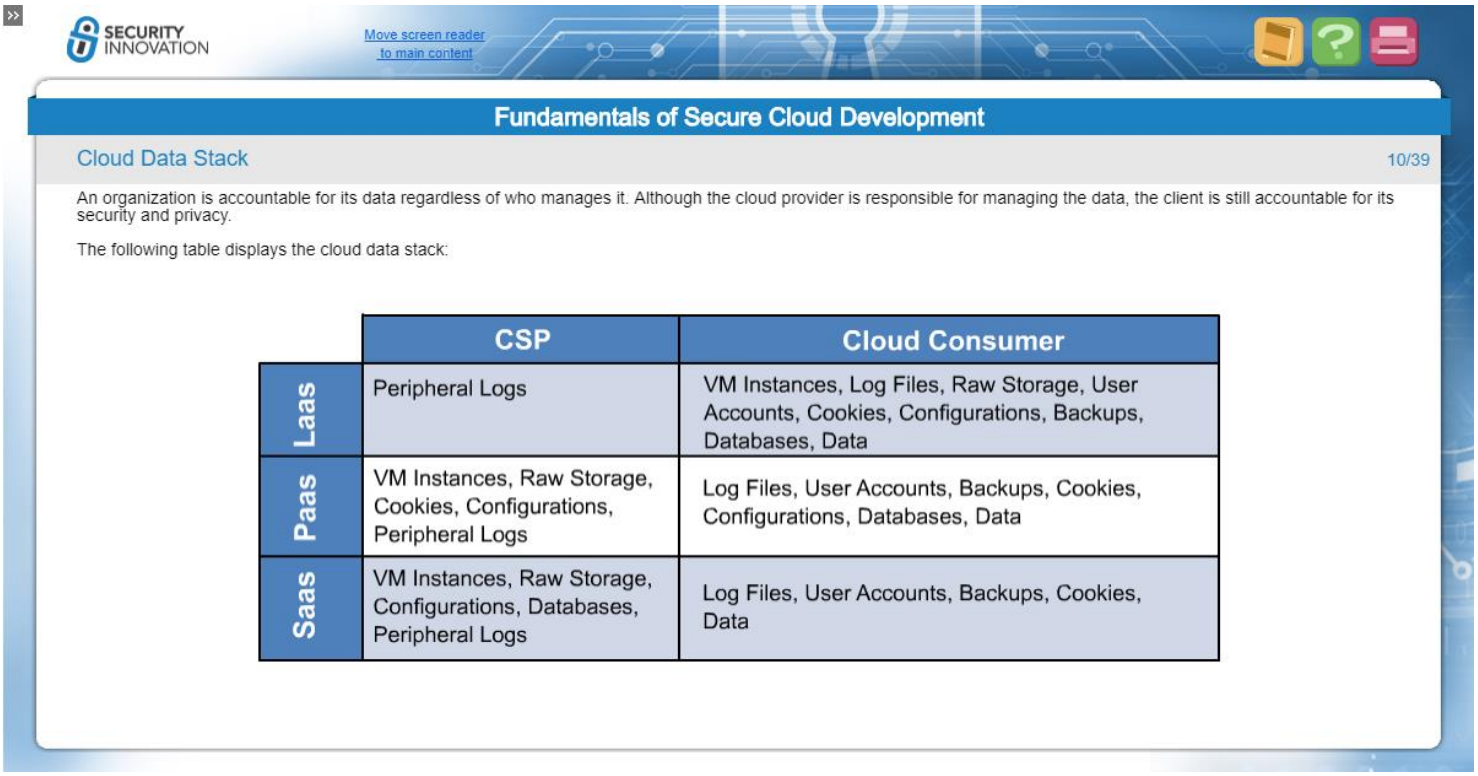
A public cloud is an infrastructure that is provisioned for open use by the public.

Hybrid Cloud

A hybrid cloud is an infrastructure composed of a combination of a private, community, or public cloud. These remain unique entities but are bound together by technology that enables data and application portability.

Note - This slide does not contain audio. Please continue to the next section once you have finished reviewing this material.

Cloud Data Stack



Narration

An organization is accountable for its data regardless of who manages it. Although the cloud provider is responsible for managing the data, the client is still accountable for its security and privacy.

The table on the screen shows the cloud data stack.

On Screen Text

Cloud Data Stack

An organization is accountable for its data regardless of who manages it. Although the cloud provider is responsible for managing the data, the client is still accountable for its security and privacy.

The following table displays the cloud data stack:

Narration

Various regulations require that organizations implement security controls and processes. Some examples are shown on the screen.

Most regulations require a security assessment on a regular basis. Many of these regulations require the use of data encryption for certain types of data and code reviews for applications that store, transmit, or process certain data.

On Screen Text

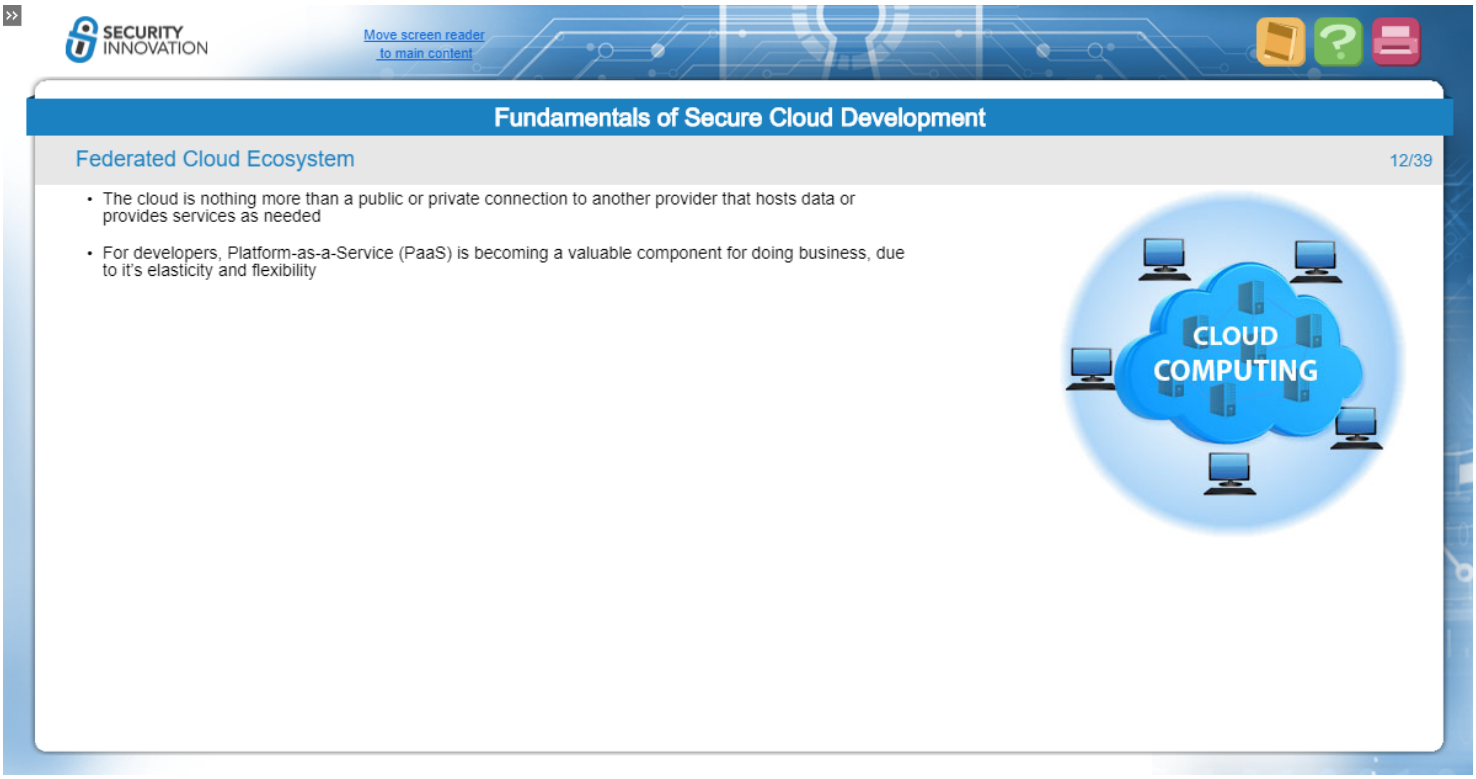
Regulatory Requirements and Application Security

Various regulations require that organizations implement security controls and processes. Here are some examples:

- PCI DSS
- HIPAA
- Sarbanes-Oxley
- NIST

Most regulations require a security assessment on a regular basis. Many of these regulations require the use of data encryption for certain types of data and code reviews for applications that store, transmit, or process certain data.

Federated Cloud Ecosystem



Narration

Federated cloud ecosystem is a term used to define the heterogeneous frameworks that constitute cloud services. The global distribution of cloud services accessible through the public Internet make up this ecosystem. Despite the vast reach of the cloud, security regulations prevent cloud services from dominating as a singular model.

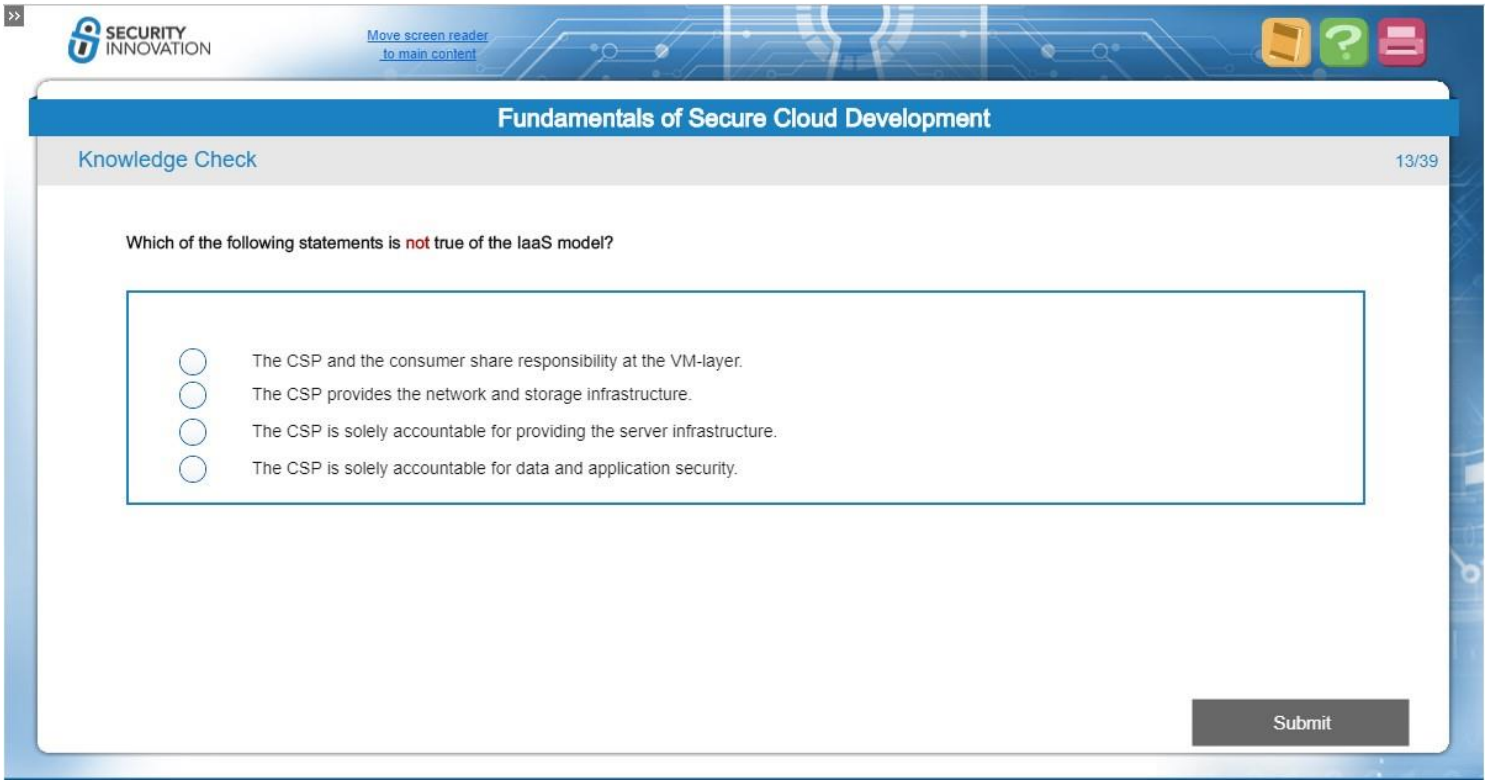
However, hybrid clouds allow companies to pick and choose the services they want to offload to the cloud and the services they want to keep in-house. This allows companies to customize their cloud solutions to fit their needs. The ability to create hybrid clouds free of vendor lock-in provides the flexibility and customization essential for those using cloud services.

