**Security, Privacy Considerations of Cloud**

1. **What Is Security?**

The quality or state of being secure – to be free from danger.

• To be protected from adversaries

• A successful Cloud implementation should have multiple layers of security in place:

• Physical security

• Personal security

• Operations security

• Communications security

• Network security

1. **What is Information Security? CIA**

Information Security refers to the protection of information and its critical elements (**confidentiality, integrity and availability**), including the *systems* and *hardware* that use, *store*, and *transmit* that information.

• **Policy**, **Training**, and **Awareness** programs and Technology are vital concepts in Information Security Management

1. **Key terms of Information Security**

Elements that affect the value of information:

• **Confidentiality • Integrity • Availability**  • Privacy • Identification • Authenticity • Authorization • Accountability (Non-repudiation) • Risk • Vulnerability, Threat, Attack, Security Breach

***Confidentiality:*** The characteristic of information whereby only those with sufficient privileges may access certain information.

***Measures used to protect confidentiality***:

• Information classification

• Secure document storage

• Application of general security policies

• Education of information custodians and end users

***Integrity:*** The quality or state of being whole, complete, and uncorrupted.

• Information integrity is threatened if exposed to corruption, damage, destruction, or other disruption of its authentic state.

• Corruption can occur while information is being compiled, stored, or transmitted.

***Availability***: The characteristic of information that enables user access to information in a required format, without interference or obstruction.

• A user may be a person or another computer system.

• Availability does not imply that the information is accessible to any user, it implies availability to authorized users.

***Privacy***: Information *collected*, *used*, and *stored* by an organization is to be used only for the purposes stated to the data owner at the time it was collected.

• Information will be used only in ways known to the person providing it

***Identification***: An information system possesses the characteristic of identification when it is able to recognize individual users.

• *Identification and* ***authentication*** are essential to establishing the level of access or authorization that an individual is granted.

***Authentication***

• Occurs when a control proves that a user possesses the identity that he or she claims.

***Authorization***

• Assures that the user has been *specifically* and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset.

• A user may be a person or a computer.

• Authorization occurs after authentication.

***Accountability (Non-repudiation)***

• Exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process.

• *Non-repudiation*: that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

• Risk: is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset).

• Vulnerability: is a weakness that could be used to endanger or cause harm to an informational asset.

• Threat: is anything (man-made or act of nature) that has the potential to cause harm.

• Attack is carrying out a threat and using a vulnerability to inflict harm

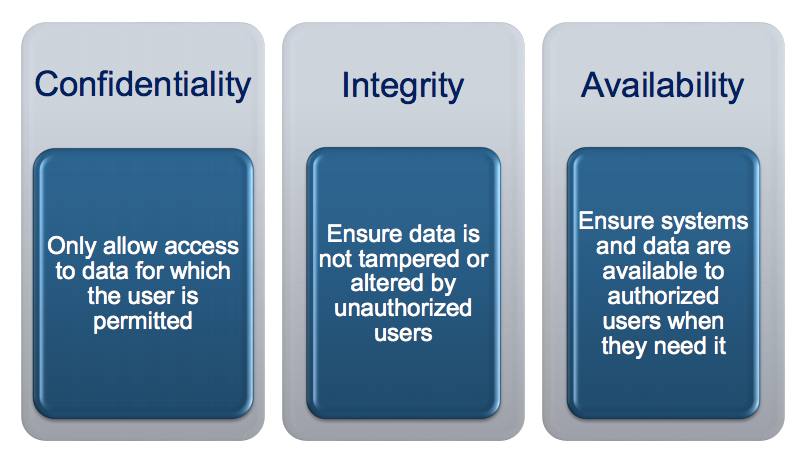
• The likelihood that a threat will use a vulnerability to cause harm creates a risk.

• When a threat does use a vulnerability to inflict harm (an attack), it has an impact.

• In the context of information security, the impact is a loss of Confidentiality, Integrity or Availability, and possibly other losses (lost income, loss of life, loss of real property).

• It is not possible to identify all risks, nor is it possible to eliminate all risk.

Every occurrence in which sensitive, protected or confidential information has potentially been viewed, stolen or used through unauthorized means and that the confidentiality, integrity and availability of the information has been inappropriately compromised, can be considered a Security Incident. A Security Incident, once confirmed, becomes a Security Breach.



**CLOUD COMPUTING GOVERNANCE**

**Cloud Business Governance: Cloud computing requires an appropriate *IT Governance* Model to ensure a secured computing environment and to comply with all relevant organizational information technology policies.**

**Governing**:

Governing is the steering (conduz) of the enterprise and demands strategic leadership.

