Module 2

Cloud Computing: Security, Risks, and Governance

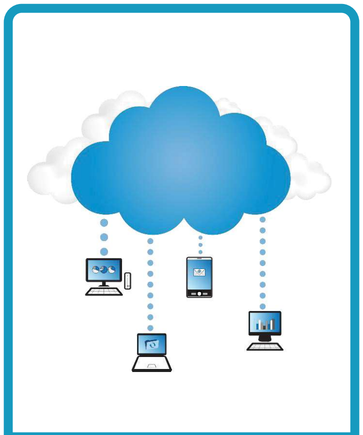
MODULE LEARNING OBJECTIVES

At the end of this module, you will be able to:

- Explain the basic concepts of cloud computing.
- Describe and explain the underpinning security concepts of information security and CIA.
- Describe the key areas of security management.
- Explain the risks and the impacts of cloud computing in terms of both business and technical security challenges and their effect on business and technical governance and policy.
- Explain and implement risk treatments and mitigations in the cloud.

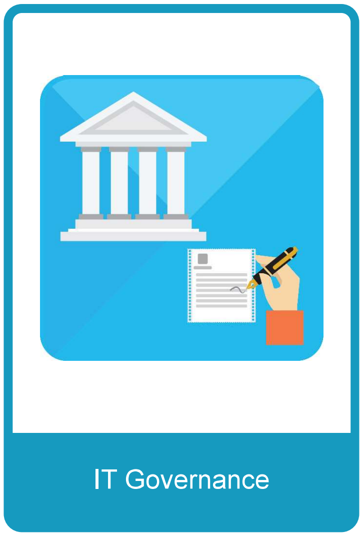
MODULE TOPICS

The following topics are covered in the module:



Cloud Computing Basics

Information Security Management



CLOUD COMPUTING BASICS

Cloud Computing Primer: What is Cloud?

Cloud computing represents a major change in IT sourcing and service delivery. It is changing how businesses purchase, deploy, and support IT services. Many companies are now responding to the new opportunities. Cloud computing is based on the convergence of Internet technologies, virtualization, and IT standardization.

Service Delivery Type

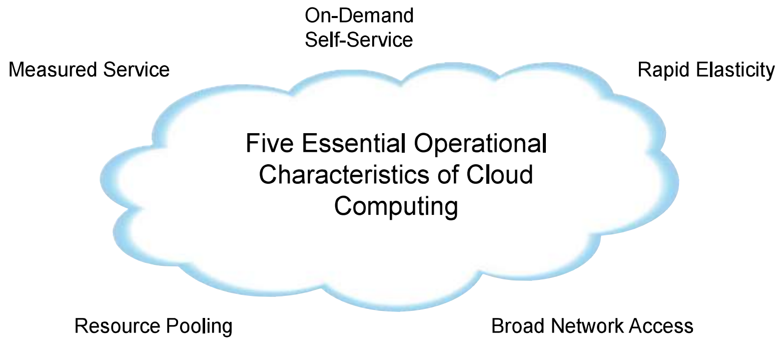
- **Software-as-a-service**
- **Platform-as-a-service**
- **Infrastructure-as-a-service**

Service Deployment Options

- **Private Cloud**
- **Community Cloud**
- **Public Cloud**
- **Hybrid Cloud**

Characteristics of Cloud Computing

The following figure shows the five essential operational characteristics of cloud computing.



On-Demand Self-Service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Rapid Elasticity

Capabilities can be rapidly and elastically provisioned. In some cases, it can be provisioned automatically to quickly scale out, and then is rapidly released to scale in.

Broad Network Access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

Resource Pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (for example, country or state).

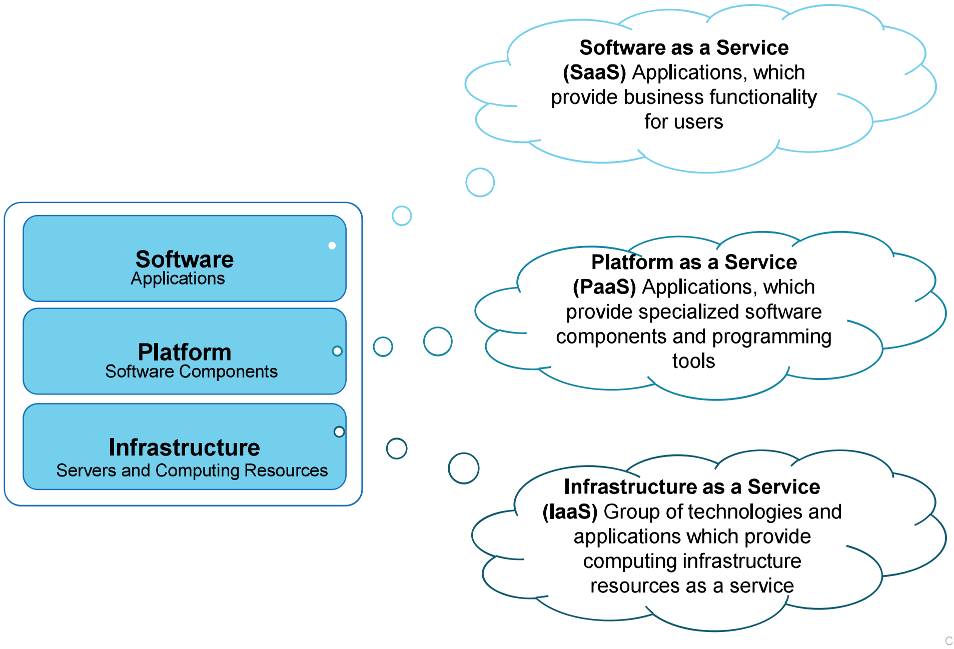
Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction, appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

In the simplest of terms, cloud computing is an Internet-based shared computing paradigm, somewhat like an electricity grid. The cloud services are based around shared mechanisms, such as:

- Internet-based computing
- Shared resources
- Shared software
- Shared platforms and infrastructure
- Available on-demand

Cloud Service Models



Software
Applications

Platform
Software Components

Infrastructure
Servers and Computing Resources

Software as a Service (SaaS) Applications, which provide business functionality for users

Platform as a Service (PaaS) Applications, which provide specialized software components and programming tools

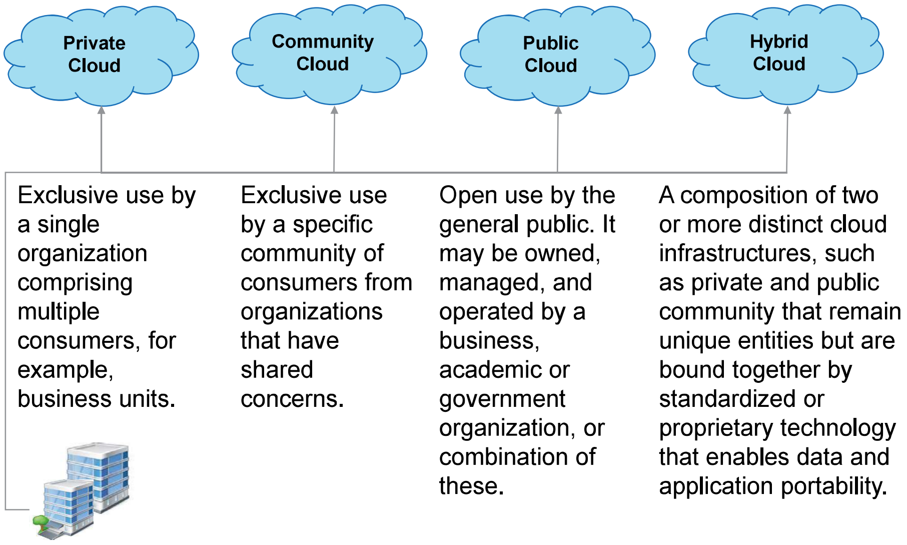
Infrastructure as a Service (IaaS) Group of technologies and applications which provide computing infrastructure resources as a service

Examples of SaaS services: E-mail, collaboration, productivity, CRM, marketing, finance, and personnel enterprise applications.

Examples of PaaS services: Software development, software testing, and systems integration.

Examples of IaaS services: Storage, database, computer, network, service management, and data center management.

Cloud Deployment Models



Exclusive use by a single organization comprising multiple consumers, for example, business units.

Exclusive use by a specific community of consumers from organizations that have shared concerns.

Open use by the general public. It may be owned, managed, and operated by a business, academic or government organization, or combination of these.