On Screen Text

Federated Cloud Ecosystem

- The cloud is nothing more than a public or private connection to another provider that hosts data or provides services as needed
- For developers, Platform-as-a-Service (PaaS) is becoming a valuable component for doing business, due to its elasticity and flexibility

Knowledge Check



Narration

On Screen Text

Knowledge Check

Which of the following statements is not true of the IaaS model?

The CSP and the consumer share responsibility at the VM-layer

The CSP provides the network and storage infrastructure

The CSP is solely accountable for providing the server infrastructure

The CSP is solely accountable for data and application security

Module Summary

Narration

In this module, you learned the cloud computing characteristics, which include on demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. You learned about different service models, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). You also learned about various deployment models, which include private, community, public, and hybrid. Finally, you learned about various regulatory requirements related to cloud computing.

On Screen Text

Module Summary

In this module, you learned the cloud computing characteristics, which include on demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. You learned about different service models, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). You also learned about various deployment models, which include private, community, public, and hybrid. Finally, you learned about various regulatory requirements related to cloud computing.

Module Overview and Objectives

Narration

This module lists the risks and threats associated with cloud computing. It also introduces “Big Data” security risks that apply to cloud computing.

After completing this module, you will be able to identify the risks and threats associated with cloud computing. You will also be able to identify the “Big Data” security risks associated with cloud computing

On Screen Text

Module Overview and Objectives

This module lists the risks and threats associated with cloud computing. It also introduces “Big Data” security risks applicable for cloud computing.

Module Objectives:

- Identify the risks and threats associated with cloud computing
- Identify the “Big Data” security risks associated with cloud computing

Securing the Cloud

Narration

Cloud computing services can be accessed over any networked device, wired or wireless. These can include thin-clients, kiosks, desktop computers, laptops, computer tablets, and mobile smartphones.

With the technological advancement of virtualization, resources can be provisioned quickly and easily to scale up solutions and scale out resources as needed. However, all of these advancements present some significant security issues and risks.

The Cloud Security Alliance has developed a list of “Top Threats to Cloud Computing,” which you can download from their website. The threats include abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking, and unknown risk profile.

On Screen Text

Securing the Cloud

Cloud computing services can be accessed over any networked device, wired or wireless. These can include:

- Thin-clients
- Kiosks
- Desktop computers

- Laptops
- Computer tablets
- Mobile smartphones

With the technological advancement of virtualization, resources can be provisioned quickly and easily to scale up solutions and scale out resources as needed. However, all of these advancements present some significant security issues and risks.

While cloud applications are ultimately vulnerable to the full range of application threats as defined by OWASP and CWE, we will focus on those threats that cloud application developers are directly responsible for mitigating, such as:

- Abuse and nefarious use of cloud computing
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

Cloud “Big Data” Security Risks

Narration

The Cloud Security Alliance has published its “Expanded Top 10 Big Data Security and Privacy Challenges”. These challenges include several that are important to application developers.

In the following screens, we will examine those issues that can be partially mitigated by using secure development best practices.

On Screen Text

Cloud “Big Data” Security Risks

Recently, the cloud security alliance published its “Expanded Top 10 Big Data Security and Privacy Challenges”. These challenges include several that are important to application developers:

1. Secure computations in distributed programming frameworks

2. Security best practices for non-relational data stores

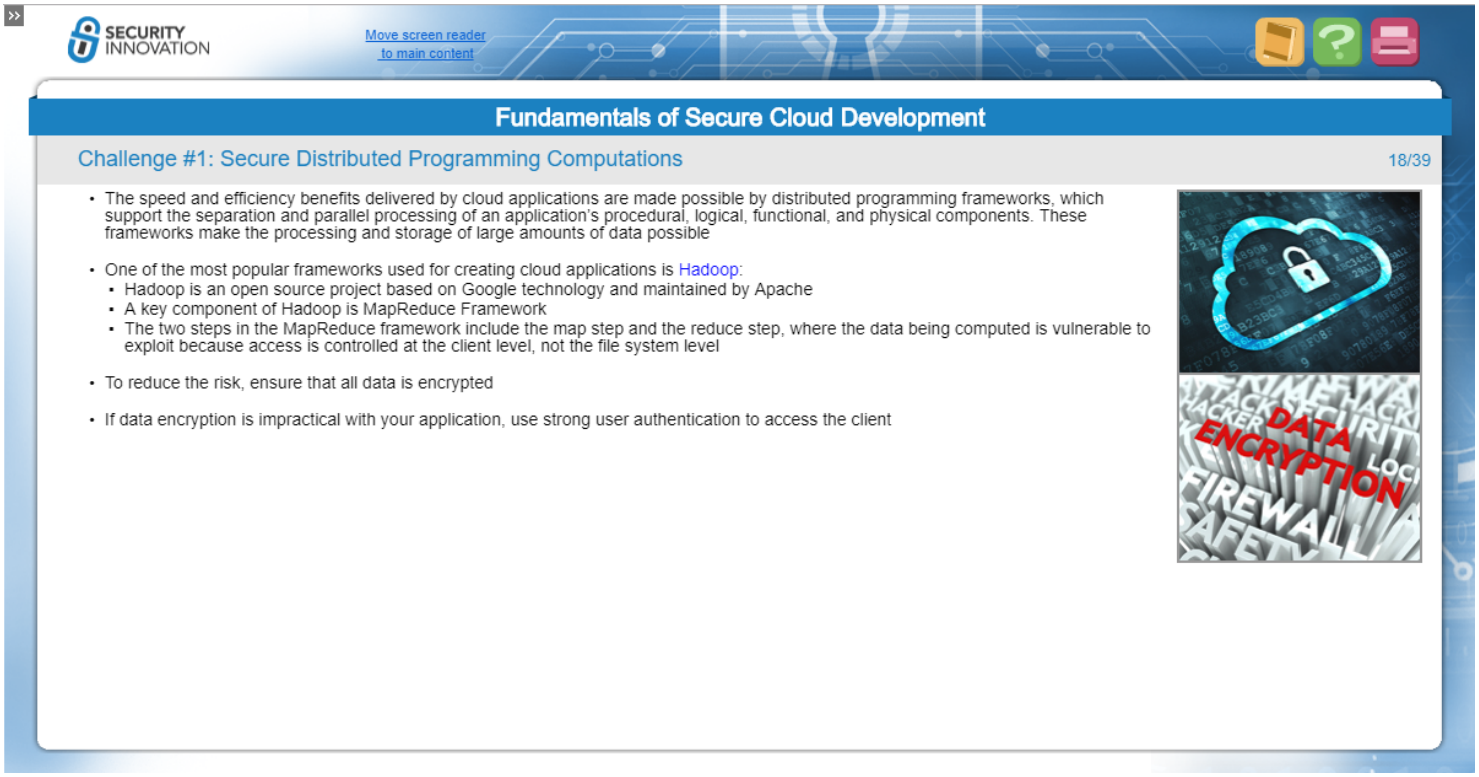
3. End-point input validation/filtering

4. Cryptographically enforced data centric security

5. Granular access control and audits

6. Data provenance

Challenge #1: Secure Distributed Programming Computations



Narration

The speed and efficiency delivered by cloud applications are made possible by distributed programming frameworks, which support the separation and parallel processing of an application's procedural, logical, functional, and physical components. These frameworks make the processing and storage of large amounts of data possible.

One of the most popular frameworks used for creating cloud applications is Hadoop. Hadoop is an open-source project based on Google technology and maintained by Apache.

A key component of Hadoop is MapReduce Framework.

There are two steps in the MapReduce framework: the map step and the reduce step, where the data being computed is vulnerable to exploit. Data is vulnerable because access is controlled at the client level, not the file system level.

To reduce the risk, ensure that all data is encrypted. If data encryption is impractical with your application, use strong user authentication to access the client.

On Screen Text

Challenge #1: Secure Distributed Programming Computations

- The speed and efficiency benefits delivered by cloud applications are made possible by distributed programming frameworks, which support the separation and parallel processing of an application's procedural, logical, functional, and physical components. These frameworks make the processing and storage of large amounts of data possible.

