

## Course Overview and Objectives

The screenshot shows a course page titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. To the right is a blue header bar with the course title. Below the header is a main content area. On the left side of the content area is a pink icon representing a cloud or server. The main text in the content area reads: "In this course, we will examine fundamental cloud security concepts for developers." Below this is a section titled "Course Objectives:" with a bulleted list: "After completing this course, you will be able to:" followed by three items: "• Explain cloud computing", "• Describe cloud computing risks, threats, and regulations", and "• Identify secure development practices for cloud computing". In the top right corner of the content area, there is a timestamp "01/39". A "Move screen reader to main content" link is located at the top left of the page.

### 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

The screenshot shows a web-based learning module titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. A "Move screen reader to main content" link is visible. The main title is centered above a content area. On the left, there's a red icon depicting a map or location. The content area contains text about the module's purpose and objectives, followed by a bulleted list of learning goals.

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

### 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?

The screenshot shows a slide titled "Fundamentals of Secure Cloud Development" with the sub-section "What Is the Cloud?". It includes a link to "Move screen reader to main content" and a timestamp "03/39". The content defines the cloud according to NIST, listing five essential characteristics, three service models, and four deployment models. Below this is a diagram illustrating the three pillars of cloud computing:

- Essential Characteristics:** Broad Network Access, Rapid Elasticity, Measured Service, On-Demand Self-Service, Resource Pooling.
- Service Models:** Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS).
- Deployment Models:** Public, Private, Hybrid, Community.

### 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

The screenshot shows a web page titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. A banner at the top right includes icons for a book, a question mark, and a refresh symbol. Below the title, a sub-section title "Five Essential Cloud Characteristics" is displayed. A progress bar indicates "04/39". A note says "Move screen reader to main content". The main content area contains a list of five characteristics:

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling

Next to the "Resource Pooling" item, a detailed description is provided: "Resource pooling allows the provider's computing resources to be shared in a multi-tenant model, with resources assigned and reassigned on demand."

### 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.)

The screenshot shows a slide titled "Fundamentals of Secure Cloud Development" with the subtitle "Five Essential Cloud Characteristics (Cont.)". A note at the top says "Move screen reader to main content". On the left, there's a sidebar with buttons for "Rapid Elasticity" (grayed out) and "Measured Service" (highlighted in blue). The main content area contains text about Measured Service and a note at the bottom.

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.

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.*

## 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

The screenshot shows a web page titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. A "Move screen reader to main content" link is visible. On the right are icons for search, help, and other navigation. The main content area has a blue header "Cloud Service Models". Below it, a message states: "The cloud has three distinct service models: (1) Software-as-a-Service (SaaS), (2) Platform-as-a-Service (PaaS), and (3) Infrastructure-as-a-Service (IaaS). Click each tab to review the three cloud service models." To the left, there is a vertical sidebar with three tabs: "Software-as-a-Service (SaaS)" (selected), "Platform-as-a-Service (PaaS)", and "Infrastructure-as-a-Service (IaaS)". The "IaaS" tab's content area contains the following text: "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."

### Narration

As described by the Cloud Security Alliance, the cloud has three distinct service models—Software-as-a-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-a-Service (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

The screenshot shows a web page titled "Fundamentals of Secure Cloud Development". In the top left corner is the "SECURITY INNOVATION" logo. A "Move screen reader to main content" link is located just below the logo. On the right side of the header are three icons: a yellow square, a green circle with a question mark, and a red square. The main content area has a blue header bar with the title "Fundamentals of Secure Cloud Development" and a progress bar showing "07/39". Below this, a section titled "Multi-Tenancy" contains the following text:

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

To the right of the text is a diagram titled "Security Guidance for Critical Areas of Focus in Cloud Computing, CSA". The diagram is a layered structure of colored rectangles representing different layers of cloud computing. From top to bottom, the layers are:

- Presentation Modality (Dark Red)
- Presentation Platform (Dark Red)
- APIs (Dark Red)
- Applications (Dark Red)
- Data, Metadata, Content (Dark Red)
- Integration & Middleware (Green)
- APIs (Dark Blue)
- Core connectivity & delivery Abstraction (Dark Blue)
- Hardware (Dark Blue)
- Facilities (Dark Blue)

Below the diagram, the text "Security Guidance for Critical Areas of Focus in Cloud Computing, CSA" is repeated. The entire diagram is enclosed in a dashed border.

