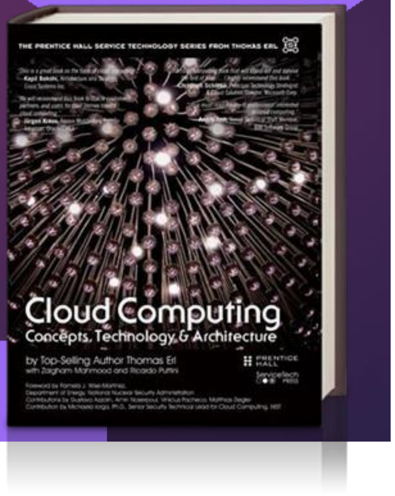
Cloud Computing

Concept, Technology & Architecture

CHAPTER 06

FUNDAMENTAL CLOUD SECURITY


THE PRENTICE HALL SERVICE TECHNOLOGY SERIES FROM THOMAS ERL
Cloud Computing
Concepts, Technology & Architecture
by Top-Selling Author Thomas Erl
with Zaigham Mahmood and Ricardo Puttini
PRENTICE HALL

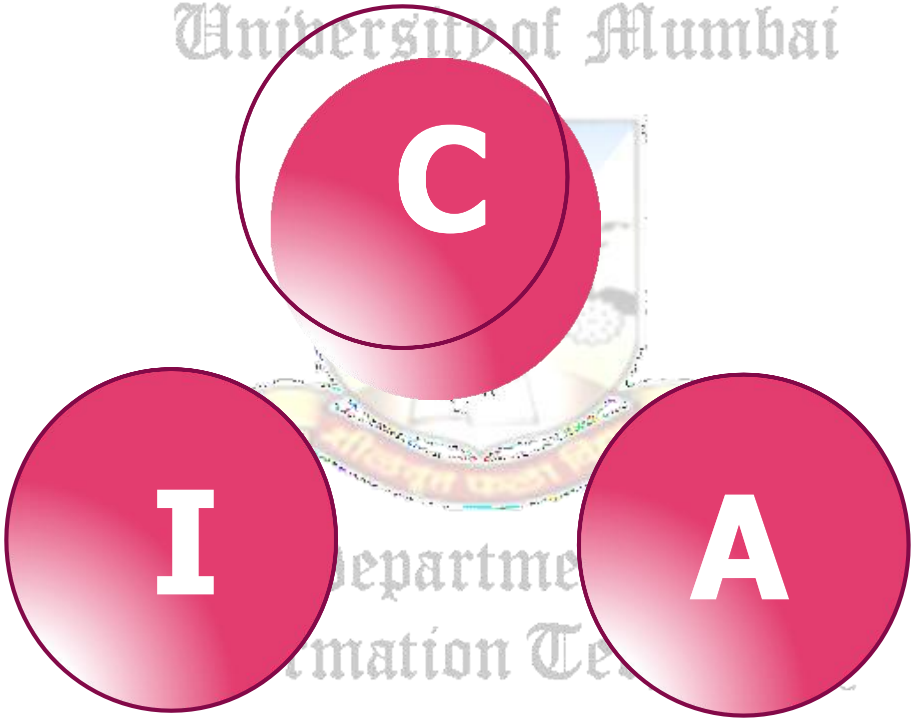
Contents

- This chapter introduces terms and concepts that address basic information security within clouds, and then concludes by defining a set of threats and attacks common to public cloud environments.

- 6.1 Basic Terms and Concepts
- 6.2 Threat Agents
- 6.3 Cloud Security Threats
- 6.4 Additional Considerations