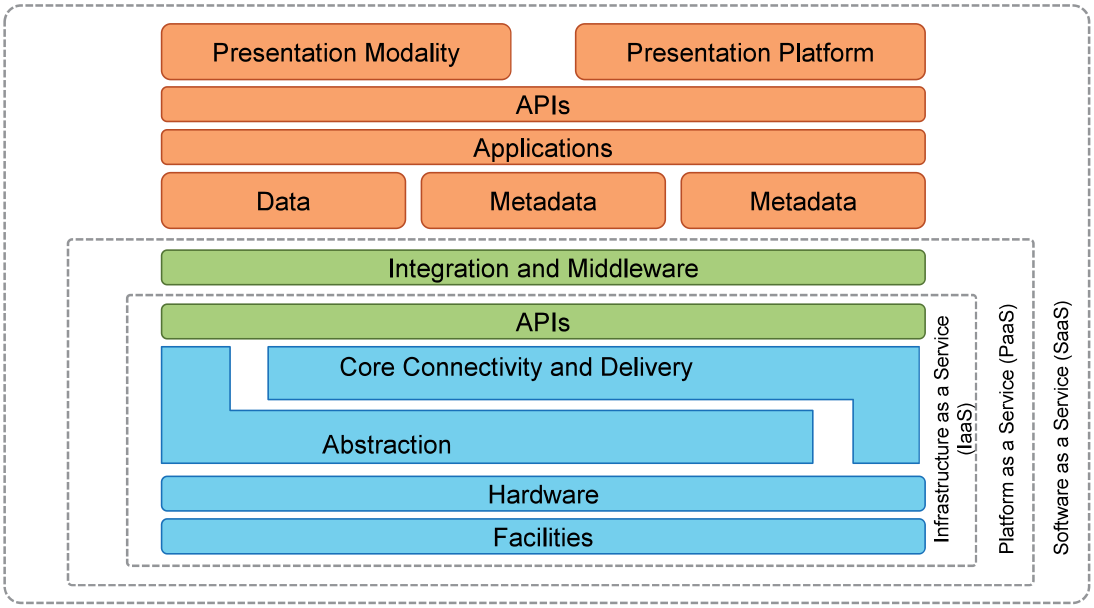
A composition of two or more distinct cloud infrastructures, such as private and public community that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Source: NIST definition of cloud computing

In addition to the cloud services models, there are a number of other ways to deliver or roll out these cloud services. In some development models, the financial commitment lies with the organizations that use these clouds.

Cloud Reference Model

The following figure shows a generic cloud reference model.


Presentation Modality
Presentation Platform
APIs
Applications
Data
Metadata
Metadata
Integration and Middleware
APIs
Core Connectivity and Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)

Understanding the relationships and dependencies between cloud computing models is critical for understanding the security risks in cloud computing. In cloud computing, cloud service provider bears a responsibility for security. The figure depicts the idea that just as capabilities are inherited, information security issues and risks are also inherited.

Some salient points depicted through the cloud reference model are:

- IaaS is the foundation of all cloud services.
- PaaS is building upon IaaS.
- SaaS, in turn, is building upon PaaS.

It is important to note that commercial cloud providers may not neatly fit into the layered service models. Nevertheless, the reference model is important for relating real-world services to an architectural framework and understanding the resources and services requiring security analysis.

Some common cloud computing reference models are:

- NIST Cloud Computing Reference Architecture
  - http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
- IBM Cloud Computing Reference Architecture
  - https://www.ibm.com/developerworks/community/wikis/home/wiki/Wf3cce8ff09b3_49d2_8ee7_4e49c1ef5d22/page/IBM%20Cloud%20Computing%20Reference%20Architecture%204.0?lang=en

- ISO/IEC 17789:2014 Information technology -- Cloud computing -- Reference architecture
  - http://www.iso.org/iso/catalogue_detail?csnumber=60545
- The Open Group Cloud Ecosystem Reference Model
  - http://www.opengroup.org/cloud/cloud/cloud_ecosystem_rm/model.htm
- Microsoft Private Cloud Reference Model
  - https://social.technet.microsoft.com/wiki/contents/articles/4399.private-cloud-reference-model.aspx

Exercise: Cloud Computing Basics

Read the given scenario and outline a business use case to present the benefits of the cloud computing using the IaaS service model.

Stelford is a leading steel manufacturing organization operating globally. The organization has manufacturing plants in three countries and the Sales and Operations teams and regional offices in more than 30 countries.

Stelford uses an ERP application that works in a distributed architecture, where the manufacturing plants and regional offices have the local deployment of the application. Every night the data from all the different sites is collected within the central site and synced backed to the other local sites. The syncing of the data takes approximately 24 hours.

The Executive team wants to have a just-in-time ordering for a better customer experience, but the time gap in syncing of data is a hindrance for the Sales and Operations teams to receive the real-time stock position and for the manufacturing plants to estimate the requirements.

As an IT Manager, you propose to migrate to the cloud to achieve high availability and scalability. In addition, as the ERP application is built and maintained internally, you want to have the administration control of the development environment. Considering the problem description and business requirements, outline a business use case to present the benefits of the cloud computing using the IaaS service model.

Outcome:

This exercise will help to recall the cloud characteristics, service, and deployment model.

Sample Answer

Company Background

Stelford is a leading steel manufacturing company with factories spread across three countries and Sales and Operations teams and regional offices in more than 30 countries.

Problem Description

The ERP application works in distributed architecture and the manufacturing sites and regional sales offices have the local deployment. The syncing of data between the central site and local sites takes approximately 24 hours. This is hindrance for the Sales and Operations teams to receive the updated stock position in real-time mode and place just-in-time orders for the customer.

Business Requirements

- Fast and efficient synchronization between the sites and regional offices at different locations
- Availability of complete, integrated, and updated data from all sites and regional offices in real-time mode
- Centralized control of the ERP application
- In-house control of the development environment

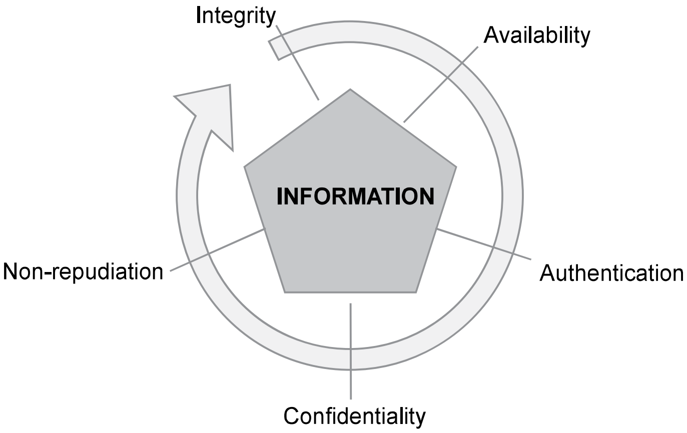
Benefits from Cloud Computing (using IaaS service model)

- Access to the centralized ERP application and data
- Specific development environment for the current ERP
- Complete administration access for the entire environment
- Scaling of the infrastructure to be controlled by the Stelford IT team
- Extensive resiliency

INFORMATION SECURITY MANAGEMENT

Information Security: Definition

Information security (also known as cyber security or INFOSEC) is security as applied to computing devices and computer networks.



Source: InfoSec Institute - Guiding Principles in Information Security and NIST 800-33

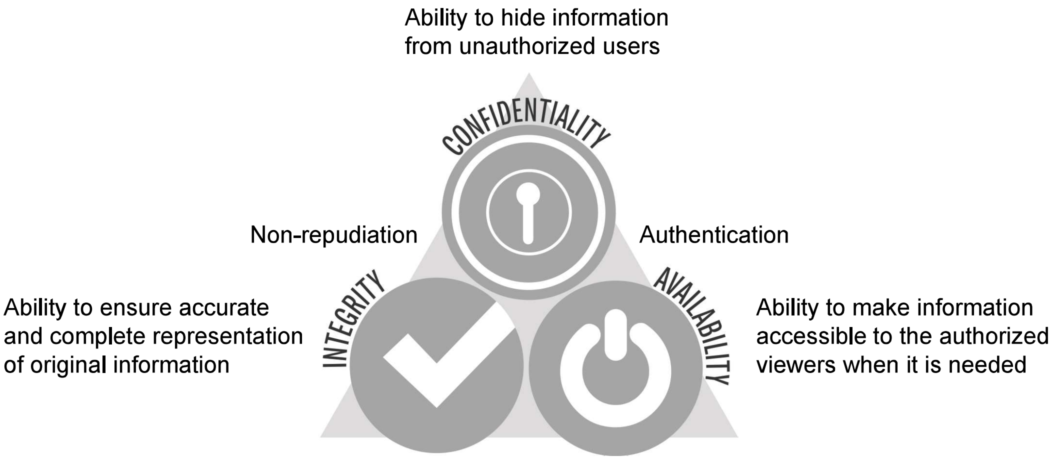
Information security covers all the processes and mechanisms by which information and services are protected from unintended or unauthorized access, change, or destruction. Information security also includes protection from unplanned events and natural disasters.