### 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

The screenshot shows a web-based learning module titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. A blue banner across the top includes a "Move screen reader to main content" link and three icons: a yellow book, a green question mark, and a red square. Below the banner, the main title "Fundamentals of Secure Cloud Development" is displayed in a blue header bar. The main content area has a light gray background. On the left, there is a vertical navigation bar with two tabs: "Private Cloud" (in black) and "Community Cloud" (highlighted in blue). The main content area contains text about community clouds and a large empty white box for further content.

### 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.)

The screenshot shows a presentation slide with a blue header bar. On the left, there's a logo for 'SECURITY INNOVATION' with a gear icon. To its right is a link 'Move screen reader to main content'. The main title 'Fundamentals of Secure Cloud Development' is at the top center. Below it, a sub-section title 'Cloud Deployment Models (Cont.)' is followed by a note: 'Let's look at the cloud deployment models, which include: (1) Private, (2) Community, (3) Public, and (4) Hybrid'. A sub-instruction says 'Click each tab to learn more about the models.' On the left, there are two tabs: 'Public Cloud' (gray background) and 'Hybrid Cloud' (blue background, indicating it's selected). A text box contains the definition of a 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.' At the bottom left, a note states: 'Note - This slide does not contain audio. Please continue to the next section once you have finished reviewing this material.'

### 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

The screenshot shows a web page with a blue header bar. On the left is the 'SECURITY INNOVATION' logo. In the center, there's a link 'Move screen reader to main content'. On the right are three icons: a yellow book-like icon, a green question mark icon, and a red document icon. Below the header, the title 'Fundamentals of Secure Cloud Development' is displayed in a blue bar. The main content area has a light gray background. A section titled 'Cloud Data Stack' is shown, followed by a paragraph of text. Below that, a table is presented.

	CSP	Cloud Consumer
LaaS	Peripheral Logs	VM Instances, Log Files, Raw Storage, User Accounts, Cookies, Configurations, Backups, Databases, Data
PaaS	VM Instances, Raw Storage, Cookies, Configurations, Peripheral Logs	Log Files, User Accounts, Backups, Cookies, Configurations, Databases, Data
SaaS	VM Instances, Raw Storage, Configurations, Databases, Peripheral Logs	Log Files, User Accounts, Backups, Cookies, Data

### 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:

### Regulatory Requirements and Application Security

The screenshot shows a web page titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. A "Move screen reader to main content" link is visible. On the right are icons for a book, a question mark, and a refresh symbol. The main content area has a blue header "Regulatory Requirements and Application Security". Below it, a text block states: "Various regulations require that organizations implement security controls and processes. Here are some examples:" followed by a bulleted list: • PCI DSS • HIPAA • Sarbanes-Oxley • NIST. To the right of the text are three decorative images: a blue cloud with colorful icons, a clipboard with a checklist, and two red puzzle pieces labeled "Regulatory". The page footer shows the date "11/39".

### 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

The screenshot shows a slide from a presentation. At the top left is the 'SECURITY INNOVATION' logo. To its right is a link 'Move screen reader to main content'. On the far right are three small icons: a yellow book, a green question mark, and a red document. The title 'Fundamentals of Secure Cloud Development' is at the top center. Below it, the section 'Federated Cloud Ecosystem' is highlighted in blue. A list of bullet points follows:

- 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

On the right side of the slide is a graphic of a light blue cloud containing the text 'CLOUD COMPUTING'. Five smaller computer icons are shown, each connected to the cloud by a line, representing a network of cloud computing resources.