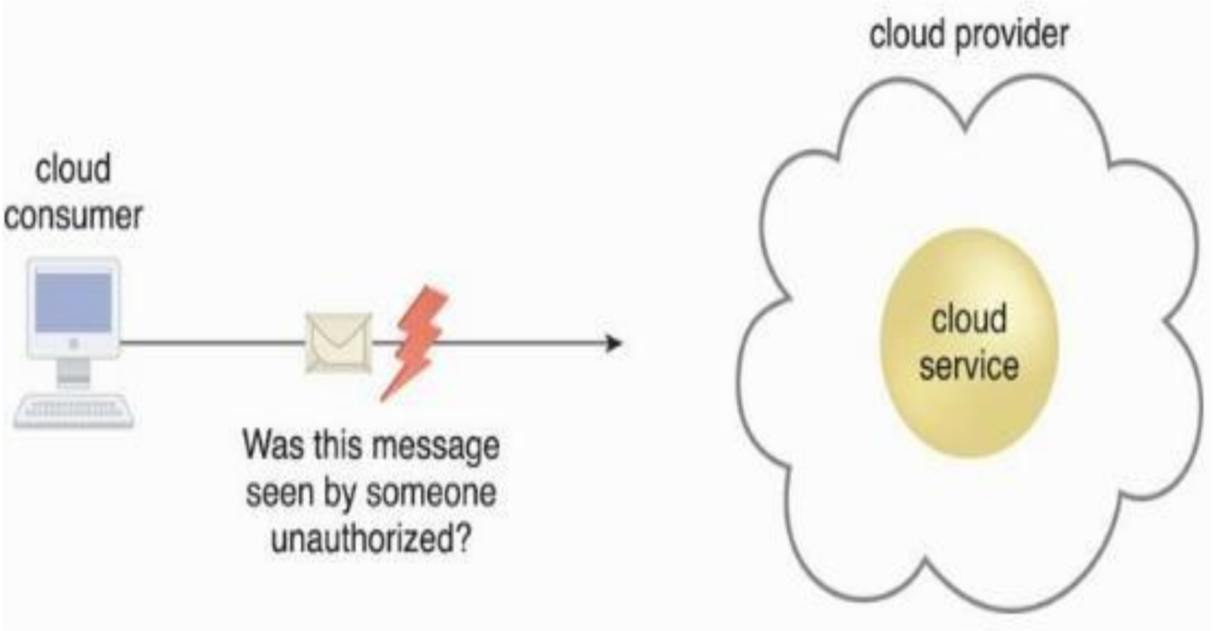
6.1. Basic Terms and Concepts

- Information security is a complex ensemble of
  - techniques,
  - technologies, regulations, and
  - Behaviors
- that collaboratively protect the integrity of and access to computer systems and data.
- IT security measures aim to defend against threats and interference that arise from both malicious intent and unintentional user error.


C
I
A

Confidentiality

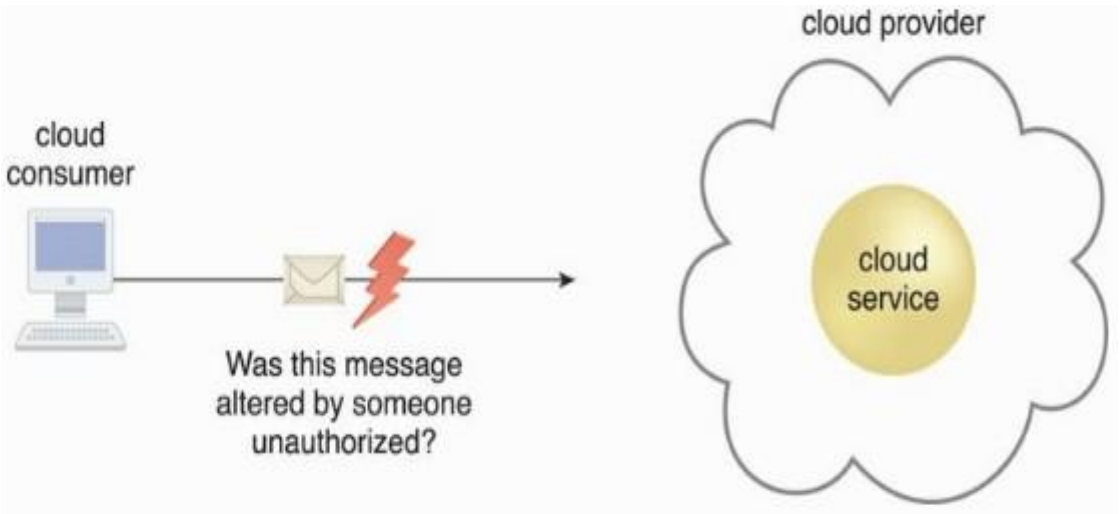
- The characteristic of something being made accessible only to authorized parties.



Within cloud environments, confidentiality primarily pertains to restricting access to data in transit and storage

Integrity

- The characteristic of not having been altered by an unauthorized party.



Important issue that concerns data integrity in the cloud is whether a cloud consumer can be guaranteed that the data it transmits to a cloud service matches the data received by that cloud service.

Integrity can extend to how data is stored, processed, and retrieved by cloud services and cloud-based IT resources.