The Confidentiality, Integrity, and Availability (CIA) triad is a venerable and well-known model for security policy development, used to identify problem areas and necessary solutions for information security.

The CIA Principle

The CIA triad is a simple but widely-applicable security model. It stands for Confidentiality, Integrity, and Availability - the three key principles, which should be guaranteed in any kind of security system.

The following figure shows the CIA triad.


Ability to hide information
from unauthorized users
CONFIDENTIALITY
Non-repudiation
Authentication
Ability to ensure accurate
and complete representation
of original information
INTEGRITY
AVAILABILITY
Ability to make information
accessible to the authorized
viewers when it is needed

These principles are applicable across the whole subject of security analysis, from access to a user's Internet history to security of encrypted data across the Internet. If any one of the three is breached, it can have serious consequences for the parties concerned.

Confidentiality

Confidentiality is the ability to hide information from those who are unauthorized to view it. It is perhaps the most obvious aspect of the CIA triad when it comes to security. However, correspondingly, it is also the one that is attacked most often. Cryptography and encryption methods are used to maintain confidentiality, especially for the data transferred from one computer to another.

Integrity

Integrity is the ability to ensure that data is an accurate and complete representation of the original secure information. A type of security attack is to intercept some important data and make changes to it before sending it on to the intended receiver.

Availability

Availability is the ability to ensure that the information concerned is readily accessible to the authorized viewers when it is needed. Distributed Denial of Service (DDoS) is one example of the attack to make an online service unavailable by staggering it with traffic from multiple sources. Some types of security attacks may attempt to deny access to the appropriate user for gaining some secondary effect. For example, by breaking a website for a particular search engine, a rival may try to become more popular.

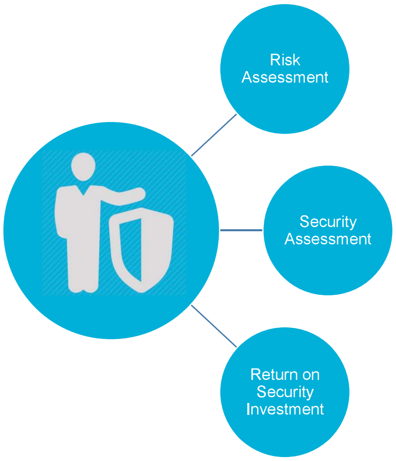
The CIA being a simple model is augmented by others concepts such as non-repudiation and authentication. The concept of non-repudiation assures that the sender of information is provided with proof of delivery and recipient is provided with proof of the sender's identity. The concept of authentication aims to verify the identity of an individual, a computer, a software, or similar.

Security Management

Security management is a set of policies and procedures for systematically securing and managing organizations' data, information, systems, and services.

The primary goal of security management is to ensure the confidentiality, availability, and integrity of organization's information, systems, and services.

Security management involves various key areas including risk assessment, security assessment, and calculation of return on security investment.



Source: ISO/IEC 27001:2005

Assets, Threats, Vulnerability, and Risk

Key terms for assets identification:

- **Assets**: What we are trying to protect.
- **Threat**: What we are trying to protect against.
- **Vulnerability**: Is a weakness or gap in our protection efforts.
- **Risk**: Is the intersection of assets, threats, and vulnerabilities.

Further explanation of threats, vulnerability, and risks are given.

- **Assets**: Any information, system, software, or hardware that is owned by the organization.
- **Threat**: Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.
- **Vulnerability**: Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset or make it unavailable to its rightful users.
- **Risk**: The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

Examples of Assets:

- **People**: People may include employees and customers.
- **Property**: Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information.
- **Information**: Information may include databases, software code, critical company records, and many other tangible items.

Example of threats: Angry employees, dishonest employees, criminals, hackers, malware, virus, and rogue software.

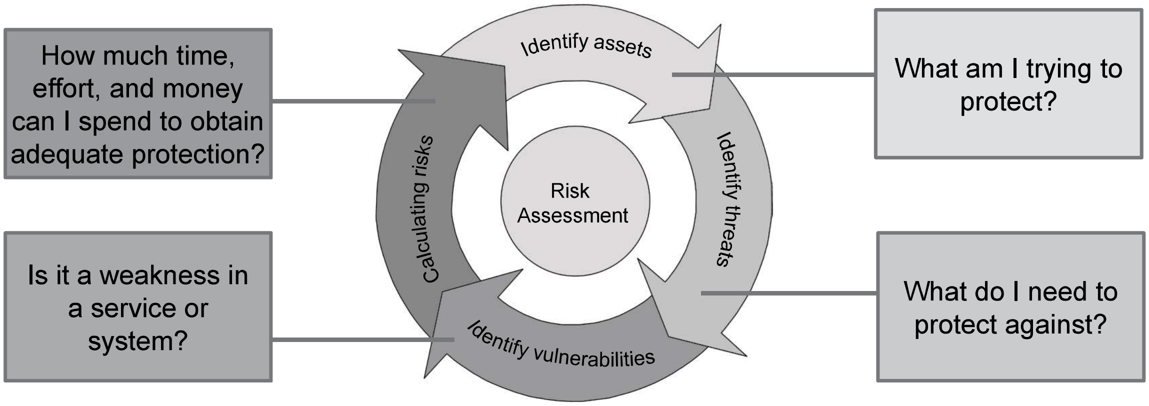
Example of vulnerability: Software bugs, broken processes, ineffective controls, hardware malfunctions, business change, legacy systems, and human error.

Example of risks: Business disruption, financial loss, loss of privacy, damage to reputation, and legal penalties.

It is important to understand the difference between the terms - threats, vulnerability, and risks - in order to understand the true risk to assets.

Risk Assessment

The following figure depicts the four important tasks carried out during risk assessment. In order to perform a comprehensive risk assessment, it is very important to identify all the assets, threats and vulnerabilities. Based on these three, the risk is calculated.


How much time, effort, and money can I spend to obtain adequate protection?
Identify assets
What am I trying to protect?
Calculating risks
Risk Assessment
Identify threats
Is it a weakness in a service or system?
What do I need to protect against?
Identify vulnerabilities

Source: Information Systems Audit and Control Association, (ISACA) – IT Governance

While conducting a risk assessment, the formula used to determine risk is as given:

R = A x T x V

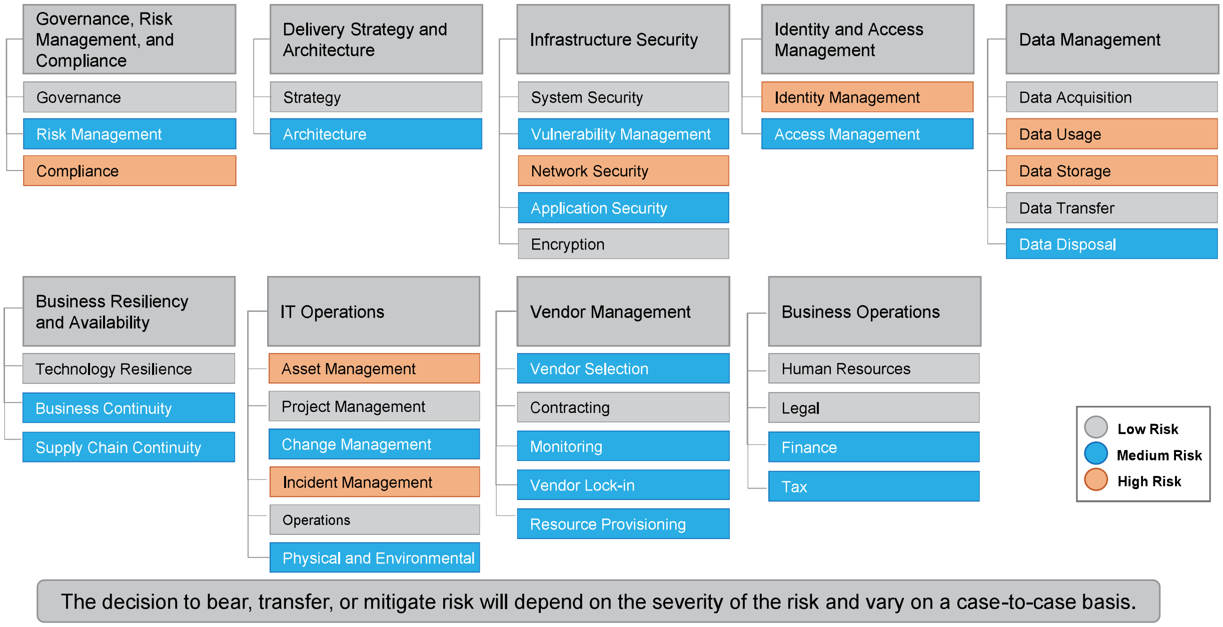
(Risk = Asset x Threat x Vulnerability)

Risk assessment is a comprehensive process that comprises various model, tools, and methodologies:

- Examine assets – Asset management helps to identify the assets and how they are maintained, changed, and depreciated.
- Identify threat and vulnerabilities – Threat modeling is a common tool to identify threats and vulnerabilities.
- Identify, categorize, and prioritize risks – Risk acceptance plan and risk assessment result matrix are the tools to assess, categorize, and prioritize risks.
- Plan security/risk remediation tasks - Risk treatment and risk remediation plan are the tools to identify, plan, and implement risk remediation tasks.