### 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

The screenshot shows a web-based knowledge check interface. At the top, there's a header bar with the "SECURITY INNOVATION" logo, a "Move screen reader to main content" link, and three icons (book, question mark, and print). Below the header is a blue navigation bar with the title "Fundamentals of Secure Cloud Development" and the section "Knowledge Check". On the right of the navigation bar, it says "13/39". The main content area contains a question: "Which of the following statements is **not** true of the IaaS model?". Below the question is a list of four options, each preceded by a radio button:

- 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.

In the bottom right corner of the main content area is a "Submit" button.

### 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

The screenshot shows a web-based learning interface. At the top left is the "SECURITY INNOVATION" logo. To its right is a link "Move screen reader to main content". On the far right are three icons: a yellow book, a green question mark, and a red square. The main title "Fundamentals of Secure Cloud Development" is centered at the top in a blue header bar. Below it, a sub-header "Module Summary" is followed by a large text area. The text describes the module's content, mentioning cloud computing characteristics, service models (IaaS, PaaS, SaaS), deployment models (private, community, public, hybrid), and regulatory requirements. A small orange icon of a book with a barcode is positioned to the left of the text area.

### 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

The screenshot shows a web-based learning module titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. To its right is a link "Move screen reader to main content". On the far right are three icons: a yellow folder, a green question mark, and a red document. The main content area has a blue header bar with the title. Below it, a sub-header "Module Overview and Objectives" is followed by a large white area containing text and a small icon. The text describes the module's purpose and lists objectives. A progress indicator "15/39" is in the top right corner.

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

### 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

The screenshot shows a slide titled "Fundamentals of Secure Cloud Development" under the section "Securing the Cloud". The content discusses how cloud computing services can be accessed over any networked device and lists various access points. It also mentions the technological advancements of virtualization and the resulting security issues. A sidebar on the right contains two icons: one showing a login screen with a lock, and another showing a padlock on a 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

### 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

The screenshot shows a web page with a blue header bar. On the left is the 'SECURITY INNOVATION' logo. In the center, there is a link 'Move screen reader to main content'. On the right are three icons: a yellow book-like icon, a green question mark icon, and a red square icon. The main content area has a white background and a blue header bar with the title 'Fundamentals of Secure Cloud Development'. Below the title, the section 'Cloud “Big Data” Security Risks' is listed. A paragraph of text follows, mentioning the 'Expanded Top 10 Big Data Security and Privacy Challenges'. To the right of the text is a small timestamp '17:39'. Below the text is a numbered list of six security challenges.

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

### 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

The screenshot shows a web-based learning interface. At the top, there's a header bar with the 'SECURITY INNOVATION' logo, a 'Move screen reader to main content' link, and three icons (book, question mark, and refresh). Below the header is a blue navigation bar with the title 'Fundamentals of Secure Cloud Development'. The main content area has a light gray background. On the right side of the content area, there's a vertical sidebar with a dark blue header containing the challenge title and a progress indicator '18/39'. The main content itself contains a list of bullet points about secure distributed programming, followed by a large graphic of a cloud with a padlock and binary code.

**Challenge #1: Secure Distributed Programming Computations**

18/39

- 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

### 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

The screenshot shows a slide from a presentation. At the top left is the 'SECURITY INNOVATION' logo. To its right is a blue bar with the text 'Move screen reader to main content'. On the far right of the bar are three icons: a yellow book, a green question mark, and a red square. Below this is a blue header bar with the title 'Fundamentals of Secure Cloud Development' in white. Underneath the header, the slide has a light gray background. The main content area contains the following 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.

In the bottom right corner of the slide, there is a graphic element consisting of a stack of four silver cylinders with red horizontal stripes, resembling a database, and two blue chain links below it.

### 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

The screenshot shows a slide from a presentation titled "Fundamentals of Secure Cloud Development". The title bar includes the "SECURITY INNOVATION" logo and navigation icons for "Move screen reader to main content", "Home", "Help", and "Logout". The main content area has a blue header bar with the title "Challenge #3: End-Point Input Validation/Filtering" and a progress indicator "20/39". The text in the content area states: "Your application's input validation and filtering capabilities must be designed to properly handle every input in a secure fashion." Below this is a bulleted list of best practices:

- 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

To the right of the text is a graphic of a blue funnel with a white document inside it.