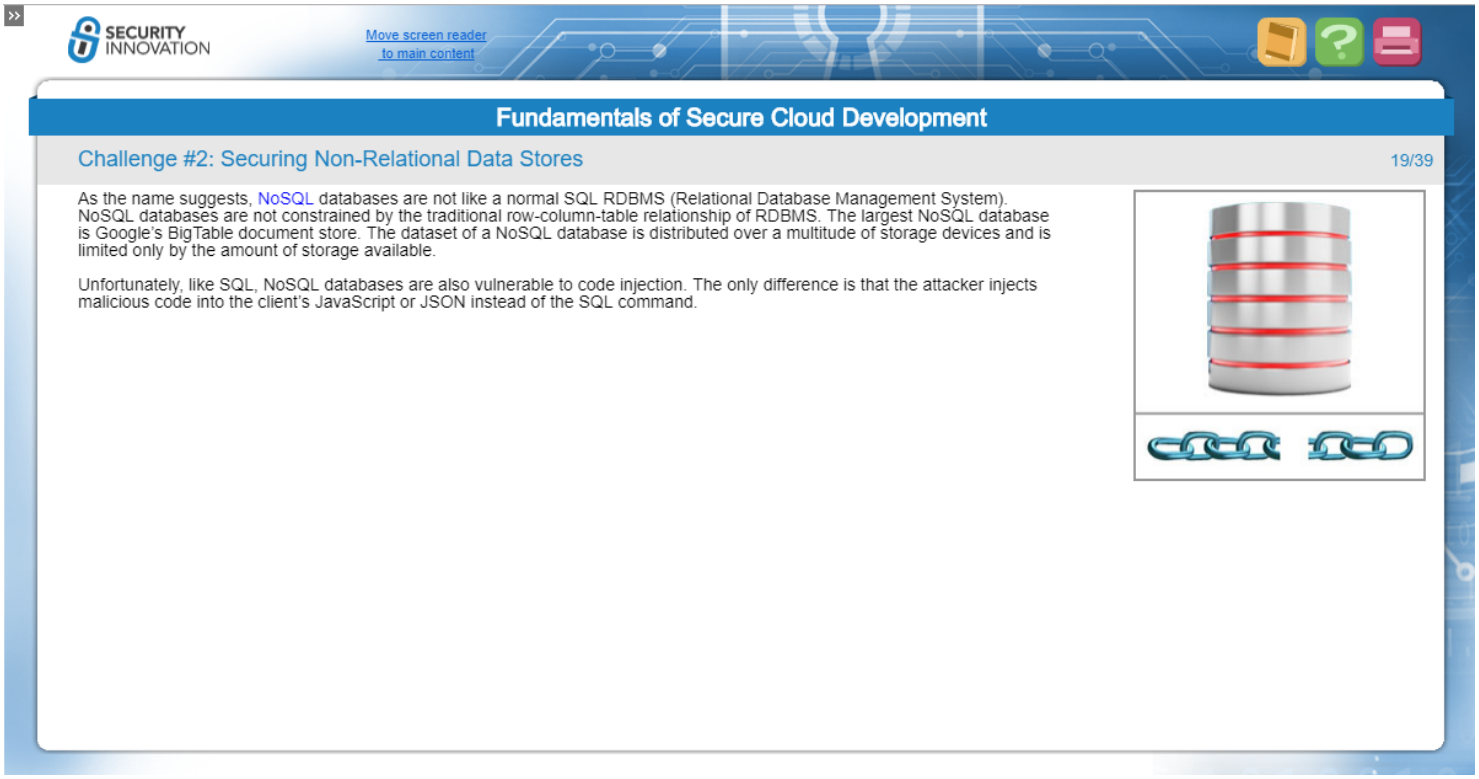
- One of the most popular frameworks used for creating cloud applications is Hadoop:

  - Hadoop is an open source project based on Google technology and maintained by Apache
  - A key component of Hadoop is MapReduce Framework
  - The two steps in the MapReduce framework include the map step and the reduce step, where the data being computed is vulnerable to exploit because access is controlled at the client level, not the file system level

- To reduce the risk, ensure that all data is encrypted

- If data encryption is impractical with your application, use strong user authentication to access the client

Challenge #2: Securing Non-Relational Data Stores



Narration

As the name suggests, NoSQL databases are not like a normal SQL RDBMS (Relational Database Management System). NoSQL databases are not constrained by the traditional row-column-table relationship of RDBMS. The largest NoSQL database is Google's BigTable document store. The dataset of a NoSQL database is distributed over a multitude of storage devices and is limited only by the amount of storage available.

Unfortunately, like SQL, NoSQL databases are vulnerable to code injection. The only difference is that the attacker injects malicious code into the client's JavaScript or JSON instead of the SQL command.

On Screen Text

Challenge #2: Securing Non-Relational Data Stores

As the name suggests, NoSQL databases are not like a normal SQL RDBMS (Relational Database Management System). NoSQL databases are not constrained by the traditional row-column-table relationship of RDBMS. The largest NoSQL database is Google's BigTable document store. The dataset of a NoSQL database is distributed over a multitude of storage devices and is limited only by the amount of storage available.

Unfortunately, like SQL, NoSQL databases are also vulnerable to code injection. The only difference is that the attacker injects malicious code into the client's JavaScript or JSON instead of the SQL command.

Challenge #3: End-Point Input Validation/Filtering

Narration

Your application's input validation and filtering capabilities must be designed to avoid the risks associated with weak or non-existent input validation.

To accomplish this task, you need to properly validate all input and ensure that input validation routines are coded correctly. Conduct thorough code analysis—including static code analysis using tools, such as Fortify and Appscan and manual code reviews to ensure that no vulnerabilities were missed by the static analysis tools. Be sure to remediate all discovered vulnerabilities before deployment.

On Screen Text

Challenge #3: End-Point Input Validation/Filtering

Your application's input validation and filtering capabilities must be designed to properly handle every input in a secure fashion.

- Properly validate and filter all input and reject incorrect values

- Conduct thorough static code analysis using tools, such as Fortify and Appscan, followed by manual code reviews to ensure that no input validation vulnerabilities were missed by the static analysis tools
- Remediate all input validation vulnerabilities before deployment

Challenge #4: Cryptographically Enforced Data-Centric Security

Narration

PKI X.509 certificates can be populated with metadata to specify their usage. For example, you can use metadata in a X.509 certificate for positively identifying an end point or a user.

Attribute-Based Encryption (ABE) and Homomorphic Encryption technologies will help secure Big Data offerings in the future. ABE inserts attributes into the public-private keys allowing for enhanced logical access controls, while homomorphic encryption allows for computations to be performed on ciphertext, negating the need for encrypted data to be decrypted for computations.

On Screen Text

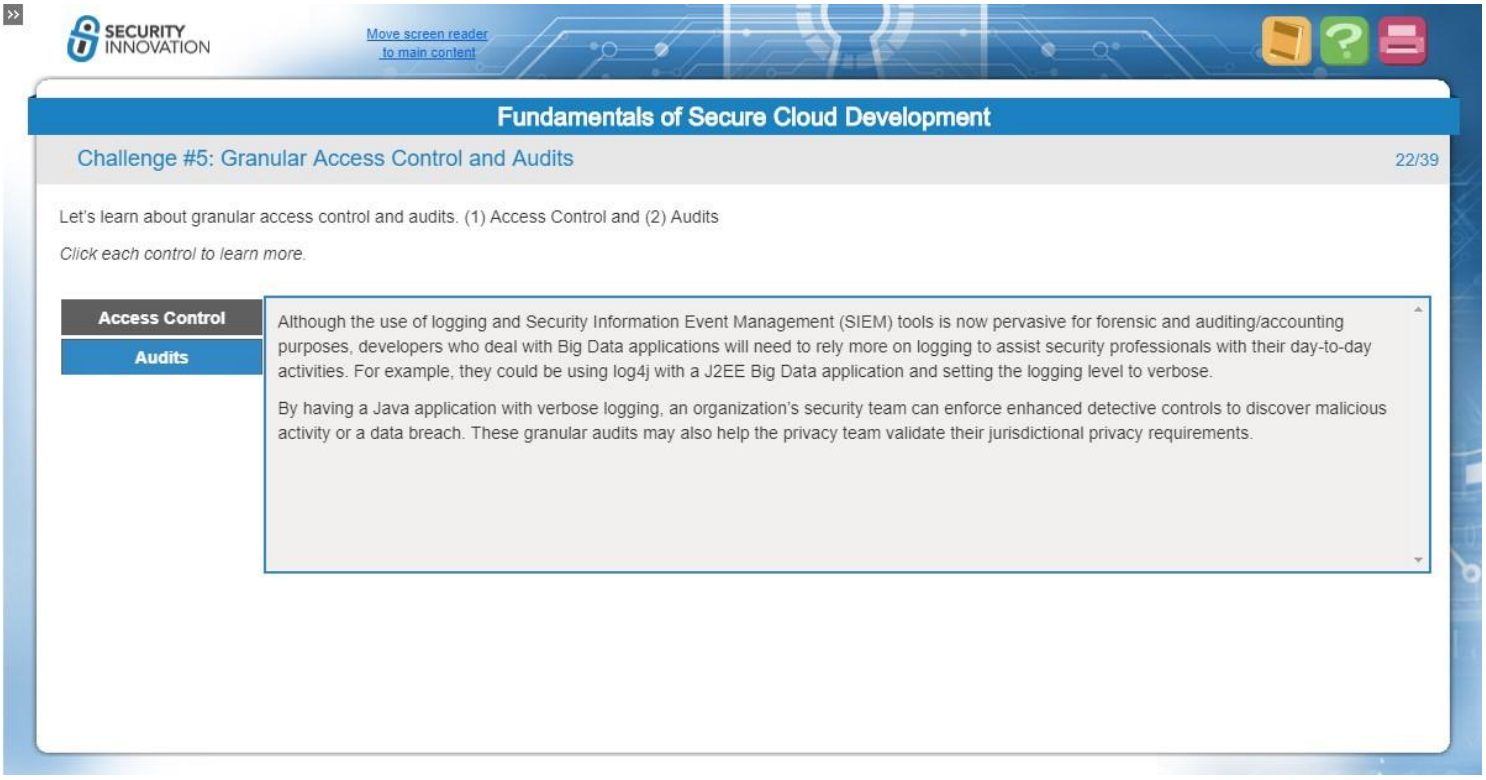
Challenge #4: Cryptographically Enforced Data-Centric Security

Public-Key Infrastructure (PKI) solutions for transport-layer protection are the optimal safeguards—for example, digital certificates that are distributed via Transport-Layer Security (TLS).

Attribute-Based Encryption (ABE) and Homomorphic encryption technologies will help secure Big Data offerings in the future.

ABE inserts attributes into the public-private keys, allowing for enhanced logical access controls, while homomorphic encryption allows for computations to be performed on ciphertext, negating the need for encrypted data to be decrypted for computations.

Challenge #5: Granular Access Control and Audits



Narration

Let's learn about granular access control and audits.

Most organizations currently use Role-Based Access Controls (RBAC) in applications and networks for logical access controls.

Attribute-Based-Access-Control (ABAC) is a more granular access control model. As described by the NIST, it is distinguishable from RBAC because it controls access to objects by evaluating rules against the attributes of the entities' (subject's and object's) actions and the environment relevant to a request.

Developers who deal with Big Data applications will need to rely more on logging and system lockouts after certain login attempts, inactivity timeouts, and session terminations to assist security professionals with their day-to-day activities.

Click each control to learn more.

On Screen Text

Challenge #5: Granular Access Control and Audits

Let’s learn about granular access control and audits.

(1) Access Control and (2) Audits

Click each control to learn more.

Access Control

Most organizations currently use Role-Based Access Controls (RBAC) within applications and networks for logical access controls.