Risk Assessment Result Matrix

The following figure represents a sample risk assessment result matrix, which identifies low, medium, and high risks across nine business risk areas.



Governance, Risk Management, and Compliance
- ⚪ Governance
- 🔵 Risk Management
- 🟠 Compliance

Delivery Strategy and Architecture
- ⚪ Strategy
- 🔵 Architecture

Infrastructure Security
- ⚪ System Security
- 🔵 Vulnerability Management
- 🟠 Network Security
- 🔵 Application Security
- ⚪ Encryption

Identity and Access Management
- 🟠 Identity Management
- 🔵 Access Management

Data Management
- ⚪ Data Acquisition
- 🟠 Data Usage
- 🟠 Data Storage
- ⚪ Data Transfer
- 🔵 Data Disposal

Business Resiliency and Availability
- ⚪ Technology Resilience
- 🔵 Business Continuity
- 🔵 Supply Chain Continuity

IT Operations
- 🟠 Asset Management
- ⚪ Project Management
- 🔵 Change Management
- 🟠 Incident Management
- ⚪ Operations
- 🔵 Physical and Environmental

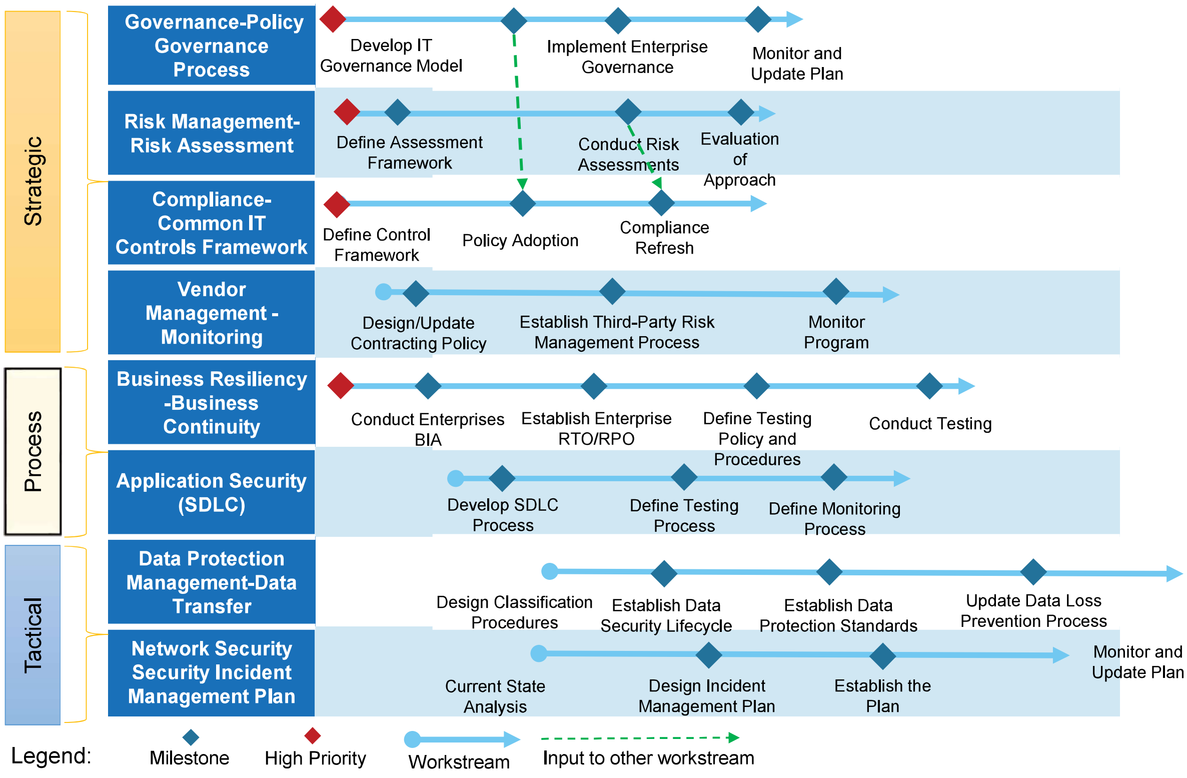
Vendor Management
- 🔵 Vendor Selection
- ⚪ Contracting
- 🔵 Monitoring
- 🔵 Vendor Lock-in
- 🔵 Resource Provisioning

Business Operations
- ⚪ Human Resources
- ⚪ Legal
- 🔵 Finance
- 🔵 Tax

⚪ Low Risk
🔵 Medium Risk
🟠 High Risk

The decision to bear, transfer, or mitigate risk will depend on the severity of the risk and vary on a case-to-case basis.

Executive Risk Treatment and Remediation Plan: Example



Strategic

Governance-Policy Governance Process: Develop IT Governance Model; Implement Enterprise Governance; Monitor and Update Plan

Risk Management-Risk Assessment: Define Assessment Framework; Conduct Risk Assessments; Evaluation of Approach

Compliance-Common IT Controls Framework: Define Control Framework; Policy Adoption; Compliance Refresh

Vendor Management - Monitoring: Design/Update Contracting Policy; Establish Third-Party Risk Management Process; Monitor Program

Process

Business Resiliency -Business Continuity: Conduct Enterprises BIA; Establish Enterprise RTO/RPO; Define Testing Policy and Procedures; Conduct Testing

Application Security (SDLC): Develop SDLC Process; Define Testing Process; Define Monitoring Process

Tactical

Data Protection Management-Data Transfer: Design Classification Procedures; Establish Data Security Lifecycle; Establish Data Protection Standards; Update Data Loss Prevention Process

Network Security Security Incident Management Plan: Current State Analysis; Design Incident Management Plan; Establish the Plan; Monitor and Update Plan

Legend: ◆ Milestone ◆ High Priority → Workstream ⇢ Input to other workstream

This figure represents an example of a risk treatment and remediation plan. It highlights the differences between strategic, process, and tactical elements of focus. The controls on each layer can be implemented accordingly as per the business preference.

Security Assessment

The goal of a security assessment, also known as a security audit or security review, is to ensure that necessary security controls are integrated into the design and implementation of a project.

A properly completed security assessment should provide documentation outlining any security gaps between a project design and approved corporate security policies.

Management can address security gaps in the following three ways:

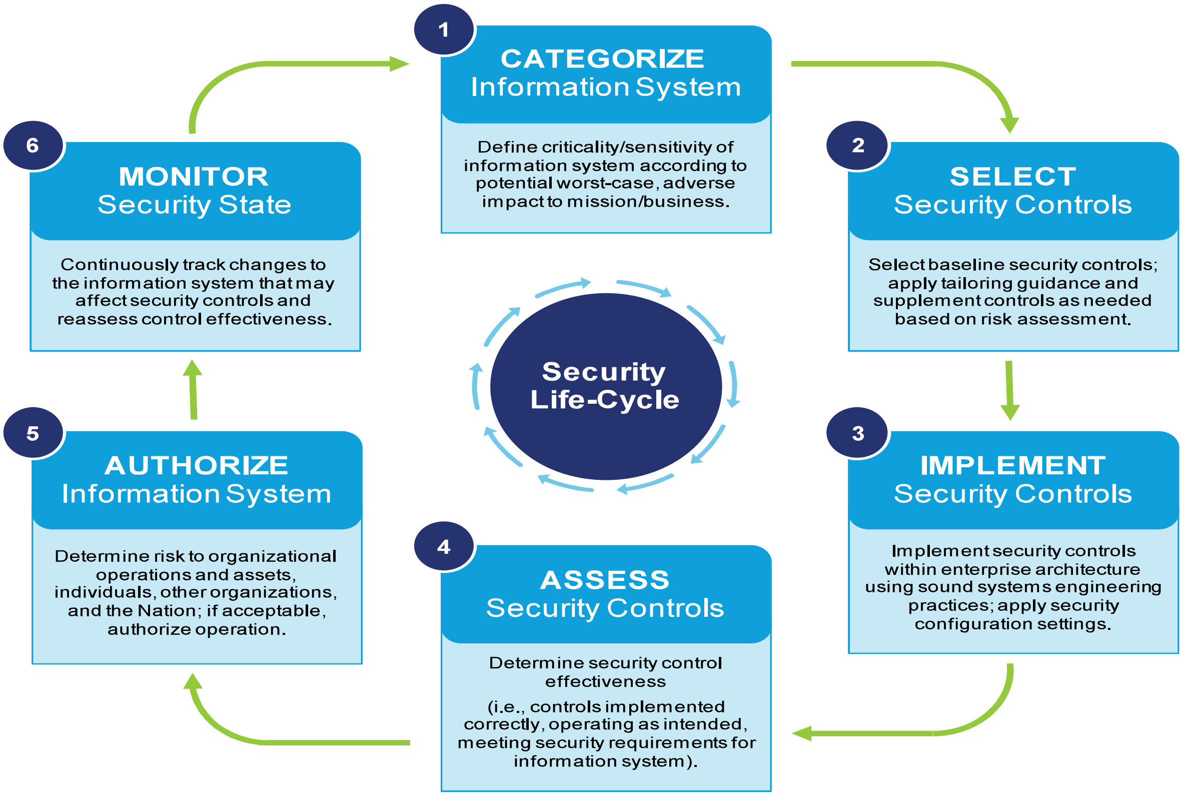
- It can decide to cancel the project.
- It can allocate the necessary resources to correct the security gaps.
- It can accept the risks, based on an informed risk/reward analysis.