### 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

The screenshot shows a web page titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. To its right is a link "Move screen reader to main content". On the far right are three icons: a yellow square, a green circle with a question mark, and a red square with a minus sign. Below the header, the main content area has a blue header bar with the title "Challenge #4: Cryptographically Enforced Data-Centric Security" and a page number "21/39". The main text discusses Public-Key Infrastructure (PKI) solutions for transport-layer protection, Attribute-Based Encryption (ABE), and Homomorphic encryption. It notes that ABE inserts attributes into public-private keys for enhanced access controls, while homomorphic encryption allows computations on ciphertext.

### 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

The screenshot shows a web-based learning interface. At the top, there's a blue header bar with the title "Fundamentals of Secure Cloud Development". Below the header, a sub-header reads "Challenge #5: Granular Access Control and Audits". On the right side of the sub-header, it says "22/39". In the top left corner, there's a logo for "SECURITY INNOVATION" with a gear icon. To its right, a link says "Move screen reader to main content". On the far right of the header are three icons: a yellow book, a green question mark, and a red square.

The main content area has a light gray background. It starts with a text block: "Let's learn about granular access control and audits. (1) Access Control and (2) Audits". Below this, a smaller text says "Click each control to learn more.".

On the left side of the content area, there's a vertical navigation bar with two buttons: "Access Control" (which is white) and "Audits" (which is blue). The "Audits" button is currently selected.

The main content area contains two paragraphs of text. The first paragraph discusses the use of SIEM tools for forensic and auditing/accounting purposes, mentioning log4j and Java applications. The second paragraph discusses how granular audits can help security teams discover malicious activity or data breaches and validate privacy requirements.

### 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

The screenshot shows a slide titled "Fundamentals of Secure Cloud Development" with the subtitle "Challenge #6: Data Provenance". The slide content includes several paragraphs of text and two small images. At the top left is the "SECURITY INNOVATION" logo. A "Move screen reader to main content" link is visible. The top right features three icons: a book, a question mark, and a print symbol. The slide footer indicates "23/39".

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://ssi.sce.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.





### 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

The screenshot shows a knowledge check interface. At the top left is the 'SECURITY INNOVATION' logo. To its right is a link 'Move screen reader to main content'. On the far right are three icons: a yellow book, a green question mark, and a red document. Below this is a blue header bar with the title 'Fundamentals of Secure Cloud Development'. Underneath the header, the section title 'Knowledge Check' is displayed next to a progress indicator '24/39'. The main content area contains a question: 'What do most organizations currently use within applications and networks for logical access controls?'. Below the question is a list of four options, each preceded by a radio button:

- ABE cryptographic algorithms
- Role-Based Access Controls (RBAC)
- Security Information Event Management (SIEM)
- Application Programming Interfaces (APIs)

At the bottom right of the main content area is a dark grey 'Submit' button.

### 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

The screenshot shows a web-based learning interface. At the top, there's a blue header bar with the title "Fundamentals of Secure Cloud Development". Below the header, a sub-header says "Module Summary". In the top right corner, it shows "25/39". On the left, there's a yellow icon of a clipboard with a checkmark. The main content area contains the following text:

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.

## 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

The screenshot shows a web-based learning module titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. A blue banner across the top has the title and a "Move screen reader to main content" link. On the right are icons for a book, a question mark, and a refresh symbol. The main content area is titled "Module Overview and Objectives". It contains a brief description of the module's purpose, a "Module Objective" section with one bullet point, and a small icon of a map with a location pin.

### 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

The screenshot shows a web page titled "Fundamentals of Secure Cloud Development". At the top left is the "SECURITY INNOVATION" logo. A "Move screen reader to main content" link is visible. On the right are icons for a book, a question mark, and a refresh symbol. The main content area has a blue header "Fundamentals of Secure Cloud Development" and a sub-header "Secure Cloud Application Development Best Practices". Below this, a paragraph explains the importance of using security best practices throughout the design, development, and deployment phases. A bulleted list follows, detailing specific steps:

- 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

At the bottom right of the content area, it says "27/39".