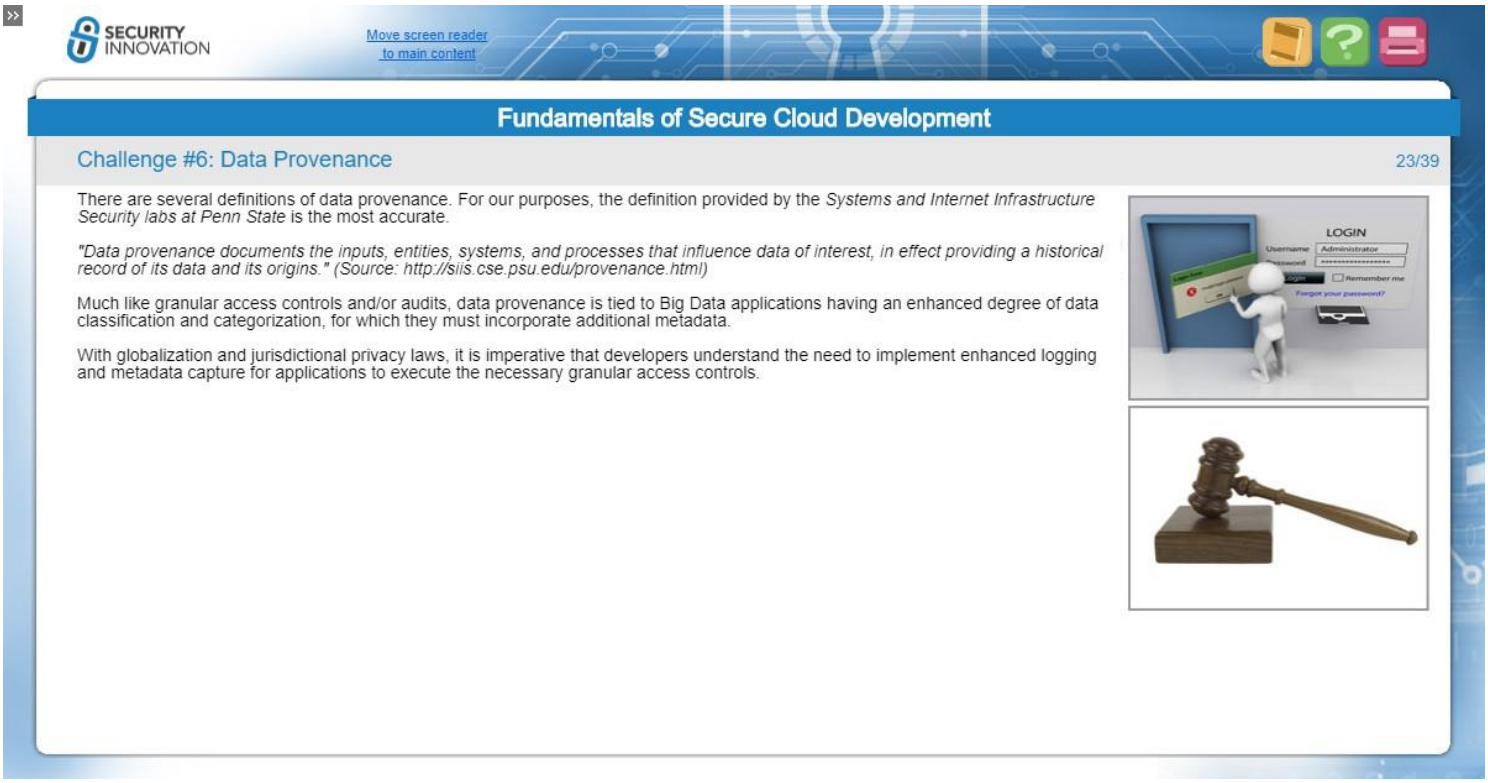
Attribute-Based Access Control (ABAC) is a more granular access control model. As described by the NIST, it is distinguishable from RBAC because it controls access to objects by evaluating rules against the attributes of the entities’ (subject’s and object’s) actions and the environment relevant to a request. Attributes may be considered characteristics of anything that may be defined and to which a value may be assigned.

Audits

Although the use of logging and Security Information Event Management (SIEM) tools is now pervasive for forensic and auditing/accounting purposes, developers who deal with Big Data applications will need to rely more on logging to assist security professionals with their day-to-day activities. For example, they could be using log4j with a J2EE Big Data application and setting the logging level to verbose.

By having a Java application with verbose logging, an organization’s security team can enforce enhanced detective controls to discover malicious activity or a data breach. These granular audits may also help the privacy team validate their jurisdictional privacy requirements.

Challenge #6: Data Provenance



Narration

Data provenance documents the inputs, entities, systems, and processes that influence data of interest, in effect providing a historical record of the data and its origins.

Much like granular access controls and audits, data provenance is tied to Big Data applications having an enhanced degree of data classification and categorization, for which they must incorporate additional metadata.

With globalization and jurisdictional privacy laws, it is imperative that developers understand the need to implement enhanced logging and metadata capture for applications to execute the necessary granular access controls.

On Screen Text

Challenge #6: Data Provenance

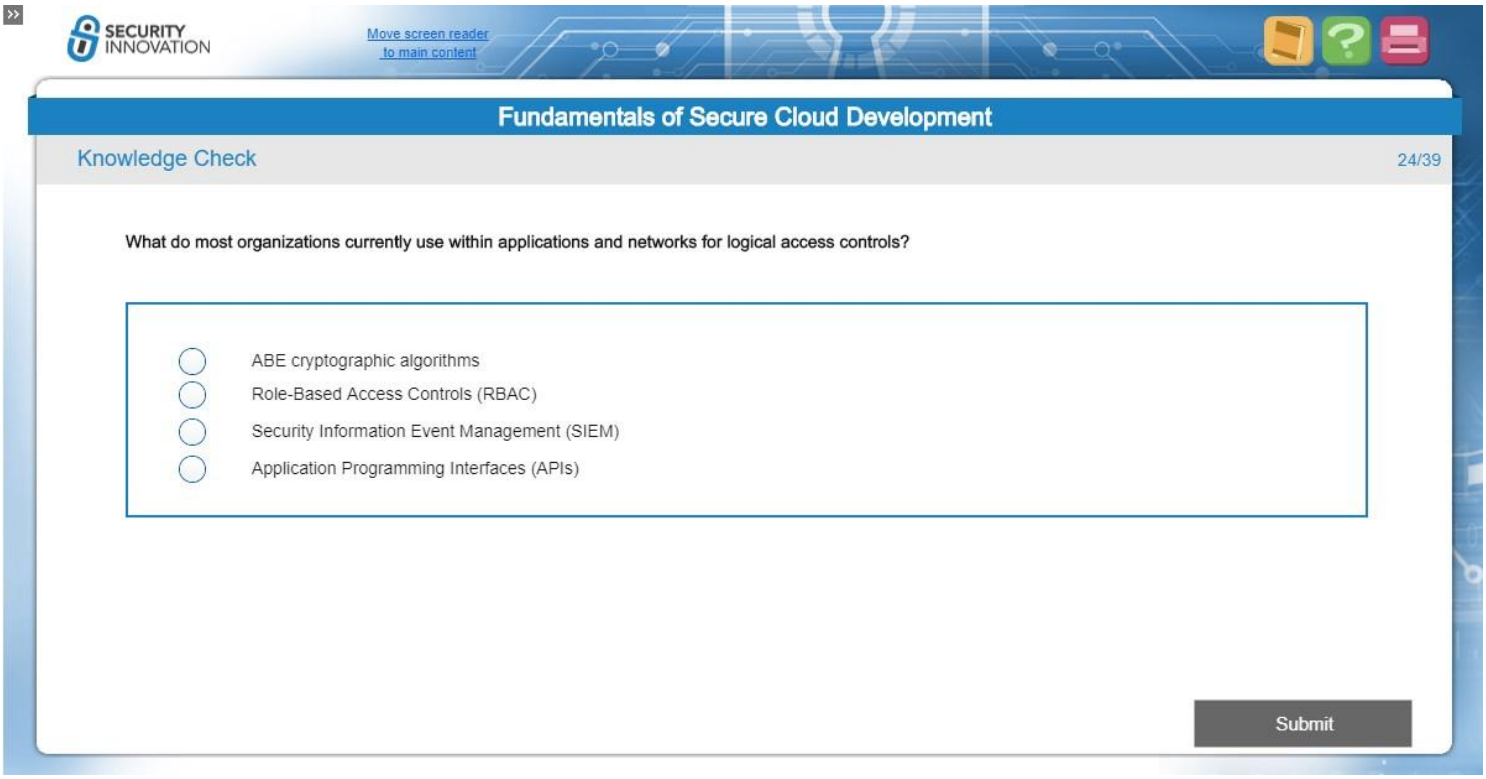
There are several definitions of data provenance. For our purposes, the definition provided by the *Systems and Internet Infrastructure Security labs at Penn State* is the most accurate.

"Data provenance documents the inputs, entities, systems, and processes that influence data of interest, in effect providing a historical record of its data and its origins." (Source: http://siis.cse.psu.edu/provenance.html)

Much like granular access controls and/or audits, data provenance is tied to Big Data applications having an enhanced degree of data classification and categorization, for which they must incorporate additional metadata.

With globalization and jurisdictional privacy laws, it is imperative that developers understand the need to implement enhanced logging and metadata capture for applications to execute the necessary granular access controls.

Knowledge Check



Narration

On Screen Text

Knowledge Check

What do most organizations currently use within applications and networks for logical access controls?

ABE cryptographic algorithms

Role-Based Access Controls (RBAC)

Security Information Event Management (SIEM)

Application Programming Interfaces (APIs)

Module Summary

Narration

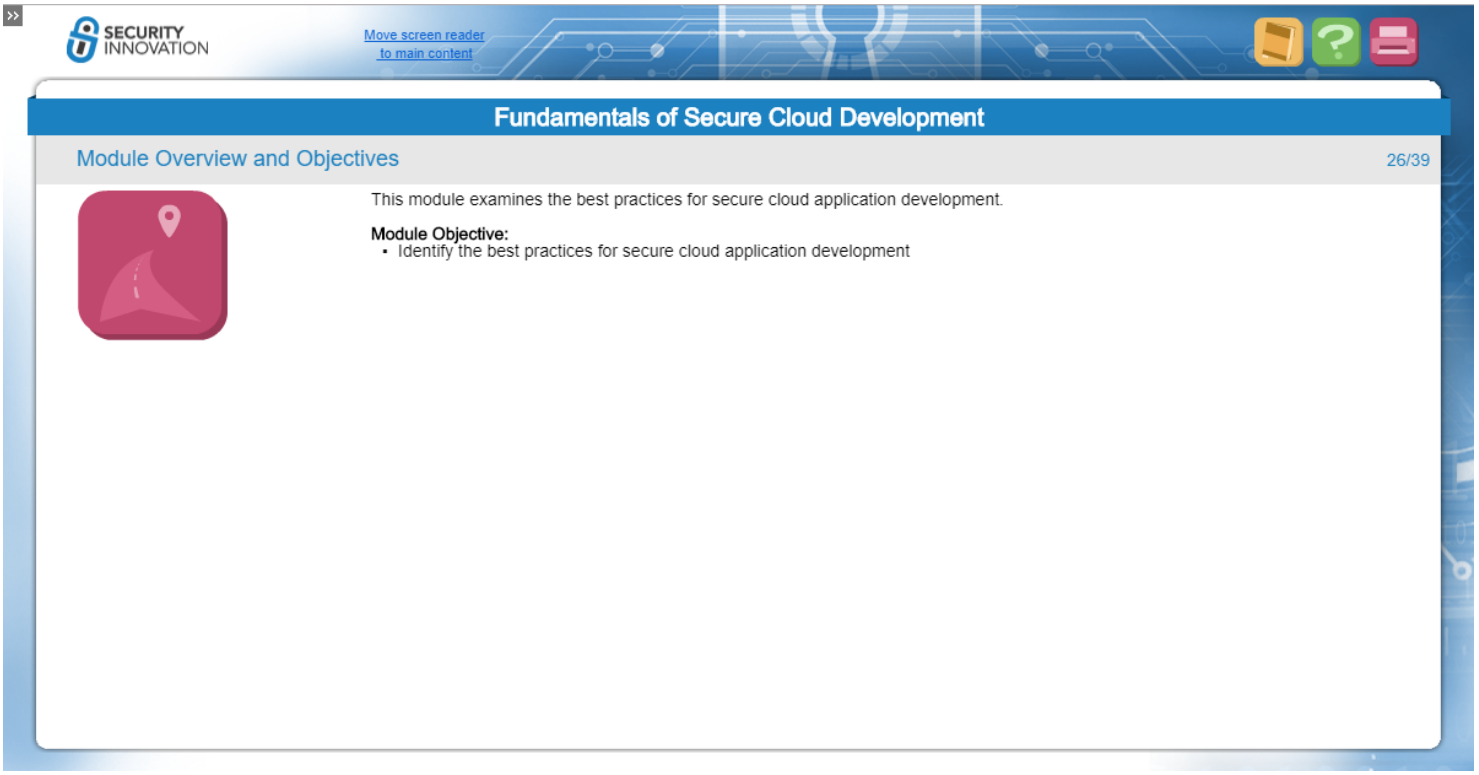
In this module, you learned about the risks and threats associated with cloud computing. You also learned about “Big Data” security risks that are applicable for cloud computing.