• It sets limits which an enterprise operates in and is implemented with processes to **monitor performance**, **describe activities** and **achieve compliance**, while providing adaptability to emergent conditions.

**Governing ensures that objectives are determined and defined, risks are managed appropriately and that the enterprise’s resources are used responsibly.**

**Governance Goals & Objectives**

• Assures that the investments in IT generate business value.

• Mitigates the risks associated with IT by implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, infrastructure, etc.

**Organization, Design & Strategy**

An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.

• Strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued.

• Design defines how the organization implements its strategy.

• Processes, culture and architecture are important to determining the design.

**Fostering a Governance Culture**

• Alignment of Business and Technology Goals

• Information Security supports the business goals of the organization.

• Aligns Senior Management to the end user.

• It is practical and provides *real*, *measurable* risk reduction.

• Risk-based Approach

• Assess actual risks and threats to the enterprise.

• Implement security controls and protection based on requirements.

• Information security must clearly understand the business and its operating environment to select appropriate controls to mitigate risks.

**Cloud Business Governance**

Organizations need a set of essential capabilities to effectively implement and manage cloud services.

Cloud Services

• Demand management

• Relationship management

• Data security management

• Application lifecycle management

• Risk and compliance management

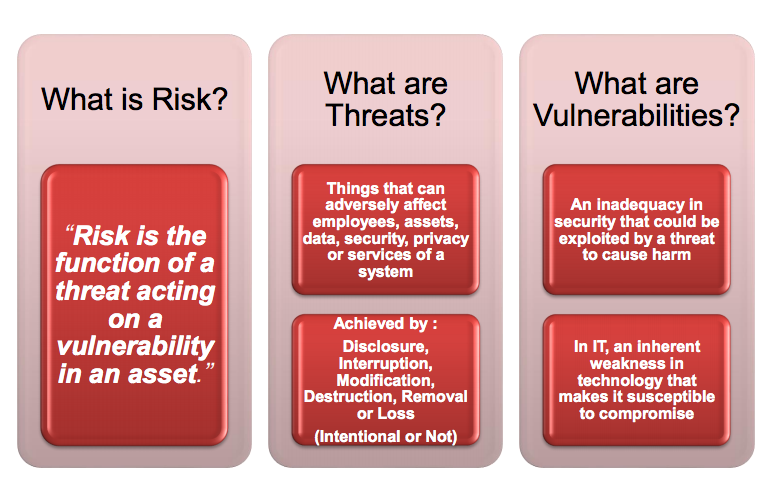
**Cloud Industry Governance Risks**

A danger lies with the explosion of companies joining the growth in cloud computing by becoming providers:

• Many of the infrastructural and logistical concerns regarding the operation of cloud computing businesses are still unknown.

• Over-saturation may have ramifications for the industry as whole.

**What is Risk?**



**A Risk Assessment is a way to:**

1. Inventory assets
2. Estimate what are the probable threats to each of the assets.
3. Predict the vulnerabilities in the protection of these assets.
4. Identify the safeguards in place to protect the vulnerabilities.
5. Calculate the risk level that is acceptable.

**AUDITS, ASSESSMENTS AND CERTIFICATIONS**

Transparency & Trust

When it is time for a business to start evaluating service providers against its needs, there is a very important factor to consider: transparency.

Cloud computing is much more than just buying IT hardware or software.

• It is about engaging a service that may be entrusted to manage critical assets and services, and there may be little day-to-day visibility of how this occurs. But, businesses can and should ensure a level of transparency.

With a traditional IT model (either on-premise or for many outsource arrangements), getting visibility is usually a case of commissioning an audit, either by internal auditors or by an outside party. For cloud services, this option is much less likely to be available or even practical, as the cloud service provider’s processing may be distributed throughout the world.

Alternative methods of gaining visibility of security and control will often be needed. There are several methods available, and, recognizing the need to establish trust, cloud providers are investing more and more in providing the information their customers need. This is an area that is likely to grow and evolve, and maybe one day a single common standard will be in place.

Cloud Computing Transparency Nondisclosure agreements

Many cloud providers are protective of information about their architecture, security and controls. Recognizing a prospective customer’s legitimate need to know these details, they will share limited information upon signing a nondisclosure. An NDA sheds valuable light on the provider’s services. Bear in mind that this information may or may not have been independently verified.