### 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

The screenshot shows a web page titled "Fundamentals of Secure Cloud Development". In the top left corner, there is a logo for "SECURITY INNOVATION" with a blue icon. Next to it is a link "Move screen reader to main content". On the right side of the header are three icons: a yellow book, a green question mark, and a red square. The main content area has a blue header bar with the title "The CIA Triad: Protecting Customer's Assets" and a progress bar showing "28/39". Below this, a text block states: "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." A note below says: "The principles are: (1) Confidentiality, (2) Integrity, and (3) Availability." A link "Click each principle to learn more." is present. To the left of the text block is a vertical sidebar with three buttons: "Confidentiality" (white), "Integrity" (dark grey), and "Availability" (blue). The "Availability" button is highlighted. To the right of the sidebar, the text "Availability is reliable access to system resources. Availability requires:" is followed by a bulleted list: "• Resistance to denial-of-service attacks.", "• Component (hardware and software) redundancy.", and "• Fault-tolerant and failure-tolerant software.".

### 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

The screenshot shows a web-based training interface. At the top, there's a navigation bar with icons for back, forward, and search, along with the "SECURITY INNOVATION" logo and a link to move the screen reader to the main content. The main title is "Fundamentals of Secure Cloud Development". Below it, the specific topic is "Implementing CIA to meet Customer Requirements". A progress indicator shows "29/39". On the left, a sidebar lists three principles: Confidentiality, Integrity, and Availability, with Availability being the active tab. The main content area contains text about implementing CIA tenets, followed by a list of measures for Availability.

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.*

<b>Confidentiality</b>	Availability can be ensured by:
<b>Integrity</b>	<ul style="list-style-type: none"><li>Redundant storage media, power backup, and event response planning network.</li></ul>
<b>Availability</b>	

### 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

The screenshot shows a slide from a presentation titled "Fundamentals of Secure Cloud Development". The title bar includes the "SECURITY INNOVATION" logo and a "Move screen reader to main content" link. The slide has a blue header bar with icons for a book, a question mark, and a refresh symbol. The main content area has a white background with a blue border. The title "Applying CIA to Cloud Applications" is at the top left, and the page number "30/39" is at the top right. Below the title, a text block says: "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." To the right of this text is a diagram of the CIA triad. It consists of three circles labeled C (Confidentiality), I (Integrity), and A (Availability). Each circle is associated with a list of artifacts:

- Confidentiality**
  - Transactional Data
  - Metadata
  - Geospatial Data
  - Credentials
- Integrity**
  - Transactional Data
  - Metadata
  - Non-Repudiation
  - Geospatial Data
- Availability**
  - Transactional Data
  - Service
  - Metadata
  - Geospatial Data

### 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

The screenshot shows a slide from a presentation titled "Fundamentals of Secure Cloud Development". The title bar includes the "SECURITY INNOVATION" logo, a "Move screen reader to main content" link, and three icons: a book, a question mark, and a refresh symbol. The slide content is titled "Multi-Tiered Application Security Architecture". It features a diagram illustrating a multi-tiered architecture with two firewalls and four distinct layers: Application, Runtime, Data, and Networking. Each layer contains specific components: Application (Runtime, Host Operating System, Virtualization, Servers), Runtime (Middleware, Host Operating System, Virtualization, Servers), Data (Storage, Host Operating System, Virtualization, Servers), and Networking (represented by a thick blue bar). The entire diagram is enclosed in a white border.

### 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

The screenshot shows a slide titled "Cloud Application Security Frames Overview". At the top left is the "SECURITY INNOVATION" logo. A blue banner across the top has the title "Fundamentals of Secure Cloud Development" and a "Move screen reader to main content" link. On the right of the banner are three icons: a yellow book, a green question mark, and a red square. The main content area contains text about security frames and a bulleted list of four major security frames.

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

### 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.)

The screenshot shows a web page titled "Fundamentals of Secure Cloud Development" with a sub-section titled "Cloud Application Security Frames Overview (Cont.)". The page includes a navigation bar with icons for search, help, and print, and a status message "Move screen reader to main content". The main content area contains text about security frames and categories, followed by three tabs: "Input/Data Validation", "Authentication", and "Authorization". The "Authorization" tab is currently selected, displaying a box of text about improperly implemented authorization mechanisms.