On Screen Text

Module Summary

In this module, you learned about the risks and threats associated with cloud computing. You also learned about “Big Data” security risks that are applicable for cloud computing.

Module Overview and Objectives



Narration

This module examines the best practices for secure cloud application development.

After completing this module, you will be able to identify the best practices for secure cloud application development.

On Screen Text

Module Overview and Objectives

This module examines the best practices for secure cloud application development.

Module Objective:

- Identify the best practices for secure cloud application development

Secure Cloud Application Development Best Practices

Narration

Let’s look at some common best practices for developing secure cloud applications. You should use these security best practices and guidelines throughout the design, development, and deployment phases of your software development process.

You need to identify security objectives to understand your key security issues and scenarios, and apply security design guidelines to avoid common security design mistakes and learn from past vulnerabilities.

You also need to conduct security architecture and design reviews to identify security problems that can have a multiplier effect in later phases of development, and create threat models to identify threats, attacks, vulnerabilities, and countermeasures.

You perform security code reviews and penetration tests to uncover vulnerabilities during development and in deployment.

Finally, you need to conduct security deployment reviews to ensure that configuration and deployment problems are found before your application enters production.

On Screen Text

Secure Cloud Application Development Best Practices

This list identifies common best practices for developing secure cloud applications. You should use these security best practices and guidelines throughout the design, development, and deployment phases of your software development process:

- Identify security objectives to understand your key security issues and scenarios
- Apply security design guidelines to avoid common security design mistakes and learn from past vulnerabilities
- Conduct security architecture and design reviews to identify security problems that can have a multiplier effect in later phases of development
- Create threat models to identify threats, attacks, vulnerabilities, and countermeasures
- Perform security code reviews and penetration tests to uncover vulnerabilities during development and in deployment
- Finally, conduct security deployment reviews to ensure that configuration and deployment problems are found before your application enters production

The CIA Triad: Protecting Customer's Assets

Narration

The CIA triad refers to the three principles of information security; to keep sensitive customer and corporate information secure, organizations need to preserve the confidentiality, integrity, and availability of that information. Only by maintaining these aspects of their information can organizations successfully engage in commercial activities. Loss of one or more of these attributes can threaten the existence of even the largest corporate entities.

Click each principle to learn more.

On Screen Text

The CIA Triad: Protecting Customer's Assets

The CIA triad refers to the three principles of information security; to keep sensitive customer and corporate information secure, organizations need to preserve the confidentiality, integrity, and availability of that information. Only by maintaining these aspects of their information can organizations successfully engage in commercial activities. Loss of one or more of these attributes can threaten the existence of even the largest corporate entities.

The principles are: (1) Confidentiality, (2) Integrity, and (3) Availability.

Click each principle to learn more.

Confidentiality

Confidentiality is achieved by limiting information access and disclosure to only authorized users and preventing access by or disclosure to unauthorized users.

Confidentiality requires:

- Authentication - For authenticating, ask the users who they are and if they can prove it with something they know, something they have, or something they are
- Access Controls - Access controls limit access to resources on a ‘need-to-know’ basis. This is generally implemented as user privilege levels

Integrity

Information integrity means that the data and the system can only be modified by authorized individuals. Integrity is achieved by:

- Ensuring the trustworthiness of information resources
- Authenticating entities and data origin points

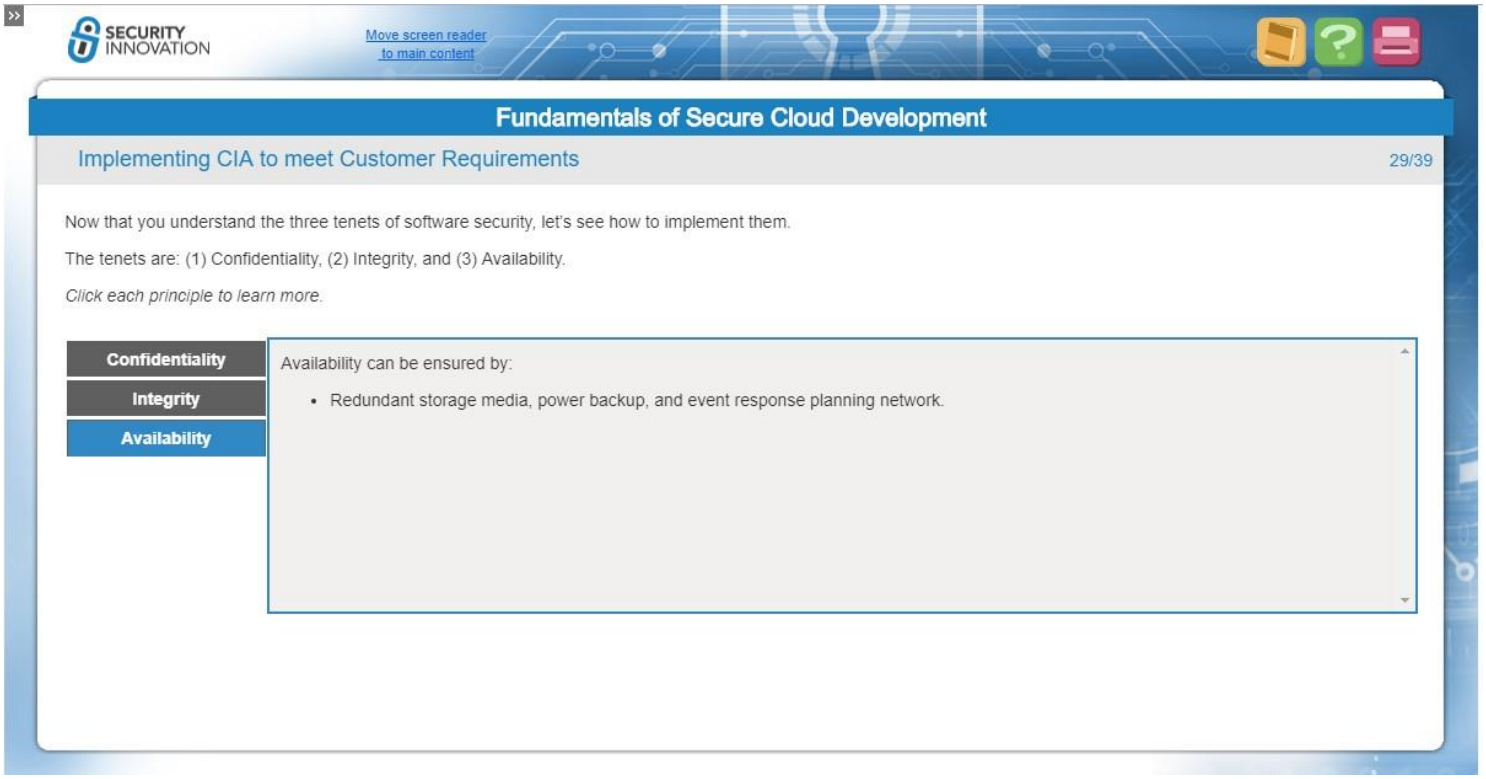
Integrity requires that data entered into our systems is correct and valid and has not been changed inappropriately, either deliberately or accidentally.

Availability

Availability is reliable access to system resources. Availability requires:

- Resistance to denial-of-service attacks
- Component (hardware and software) redundancy
- Fault-tolerant and failure-tolerant software

Implementing CIA to meet Customer Requirements



Narration

Now that you understand the three tenets of software security, let's see how to implement them.

You achieve confidentiality primarily through encryption and access control mechanisms. Limit data to intended users only, and protect the data in transit and at rest. In many cases, integrity is achieved through digital signatures. This allows you to not only validate the data, but also to check whether the data has been changed or modified in transit, or on the disk. In addition, you can also determine if the data originated from the right user.

Availability is probably the most challenging aspect for any company. You can build software controls to mitigate confidentiality and integrity risks. However, for availability, you need passive and proactive protection for data, redundant disks, machines, power, and network.

Click each principle to learn more.

On Screen Text

Implementing CIA to meet Customer Requirements

Now that you understand the three tenets of software security, let's see how to implement them.

The tenets are: (1) Confidentiality, (2) Integrity, and (3) Availability.

Click each principle to learn more.

Confidentiality

Confidentiality can be ensured by encryption and access control mechanisms:

- Limiting data to intended users
- Protecting data in transit and at rest

Integrity

Integrity can be achieved by using digital signatures:

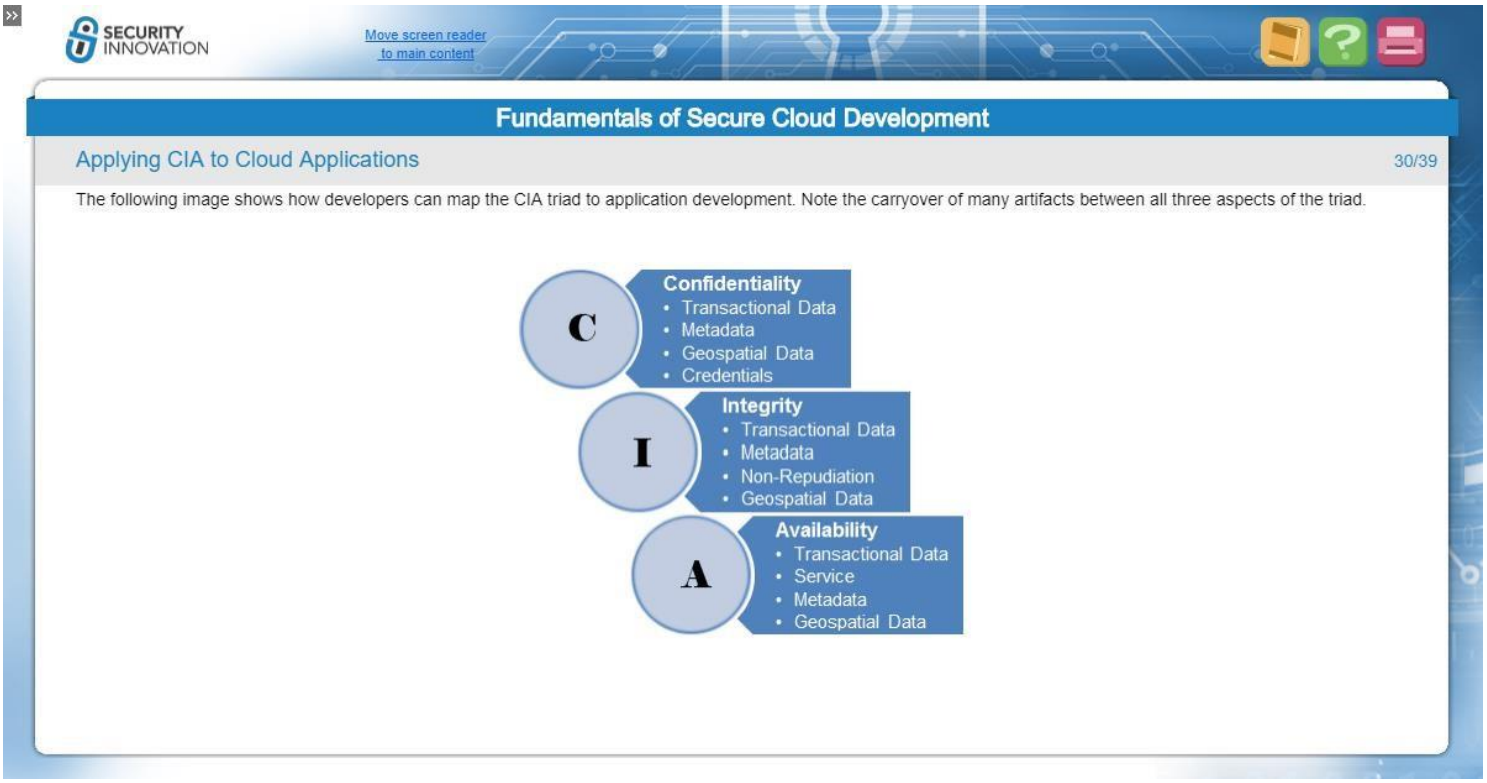
- They help ensure that messages and documents are not tampered with throughout their lifetime

Availability

Availability can be ensured by:

- Redundant storage media, power backup, and event response planning network

Applying CIA to Cloud Applications



Narration

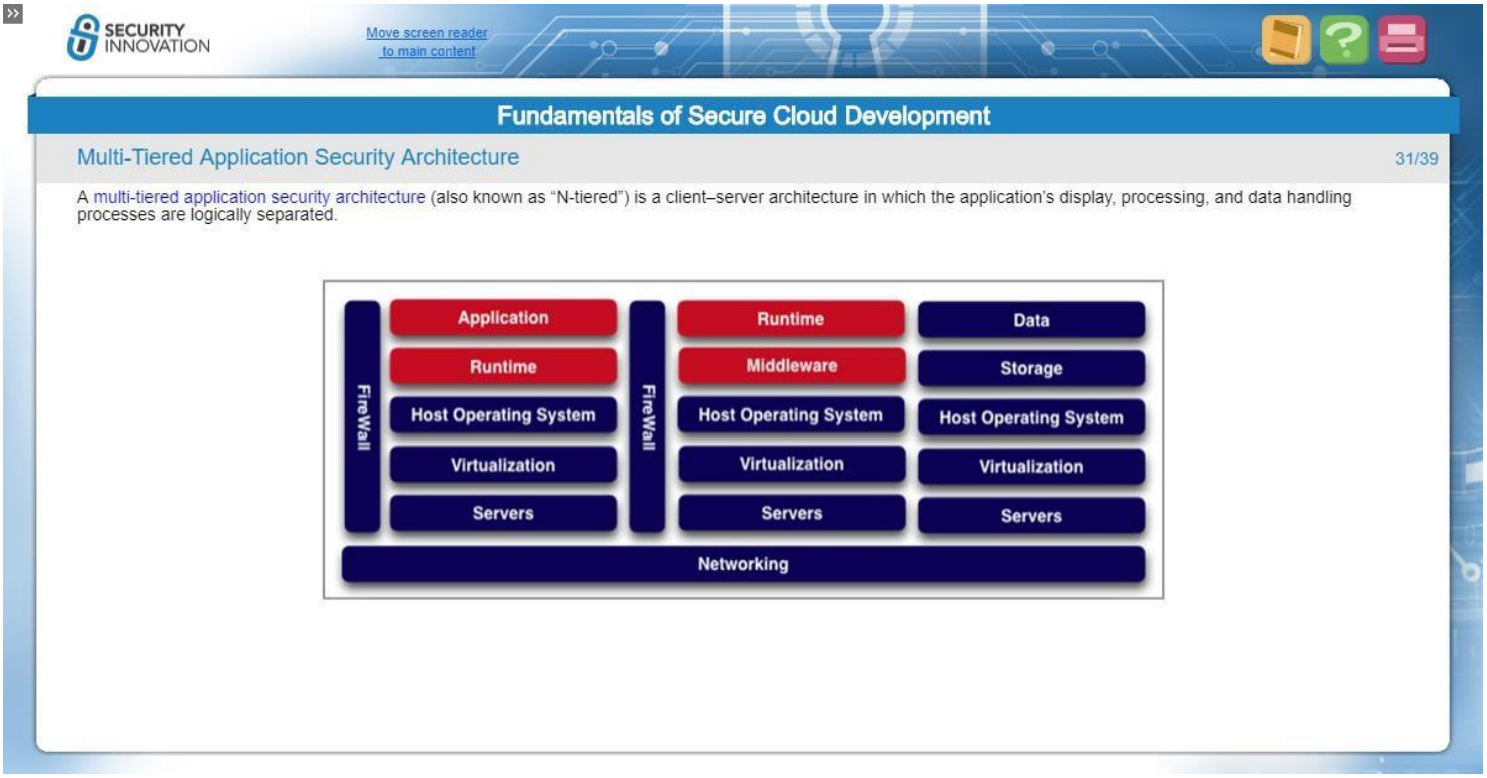
The image on the screen shows how developers can map the CIA triad to application development. Note the carryover of many artifacts between all three aspects of the triad.

On Screen Text

Applying CIA to Cloud Applications

The following image shows how developers can map the CIA triad to application development. Note the carryover of many artifacts between all three aspects of the triad.

Multi-Tiered Application Security



Narration

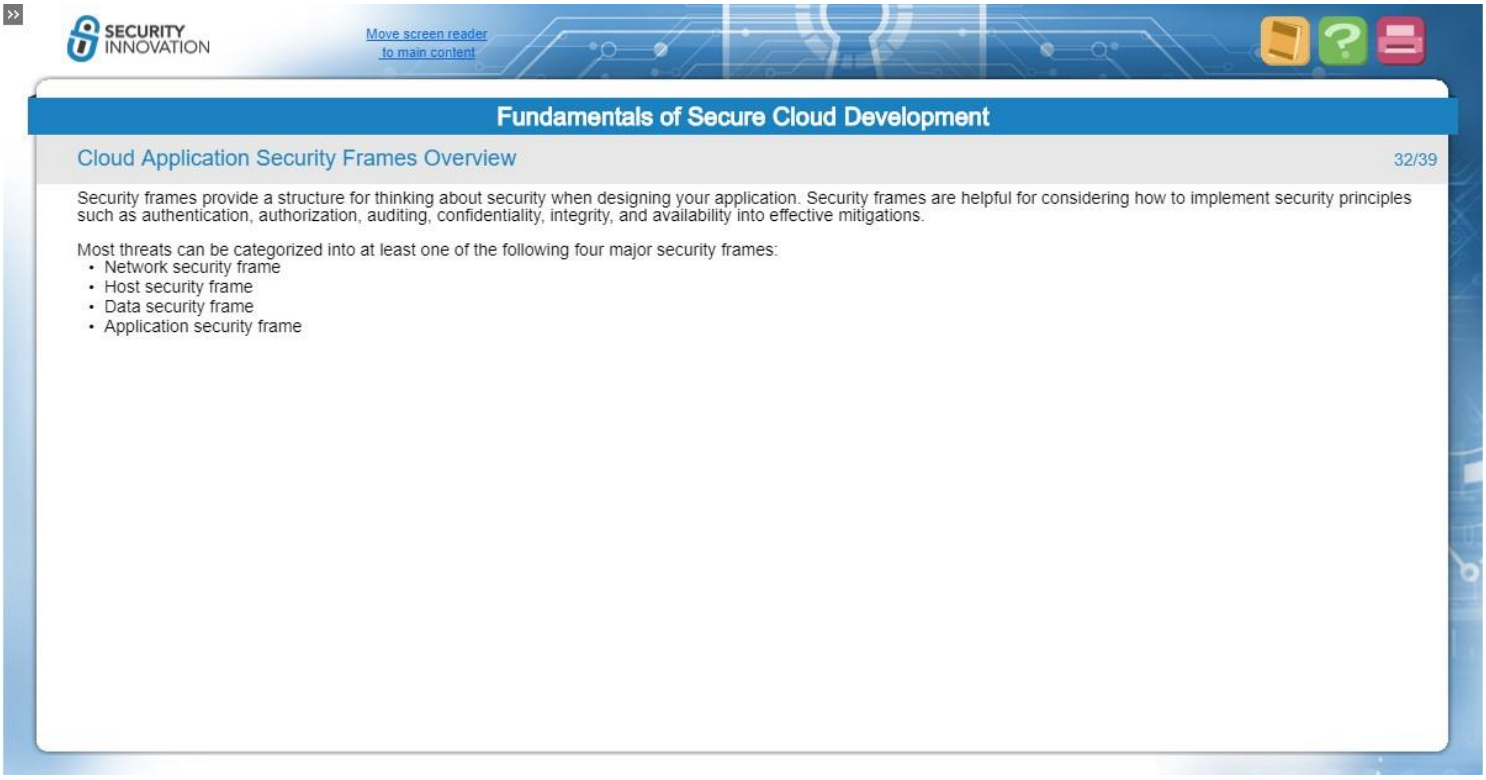
A multi-tiered application security architecture (also known as “N-tiered”) is a client–server architecture in which the application’s display, processing, and data handling processes are logically separated. When applied to cloud applications, this model provides developers with a tool to create different security mitigations for the front-end of the application, which is exposed to users and dependent on the host web server’s security services, and the back-end of the application, which is hosted behind additional levels.

On Screen Text

Multi-Tiered Application Security Architecture

A multi-tiered application security architecture (also known as “N-tiered”) is a client–server architecture in which the application’s display, processing, and data handling processes are logically separated.

Cloud Application Security Frames Overview



Narration

Security frames provide a structure for thinking about security when designing your application. Security frames are helpful for considering how to implement security principles, such as authentication, authorization, auditing, confidentiality, integrity, and availability into effective mitigations.

Most threats can be categorized into at least one of four major security frames: network, host, data, or application.

All of these frames can be applied to cloud applications. However, in this course, we focus on the application security frame, for which developers have the primary responsibility.

On Screen Text

Cloud Application Security Frames Overview

Security frames provide a structure for thinking about security when designing your application. Security frames are helpful for considering how to implement security principles such as authentication, authorization, auditing, confidentiality, integrity, and availability into effective mitigations.

Most threats can be categorized into at least one of the following four major security frames:

- Network security frame
- Host security frame
- Data security frame
- Application security frame

Cloud Application Security Frames Overview (Cont.)