Security Management Lifecycle

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of organizational risk.

Security management lifecycle consists of six steps that are paramount to the effective management of risk resulting from the operation and use of information systems.

The following figure shows the security management lifecycle.



1 CATEGORIZE Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

2 SELECT Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

3 IMPLEMENT Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

4 ASSESS Security Controls

Determine security control effectiveness

(i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

5 AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

6 MONITOR Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Source: NIST SP 800-37 Applying the Risk Management Framework
NIST SP 800-30 Risk Management Guide for Information Technology Systems

Using these corresponding requirements in an integrated way can provide a methodical, repeatable, and risk-based approach for selecting, specifying, and implementing security controls to adequately protect within the cloud.

Return on (Security) Investment

1. Have you ever faced a situation where you have been told that your security measures are too expensive?
2. Have you ever faced a situation where you find it very difficult to explain to management the consequences of an incident in terms of profit or loss?

Return on Security Investment Formula:
ROSI = Monetary Risk Mitigation – Cost of Control

For each threat, we can then calculate:
Annualized Loss Expectancy = Annual Rate of Occurrence * Single Loss Expectancy

A security investment is judged to be profitable, if the risk mitigation effect is greater than the expected costs.

Source: Christian Locher, Methodologies for evaluating information security investments, 2005

Some common metrics for security investment are:

- **Single Loss Expectancy (SLE)**: SLE is the expected amount of money that will be lost when a risk occurs. It can be considered as the total cost of an incident assuming its single occurrence.
- **Annual Loss Expectancy (ALE)**: ALE is the annual monetary loss that can be expected from a specific risk on a specific asset. It is calculated as follows: ALE = ARO * SLE
- **Annual Rate of Occurrence (ARO)**: ARO is a measure of the probability that a risk occurs in a year.

Return on Security Investment: Example

The Acme Corp. is considering investing in an anti-virus solution. Each year, Acme suffers 5 virus attacks (ARO=5). The CSO estimates that each attacks cost approximately 15.000€ in loss of data and productivity (SLE=15.000). The anti-virus solution is expected to block 80% of the attacks (Mitigation ratio=80%) and costs 25.000€ per year (License fees 15.000€ + 10.000€ for trainings, installation, maintenance etc.).

The Return on security investment for this solution is then calculated as follows:

ROSI = (5*15000)*0.8 - 25000 = 140%

25000

Source: https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport

Information Security Management System

Information Security Management System (ISMS) is a set of policies concerned with information security management or IT-related risks. It includes managing people, processes, and IT systems by applying a security/risk management process.

An ISMS can help your organization manage the security of assets such as financial information, intellectual property, employee details, or information entrusted to you by third parties.

The best known standard providing the requirements for an ISMS is the ISO/IEC 27001.

Source: ISO/IEC 27001:2005

As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. ISO/IEC 27001:2005, therefore, incorporated the ‘Plan-Do-Check-Act’ (PDCA) or Deming cycle approach. The activities carried out in the four phases are:

Plan: This phase is about designing the ISMS, assessing information security risks, and selecting appropriate controls.

Do: This phase involves implementing and operating the controls.

Check: The objective of this phase is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.

Act: In this phase, changes are made, where necessary, to bring the ISMS back to peak performance.

Source: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

COBIT 5, a framework for the governance and management of enterprise IT, uses a very similar approach as PDCA (Plan - APO, Build - BAI, Run - DSS, Monitor - MEA).

- Align, Plan, and Organize (APO)
- Build, Acquire, and Implement (BAI)
- Deliver, Service, and Support (DSS)
- Monitor, Evaluate, and Assess (MEA)

Another competing standard for ISMS is Information Security Forum's Standard of Good Practice (SOGP). It is more best practice-based as it comes from ISF's industry experiences.

Some other best-known ISMSs are Common Criteria (CC) international standard and IT Security Evaluation Criteria (ITSEC).

- Some nations use their own ISMS, such as:
  - Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) of USA
  - Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) of USA and Trusted Computer System Evaluation Criteria (TCSEC) of USA
  - IT Baseline Protection Manual (ITBPM) of Germany
  - ISMS of Japan
  - ISMS of Korea and Information Security Check Service (ISCS) of Korea

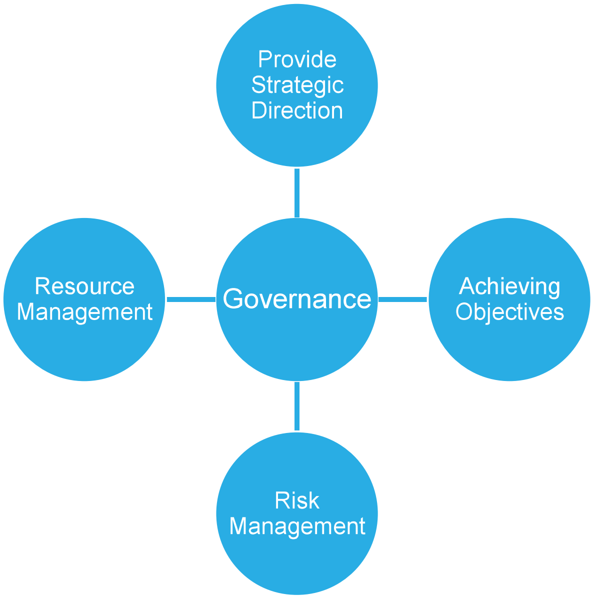
Other frameworks such as COBIT and ITIL touch on security issues, but are mainly geared toward creating a governance framework for information and IT more generally. COBIT has a companion framework “Risk IT”, which is dedicated to information security. ITIL has RESILIA best practice portfolio to address security and improve cyber resilience.

IT GOVERNANCE

Governance: Definition

Enterprise Governance: The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise’s resources are used responsibly.

IT Governance: IT governance is an integral part of Enterprise Governance and focuses on IT structures and processes to ensure that organization’s IT supports and extends the organization’s strategies and objectives.



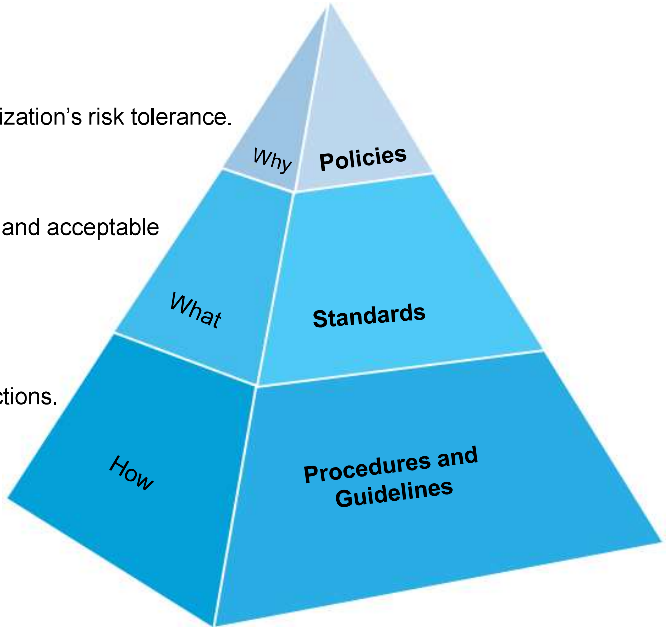
Source: http://www.isaca.org/Pages/Glossary.aspx

IT governance is a subset discipline of corporate governance, focused on IT and its performance and risk management. The interest in IT governance is due to:

- The on-going need within organizations to focus value creation efforts on an organization’s strategic objectives.
- Better manage the performance of those responsible for creating this value in the best interest of all stakeholders.