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 tab to learn more.

Input/Data Validation	Authentication	Authorization
Improperly implemented or weak authorization mechanisms can result in unauthorized access to confidential or restricted data, data tampering, and execution of unauthorized operations.		

### 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.)

The screenshot shows a slide titled 'Fundamentals of Secure Cloud Development' with a sub-section titled 'Cloud Application Security Frames Overview (Cont.)'. At the top left is the 'SECURITY INNOVATION' logo. A blue banner at the top right contains icons for a clipboard, a question mark, and a print symbol. Below the title, a message says 'Move screen reader to main content'. The slide content includes a note: 'Click each tab to learn more.' followed by three tabs: 'Configuration Management', 'Sensitive Data', and 'Cryptography'. The 'Cryptography' tab is selected, displaying the text: 'Improperly implemented cryptography can expose confidential data and account credentials to unauthorized access.' A note at the bottom states: 'Note - This slide does not contain audio. Please continue to the next section once you have finished reviewing this material.'

## 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.)

The screenshot shows a slide titled "Fundamentals of Secure Cloud Development" with the subtitle "Cloud Application Security Frames Overview (Cont.)". At the top left is the "SECURITY INNOVATION" logo. A blue banner at the top right contains icons for a magnifying glass, a question mark, and a refresh symbol. Below the title, a sub-header says "Move screen reader to main content". The slide content area has a light gray background. It displays the text "Click each tab to learn more." above two tabs: "Exception Management" (dark gray) and "Auditing and Logging" (blue). A large text box below the tabs contains the note: "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." At the bottom of the slide, a note states: "Note - This slide does not contain audio. Please continue to the next section once you have finished reviewing this material."

## 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

The screenshot shows a slide from a presentation. At the top left is the Security Innovation logo. To its right is a link "Move screen reader to main content". On the far right are three icons: a yellow folder, a green question mark, and a red square. The title "Fundamentals of Secure Cloud Development" is at the top center. Below it, the section title "Developing Secure APIs" is in blue. A text block follows, stating: "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." At the bottom right of the slide is the page number "36/39".

### 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

The screenshot shows a web-based knowledge check interface. At the top left is the "SECURITY INNOVATION" logo. To its right is a link "Move screen reader to main content". On the far right are three icons: a yellow square with a gear, a green square with a question mark, and a red square with a document. The main title "Fundamentals of Secure Cloud Development" is centered at the top in a blue bar. Below it, the section title "Knowledge Check" is displayed, along with a progress indicator "37/39". The main content area contains a question: "Which of the following help ensure confidentiality within the CIA triad? (Choose 2)". Below the question is a list of four options, each preceded by a small square checkbox:

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

In the bottom right corner of the main content area is a dark grey "Submit" button.

## 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

The screenshot shows a web-based learning interface. At the top left is the "SECURITY INNOVATION" logo. To its right is a link "Move screen reader to main content". On the far right are three icons: a yellow book-like icon, a green question mark icon, and a red document icon. The main title "Fundamentals of Secure Cloud Development" is centered at the top in a blue header bar. Below it, a sub-header "Module Summary" is followed by the text: "In this module, you learned the best practices for secure cloud application development." A small orange icon depicting a book with a striped cover is positioned to the left of the text. In the top right corner of the main content area, there is a progress indicator showing "38/39".

## 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

The screenshot shows a web-based course completion page. At the top left is the "SECURITY INNOVATION" logo with a blue circular icon. Next to it is a link "Move screen reader to main content". The top center features the course title "Fundamentals of Secure Cloud Development". On the right side of the header are three icons: a yellow book, a green question mark, and a red square. Below the header, the main content area has a light gray background. It displays the text "Thank You" in blue and "39/39" in the top right corner. A message reads: "This concludes the **Fundamentals of Secure Cloud Development** course. Please close this window to finish the course. Thank you." At the bottom center is a gray button labeled "Take The Exam".

## 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.