Narration

Cloud application security design guidelines are categorized in a security frame, which describes the areas where poor design can cause security vulnerabilities.

The security frame categorizes common mistakes in a cloud application. For each of the categories, you can identify examples of problems that can cause an attack.

The categories are: input/data validation, authentication, authorization, configuration management, sensitive data, cryptography, exception management, and auditing and logging.

Click each category to learn more.

On Screen Text

Cloud Application Security Frames Overview (Cont.)

Cloud application security design guidelines are categorized in a security frame, which describes the areas where poor design can cause security vulnerabilities.

The security frame categorizes common mistakes observed in a cloud application. For each of the categories, you can identify examples of problems that can cause an attack.

The categories are: (1) Input/Data Validation, (2) Authentication, (3) Authorization, (4) Configuration Management, (5) Sensitive Data, (6) Cryptography, (7) Exception Management, and (8) Auditing and Logging.

Click each category to learn more.

Input/Data Validation

Improperly implemented input/data validation can lead to insertion of malicious strings in UIs or public APIs. Threats include command execution, cross-site scripting (XSS), SQL injection, and buffer overflow attacks. Results can range from information disclosure to elevation of privilege and arbitrary code execution.

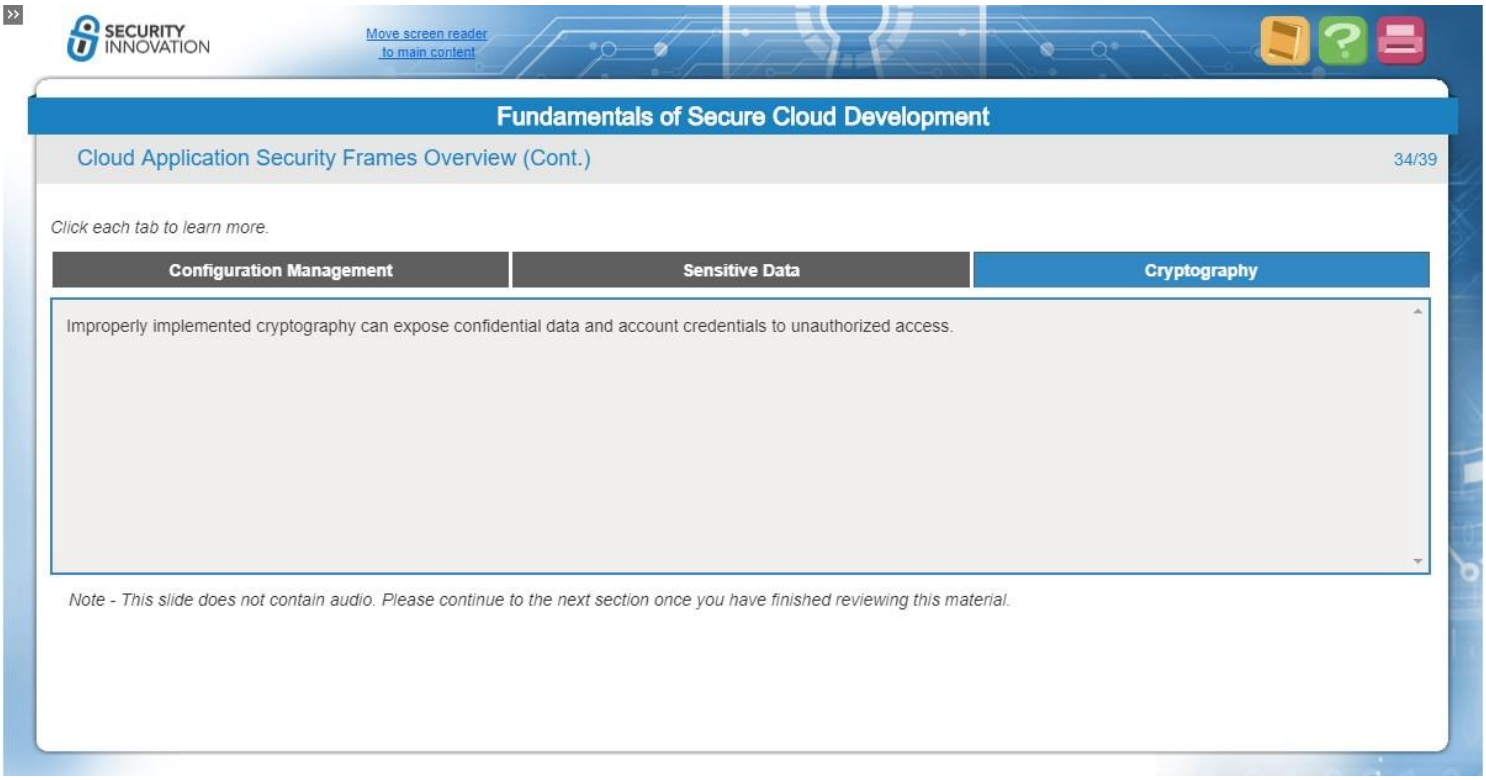
Authentication

Improperly implemented or weak authentication mechanisms can lead to identity spoofing, password cracking, elevation of privileges, and unauthorized access.

Authorization

Improperly implemented or weak authorization mechanisms can result in unauthorized access to confidential or restricted data, data tampering, and execution of unauthorized operations.

Cloud Application Security Frames Overview (Cont.)



Narration

On Screen Text

Cloud Application Security Frames Overview (Cont.)

Click each category to learn more.

Configuration Management

Improper configuration management can result in an attacker gaining access to administration interfaces, user accounts, and account profiles, and gaining the ability to change configuration data.

Sensitive Data

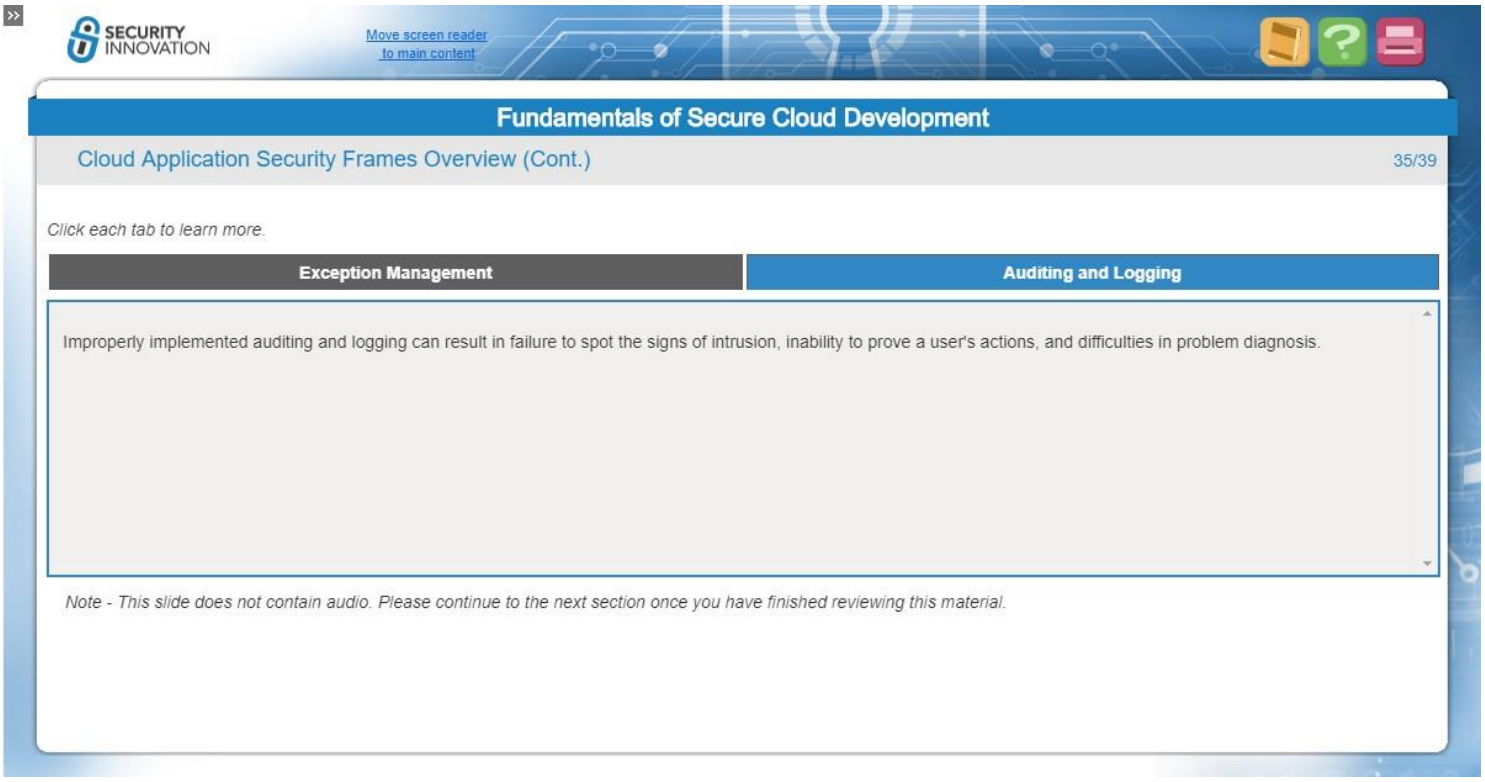
Sensitive data that is not properly secured can result in confidential information disclosure and data tampering.

Cryptography

Improperly implemented cryptography can expose confidential data and account credentials to unauthorized access.

Note - This slide does not contain audio. Please continue to the next section once you have finished reviewing this material.

Cloud Application Security Frames Overview (Cont.)



Narration

On Screen Text

Cloud Application Security Frames Overview (Cont.)

Click each category to learn more.