Governance Structure

The structure of a governance consists of three main components: policies, standards, and procedures and guidelines.



Sets the tone of an organization’s risk tolerance.

Defines mandatory performance criteria and acceptable levels of control.

Explains how to carry out policy in step by step directions.

Policies

Policies are high-level statements regarding principles and requirements that set the tone and temperament of management’s risk tolerance and direction for logical, physical, and managerial practices. A policy is a governing principle that provides the basis for standards and carries the highest authority in the organization. Policies are generally not technology, process, or vendor specific and therefore should not change frequently.

Standards

Standards provide detailed, mandatory performance criteria to ensure conformity with company policies. Standards define an acceptable level of control and associated measurable compliance criteria. Any deviation from a standard must be approved by management and be documented. Standards may be technology, process, and vendor-specific and, typically, require frequent maintenance.

Procedures and Guidelines

Procedures are detailed step-by-step activities and tasks that the personnel are required to follow when performing certain aspects of their job responsibilities. Standards may include corporate, local, and business unit specific procedures. Procedures are also structured into ‘Guidelines’ and typically require frequent maintenance.

IT Governance Practices and Standards

Over the years, a number of IT practices and standards have emerged. The following table depicts the common practices and standards for IT Governance.

Common Practices	Industry Standards
⇥ AICPA Privacy Framework ⇥ ISO/IEC 38500 ⇥ ISO 17799 ⇥ ISO 27001 ⇥ ISO 13335 ⇥ COBIT	⇥ Payment Card Industry (PCI) DSS ⇥ FISMA ⇥ HIPAA

Governance Regulatory Example

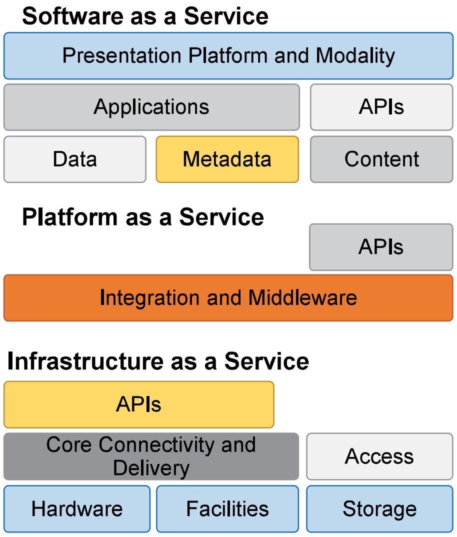
A common example of enterprise governance of information technology is ISO/IEC 38500 - an international standard published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 38500 provides a framework for effective IT governance to assist the organizations' policy maker to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organizations' use of IT. ISO/IEC 38500 is applicable to organizations of all sizes, including public and private companies, government entities, and not-for-profit organizations.

CLOUD COMPUTING SECURITY

Cloud Computing: Shared Security Responsibility

It is critical to recognize that security is a cross-cutting aspect of cloud computing, which spans across all layers of the various deployment/service models, ranging from physical security to application security.

The figure depicts the security aspects for different deployment/service models.

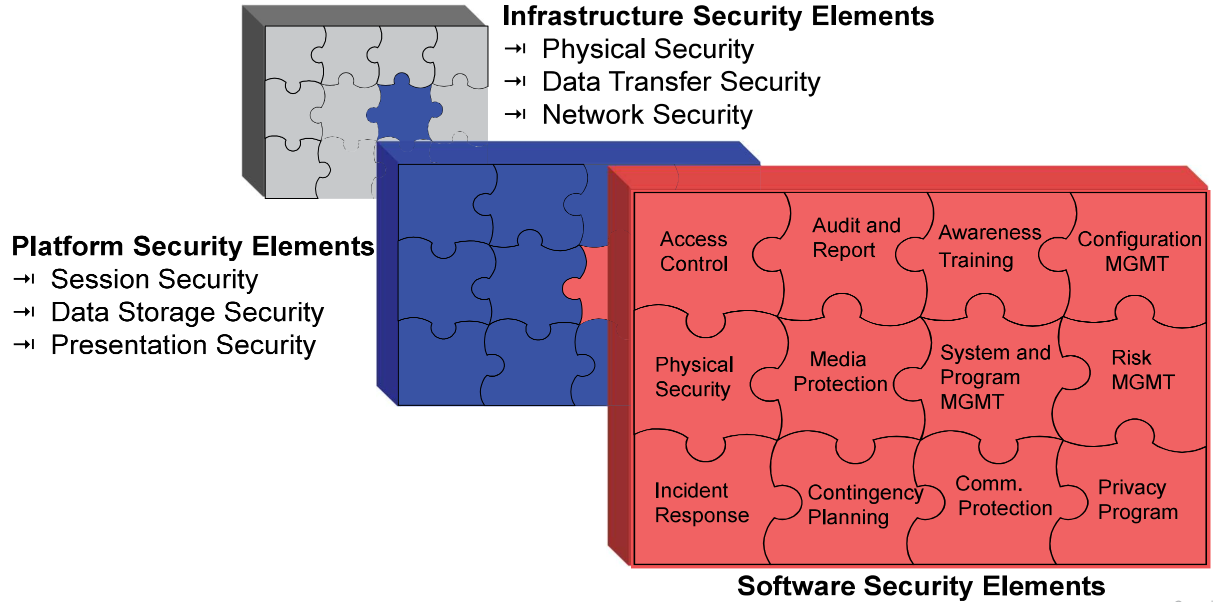

Software as a Service
Presentation Platform and Modality
Applications
APIs
Data
Metadata
Content
Platform as a Service
APIs
Integration and Middleware
Infrastructure as a Service
APIs
Core Connectivity and Delivery
Access
Hardware
Facilities
Storage

Source: Cloud reference architecture

In traditional IT systems, an organization has control over the whole stack of computing resources and entire lifecycle of the systems. However, in the cloud the security is not solely under the purview of the cloud providers but also depends on the cloud subscribers and other relevant services, for example, layered services. Cloud providers and cloud subscribers collaboratively design, build, deploy, and operate cloud-based systems. The split of control means both parties share the responsibilities in providing adequate protections to the cloud-based systems.

Security Risk Elements by Service Models

Each service model has specific security elements and considerations, but it takes a 'Shared Security Responsibility' approach to be successful. The following figure is a visual example of the different security elements within the various service models.



Infrastructure Security Elements

- Physical Security
- Data Transfer Security
- Network Security

Platform Security Elements

- Session Security
- Data Storage Security
- Presentation Security

Software Security Elements

Risks to Consider in the Cloud

Despite the existence of different deployment and service models, there are few generic considerations related to the deployment of cloud services. The following key risk questions should be considered before deployment of cloud services.

Governance, Risk, and Compliance

- How will we monitor usage of the cloud and avoid taking on unacceptable risks or getting into compliance hot water?
- How do we provide proper assurance to our auditors and regulators?

Business Transformation

- Will cloud fundamentally change the business?
- Do new license models need to be created to be compatible with a cloud computing model?

Security and Privacy Risks

- How is our data controlled throughout its lifecycle while in a shared environment?
- How can we protect against unauthorized usage or sharing?

Industry Risks

- Will industry specific regulatory changes impact how we use cloud computing?

Operational Risks

- How do we manage rapid SaaS application changes?
- Do processes and procedures need to change?
- What are the new roles and responsibilities and who take them up?

Some prominent risk aspects that should be considered in the cloud are as follows:

- **Environmental security**: The concentration of computing resources and users in a cloud computing environment also represents a concentration of security threats. Because of their size and significance, cloud environments are often targeted by virtual machines and bot malware, brute force attacks, and other attacks. Ask your cloud provider about access controls, vulnerability assessment practices, and patch and configuration management controls to see that they are adequately protecting your data.

- **Data privacy and security**: Hosting confidential data with cloud providers involves the transfer of a considerable amount of an organization's control over data security to the provider. It is important that cloud provider understands the consumer's data privacy and security needs. Also, the cloud provider should be aware of particular data security and privacy rules and regulations that apply to the consumer entity, such as HIPAA, the Payment Card Industry Data Security Standard (PCI DSS), the Federal Information Security Management Act of 2002 (FISMA), or the privacy considerations of Gramm-Leach-Bliley Act.

- **Data availability and business continuity**: A major risk to business continuity in the cloud computing environment is loss of Internet connectivity. If a vulnerability is identified, you may have to terminate all access to the cloud provider until the vulnerability is rectified. Additionally, the seizure of a data-hosting server by law enforcement agencies may result in the interruption of unrelated services stored on the same machine.

- **Record retention requirements**: If your business is subject to record retention requirements, make sure your cloud provider understands what they are and so they can meet them.

- **Disaster recovery**: Hosting your computing resources and data at a cloud provider makes the cloud provider's disaster recovery capabilities vitally important to your company's disaster recovery plans. Know your cloud provider's disaster recovery capabilities and ask your provider if they been tested.

- **Loss of governance**: For using cloud infrastructures, the client necessarily cedes control to the cloud provider on a number of issues that may affect security. At the same time, Service Level Agreements may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defenses. This also includes compliance risks because investment in achieving a required certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud.

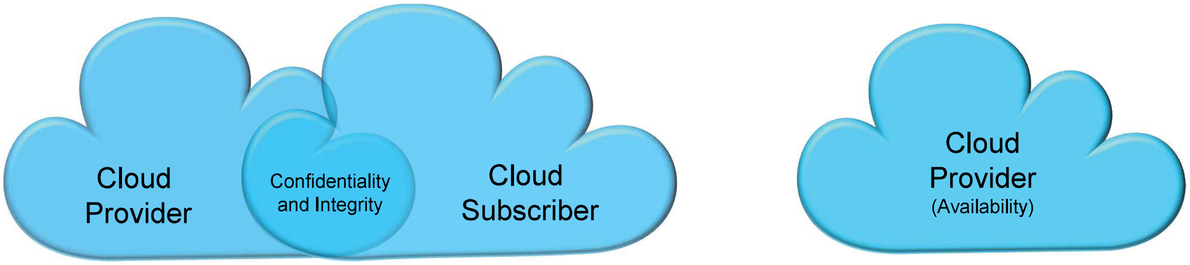
- **Malicious insider**: Although less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

- **Isolation failure**: Multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and reputation between different tenants (for example, the so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (for example, against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.

CIA Within the Cloud

The CIA protection goals that form the basis for the security requirements must be fulfilled by IT systems in general.

Within cloud computing systems, the CIA protections methodologies have split responsibilities or a shared security responsibility depending on the type of service model being deployed.



The implementation of CIA within the cloud is explained as given:

- **Confidentiality**: Confidentiality within a cloud environment may be shared between the provider and subscriber or may be a dual or inherited security process.
- **Integrity**: Integrity within the cloud may also be a shared element that needs to be considered as a part of cloud service deployment.
- **Availability**: Availability is usually a cloud provider responsibility across all service and deployment models.

Multi-Tenancy

Multi-tenancy refers to a principle within software architecture where a single instance of the software runs on a server, serving multiple client-organizations (tenants).

It contrasts with multi-instance architectures where separate software instances (or hardware systems) operate on behalf of different client organizations.

With a multi-tenant architecture, a software application is designed to virtually partition its data and configuration, and each client organization works with a customized virtual application.

Difference with Virtualization

In a multi-tenancy environment, multiple customers share the same application, running on the same operating system, on the same hardware, with the same data-storage mechanism.

The distinction between the customers is achieved during application design, thus customers do not share or see each other's data.

Compare this with virtualization where components are abstracted enabling each customer application to appear to run on a separate virtual machine.

Multi-tenancy in the Cloud

Multi-tenancy in the cloud means sharing of resources and services to run software instances serving multiple consumers and client organizations (tenants). It means physical resources (such as computing, networking, and storage) and services are shared. The administrative functionality and support may also be shared. One of the big drivers for providers is to reduce cost by sharing and reusing resources among tenants.

Security Risks Within Multi-Tenancy Design

Some of the security risks within multi-tenancy design are:

- **Inadequate logical security controls**: Physical resources (CPU, networking, storage and databases, and application stack) are shared between multiple tenants.
- **Malicious or ignorant tenants**: If the provider has weaker logical controls between tenants, a malicious or an ignorant tenant may reduce the security posture of other tenants.
- **Shared services can become single point of failure**: If the provider has not architected the common services well, they can easily become single point of failure, due to misuse or abuse by a tenant.
- **Uncoordinated change controls and misconfigurations**: When multiple tenants are sharing the underlying infrastructure, all changes need to be well coordinated and tested.
- **Comingled tenant data**: To reduce cost, providers may be storing the data from multiple tenants in the same database table-spaces and backup tapes.

Specific risks by service model include:

- **SaaS**: Multiple clients (tenants) may be sharing the same application stack (database, app and web servers, and networking).
- **PaaS**: Platform stack is shared among the tenants. Vulnerability in the platform stack can allow bleeding among tenants, shared data backups, and archives.
- **IaaS**: Cross network traffic listening. Core residents with lower security posture, where they are less concerned about keeping their hosts hardened and patched.

Cloud Risk Considerations

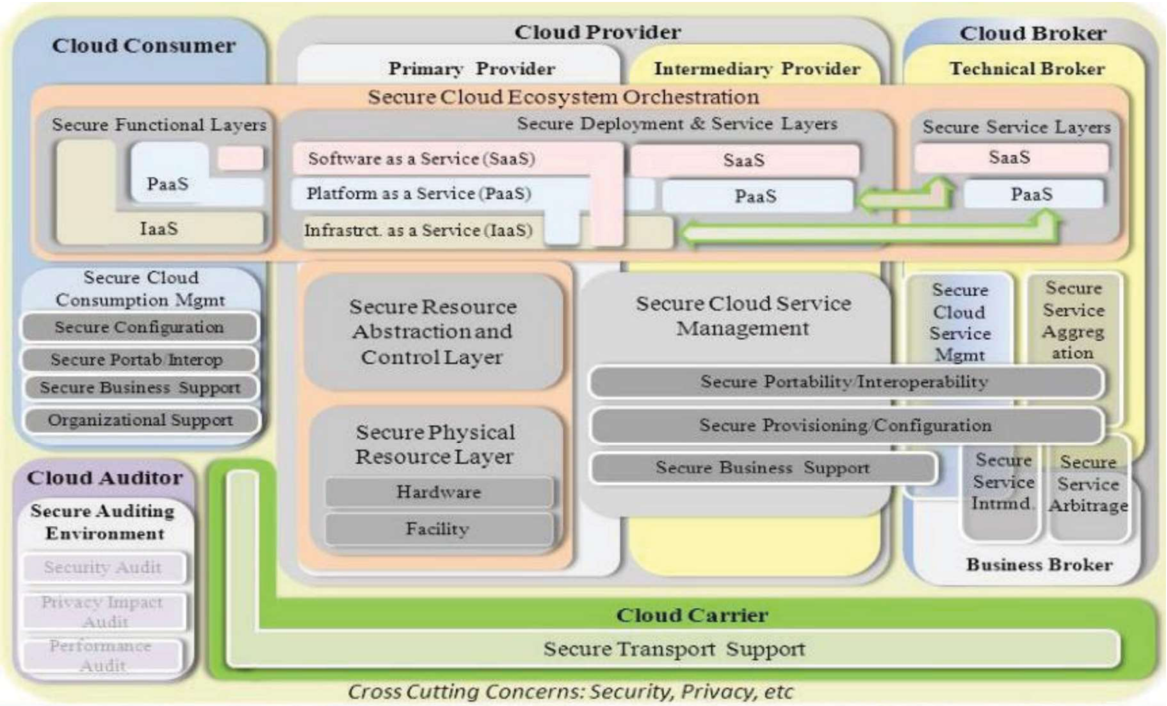
The table includes the high-level considerations for cloud computing from different aspects:

Governance and Compliance	⇥ Monitoring usage of cloud ⇥ Monitoring compliance with regulatory requirements ⇥ Compliance with multijurisdictional data privacy laws
Privacy and Data Protection	⇥ Delineating ownership of data across organizational lines ⇥ Managing access to appropriate levels of data ⇥ Implementing data storage and retention policies at the cloud vendor
Security Incident Response	⇥ Managing incident investigations in a virtualized environment ⇥ Limiting incident spill over to multiple cloud tenants ⇥ Handling complicated troubleshooting due to continuous environment changes
Access Control	⇥ Access controls for cloud management interfaces ⇥ Access controls for segregation of duties ⇥ Due diligence prior to assignment of access privileges
Vulnerability Management	⇥ Managing virtualization induced vulnerabilities ⇥ Ensuring timely security patches ⇥ Adequate vulnerability testing of cloud components
Vendor Management	⇥ Obtaining assurance on cloud vendor’s solution ⇥ Monitoring vendor’s performance ⇥ Building in the cloud portability and interoperability

Geography	Given various countries and regulatory authorities, controls for supporting appropriate cross border data views/use must be maintained.
Ownership, Rights, and Obligations	Clear establishment of rights and obligations associated with data assets must be established. Often rights and obligations are dependent on the physical location of the data owner, custodian, and user. Designing and implementing effective controls to support appropriate rights and obligations may be complex.
Multi-Tenancy	In a multi-tenant cloud environment, users may access shared resources, possibly gaining unauthorized access or may attack other tenants. This may have less risk in a private cloud, but more risk in a vendor-hosted cloud.
Data Seizures	In a cloud provider environment, server seizures for one customer may include other customer, simply because they were on the same physical server. Seizing the hardware may lead to data loss or data disclosure of other customers in multi-tenant storage models.
Data Loss	On ephemeral or transient systems, a cloud-vendor-provider-instance-failure may lead to permanent loss of system information, including system configuration and data stored locally.
Ephemeral and Transient Systems	'Disposable' server concept challenges the role of change control.