Exception Management

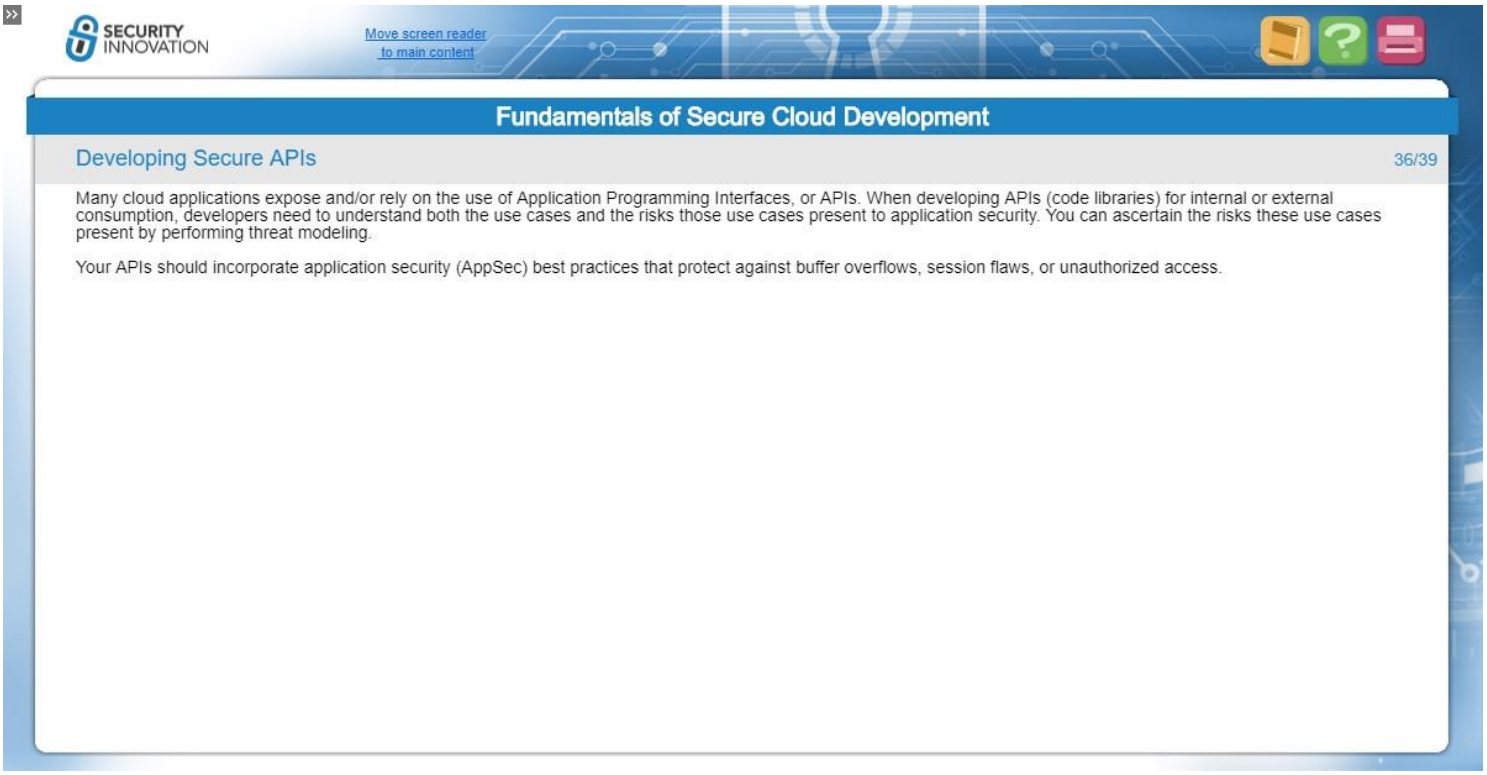
Improperly implemented exception management can lead to denial of service and disclosure of sensitive system-level details.

Auditing and Logging

Improperly implemented auditing and logging can result in failure to spot the signs of intrusion, inability to prove a user's actions, and difficulties in problem diagnosis.

Note - This slide does not contain audio. Please continue to the next section once you have finished reviewing this material.

Developing Secure APIs



Narration

Many cloud applications expose and/or rely on the use of Application Programming Interfaces, or APIs. Think of how an attacker might use your API and what threats may be present.

When developing APIs (code libraries) for internal or external consumption, developers need to understand both the use cases and the risks those use cases present to application security. You can ascertain the risks these use cases present by performing threat modeling.

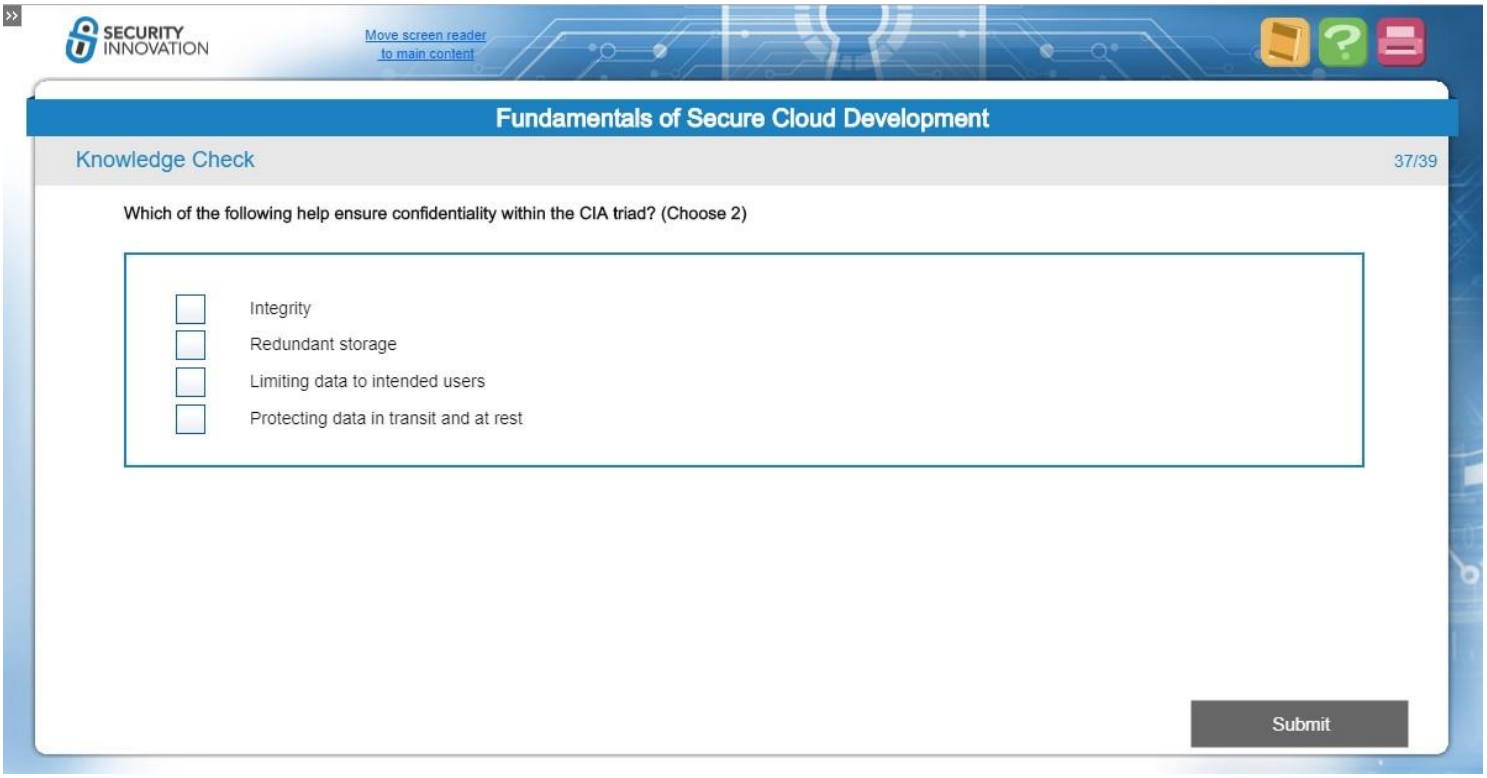
On Screen Text

Developing Secure APIs

Many cloud applications expose and/or rely on the use of Application Programming Interfaces, or APIs. When developing APIs (code libraries) for internal or external consumption, developers need to understand both the use cases and the risks those use cases present to application security. You can ascertain the risks these use cases present by performing threat modeling.

Your APIs should incorporate application security (AppSec) best practices that protect against buffer overflows, session flaws, or unauthorized access.

Knowledge Check



Narration

On Screen Text

Knowledge Check

Which of the following help ensure confidentiality within the CIA triad? (Choose 2)

Integrity

Redundant storage

Limiting data to intended users

Protecting data in transit and at rest

Module Summary

Narration

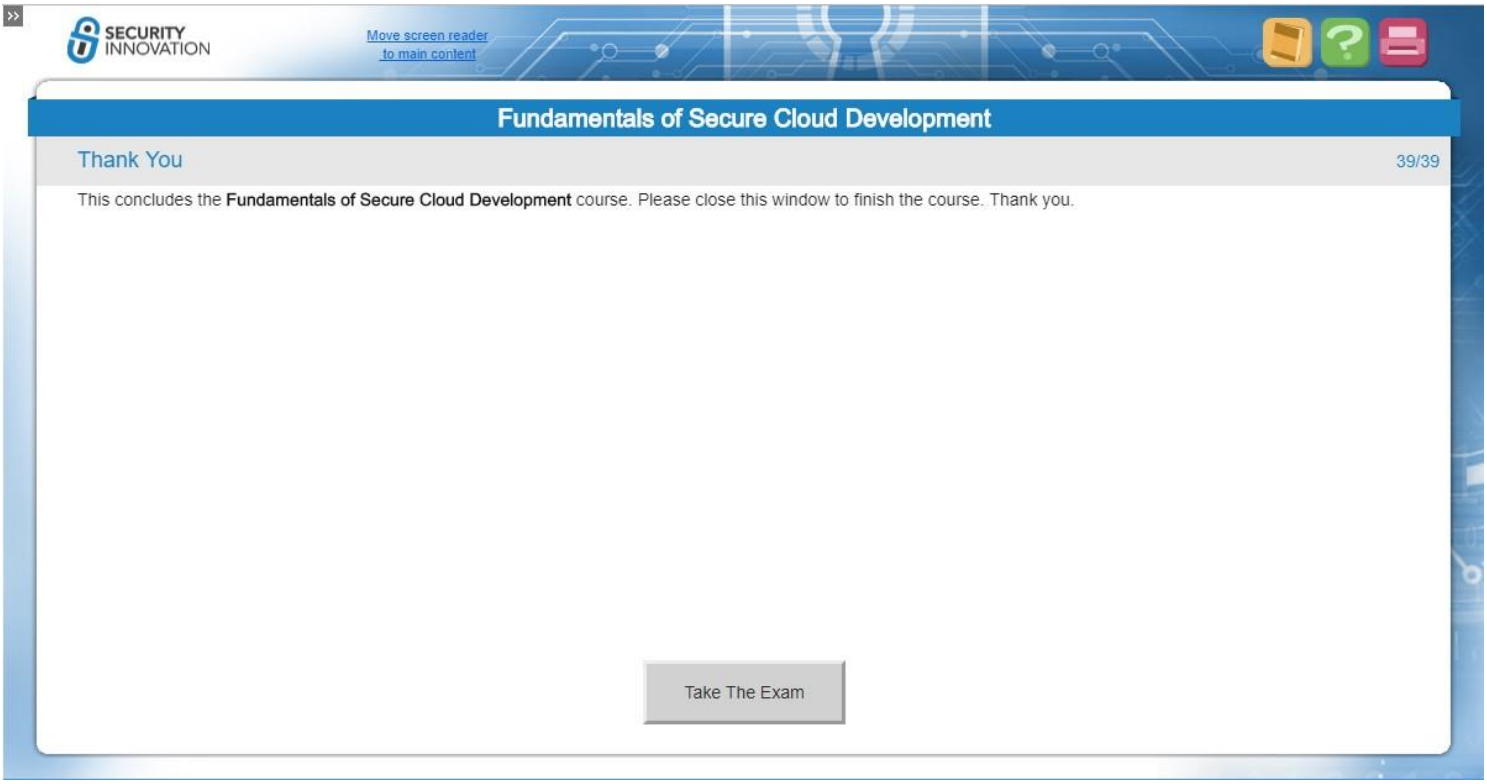
In this module, you learned the best practices for secure cloud application development.

On Screen Text

Module Summary

In this module, you learned the best practices for secure cloud application development.

Thank You



Narration

On Screen Text

Thank You

This concludes the **Fundamentals of Secure Cloud Development** course. Please close this window to finish the course. Thank you.