Cloud Computing Security Reference Architecture

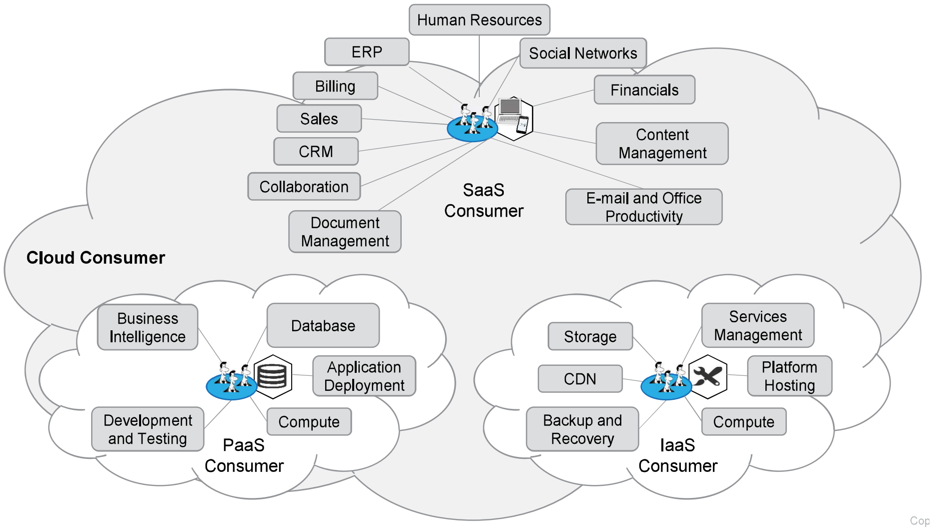
The Cloud Computing Security Reference Architecture formal model is derived from the NIST Reference Architecture (NIST RA).


Cloud Consumer
Cloud Provider
Cloud Broker
Primary Provider
Intermediary Provider
Technical Broker
Secure Cloud Ecosystem Orchestration
Secure Functional Layers
Secure Deployment & Service Layers
Secure Service Layers
PaaS
IaaS
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastrct. as a Service (IaaS)
SaaS
PaaS
SaaS
PaaS
Secure Cloud Consumption Mgmt
Secure Configuration
Secure Portab/Interop
Secure Business Support
Organizational Support
Secure Resource Abstraction and Control Layer
Secure Physical Resource Layer
Hardware
Facility
Secure Cloud Service Management
Secure Portability/Interoperability
Secure Provisioning/Configuration
Secure Business Support
Secure Cloud Service Mgmt
Secure Service Aggregation
Secure Service Intrmd.
Secure Service Arbitrage
Business Broker
Cloud Auditor
Secure Auditing Environment
Security Audit
Privacy Impact Audit
Performance Audit
Cloud Carrier
Secure Transport Support
Cross Cutting Concerns: Security, Privacy, etc

Source: NIST SP 500-292: NIST Cloud Computing Reference Architecture

Consumer: Cloud Computing Security Reference Architecture

The following figure shows the consumer cloud computing security reference architecture by model and access elements. Cloud consumers need Service Level Agreements (SLAs) to specify the technical requirements fulfilled by a cloud provider.



A few important points to be considered are:

- SaaS applications in the cloud are made accessible through a network to the SaaS consumers.
- PaaS can employ the tools and execution resources provided by cloud providers to develop, test, deploy, and manage the applications.
- IaaS subscribers have access to virtual computers, network-accessible storage, network infrastructure components, and other fundamental computing resources on which they can deploy and run arbitrary software.

Cloud Provider: Cloud Computing Security Reference Architecture

A cloud provider is an organization responsible for making a service available to subscribers. It provides the following services:

- **Software as a Service**: The cloud provider deploys, configures, maintains, and updates the operation of the software applications on a cloud infrastructure. The SaaS provider assumes most of the responsibilities in managing and controlling the applications and the infrastructure, while the cloud consumers have limited administrative control of the applications.
- **Platform as a Service**: The cloud provider manages the computing infrastructure for the platform and runs the cloud software, which provides the components of the platform, such as runtime software execution stack, databases, and other middleware components.
  - The PaaS cloud provider typically also supports the development, deployment, and management process of the PaaS cloud consumer by providing tools such as Integrated Development Environments (IDEs), development version of cloud software, Software Development Kits (SDKs), deployment, and management tools.

- **Infrastructure as a Service**: The cloud provider acquires the physical computing resources underlying the service, including the servers, networks, storage, and hosting infrastructure. The cloud provider runs the cloud software necessary to make computing resources available to the IaaS cloud consumer through a set of service interfaces and computing resource abstractions, such as virtual machines and virtual network interfaces.
  - IaaS cloud consumer, in turn, uses these computing resources, such as a virtual computer, for their fundamental computing needs compared to SaaS and PaaS cloud consumers. An IaaS cloud consumer has access to more fundamental forms of computing resources and thus has more control over the more software components in an application stack, including the OS and network.

Exercise: Cloud Computing Security

Explain the risks and the impacts of cloud computing in terms of both business and technical security challenges and their effect on business and technical governance and policy.

Outcome:

This exercise will enable you to look at a business and identify the risks of cloud computing.

Sample Answer

Business risks and impacts:

- **Lock-in and data portability**: Lock-in refers to the inability of a cloud consumer to move their data away from a cloud service provider. In addition, data portability issues can hinder to change the service provider.
- **Data security and privacy**: The data integrity, confidentiality and privacy is a major challenge of cloud computing.
- **Data storage location**: The location of data storage may hinder compliance to government and other regulatory bodies. Cloud computing introduces the risk that data belonging to one organization may be stored in several locations and coexist with another organization's data.
- **Loss of governance**: Loss of governance to cloud service providers is perceived as a potential security risk by organizational leaders. Businesses are exposed to many types of risks when they entrust their data to a third party. The impact from the loss of control may lead to the inability to comply with security requirements, a lack of confidentiality, availability, and integrity of data, a decline in the performance and quality of service.

Technical risks and impacts:

- **Availability of service**: Availability of service can be a major challenge in cloud computing. The cloud computing service can be impacted because of various reasons such as use of cheap commodity hardware and network downgrade.
- **Resource exhaustion**: Cloud computing services are on-demand and resources are allocated by the cloud service provider based on statistical projection. There is a potential of calculated risk and high performance computing applications and transactional database systems may lead to performance unpredictability and/or resource exhaustion.
- **Distributed Denial of Service**: Cloud computing systems are easy target for attackers and transmission of viruses or the victims of a hack

MODULE SUMMARY

The module includes the following topics.

Cloud Computing Basics

- Cloud Computing Primer: What is the Cloud?
- Characteristics of Cloud Computing
- Cloud Service Models
- Cloud Deployment Models
- Cloud Reference Models

Information Security Management

- Information Security: Definition
- The CIA Principle
- Security Management
- Assets, Threats, Vulnerability, and Risk
- Risk Assessment
- Risk Assessment Result Matrix
- Executive Risk Treatment and Remediation Plan: Example
- Security Assessment
- Security Management Lifecycle
- Return on (Security) Investment
- Return on Security Investment: Example
- Information Security Management System

IT Governance

- Governance: Definition
- Governance Structure
- IT Governance Practices and Standards

Cloud Computing Security

- Cloud Computing: Shared Security Responsibility
- Security Risk Elements by Service Models
- Risks to Consider in the Cloud
- CIA Within the Cloud
- Multi-Tenancy

- Security Risks Within Multi-Tenancy Design
- Cloud Risk Considerations
- Cloud Computing Security Reference Architecture
- Consumer: Cloud Computing Security Reference Architecture
- Cloud Provider: Cloud Computing Security Reference Architecture