Authenticity

- The characteristic of something having been provided by an authorized source. This also encompasses non-repudiation.
- Non-repudiation?
  - The inability of a party to deny or challenge the authentication of an interaction.

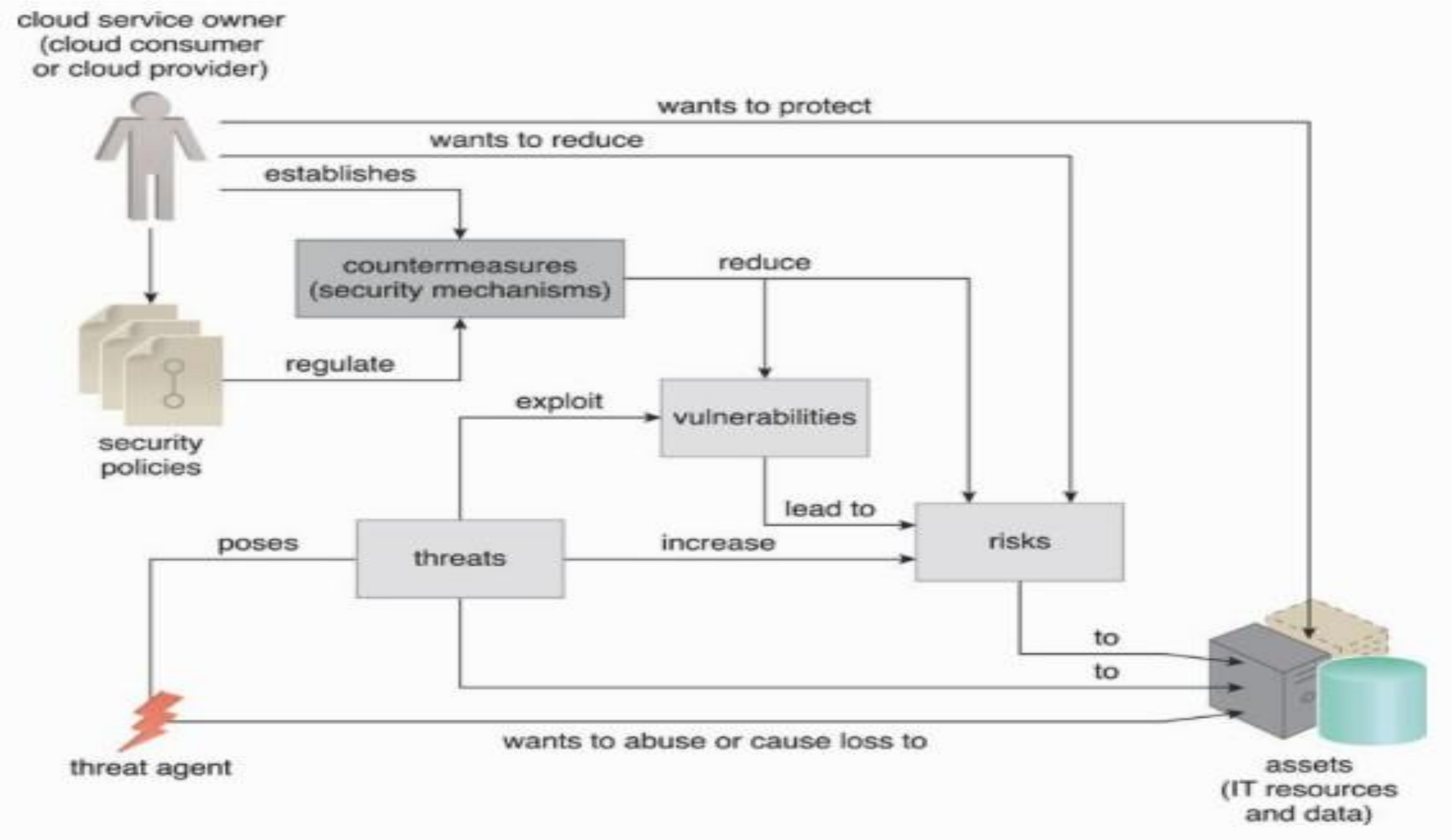
Other Relevant Terms

- ❑ **Availability** - being accessible and usable during a specified time period.
- ❑ **Threat** - a potential security violation that can challenge defenses in an attempt to breach privacy and/or cause harm.
- ❑ Vulnerabilities - a weakness that can be exploited either because it is protected by insufficient security controls.
- ❑ **Risk** - the possibility of loss or harm arising from performing an activity.

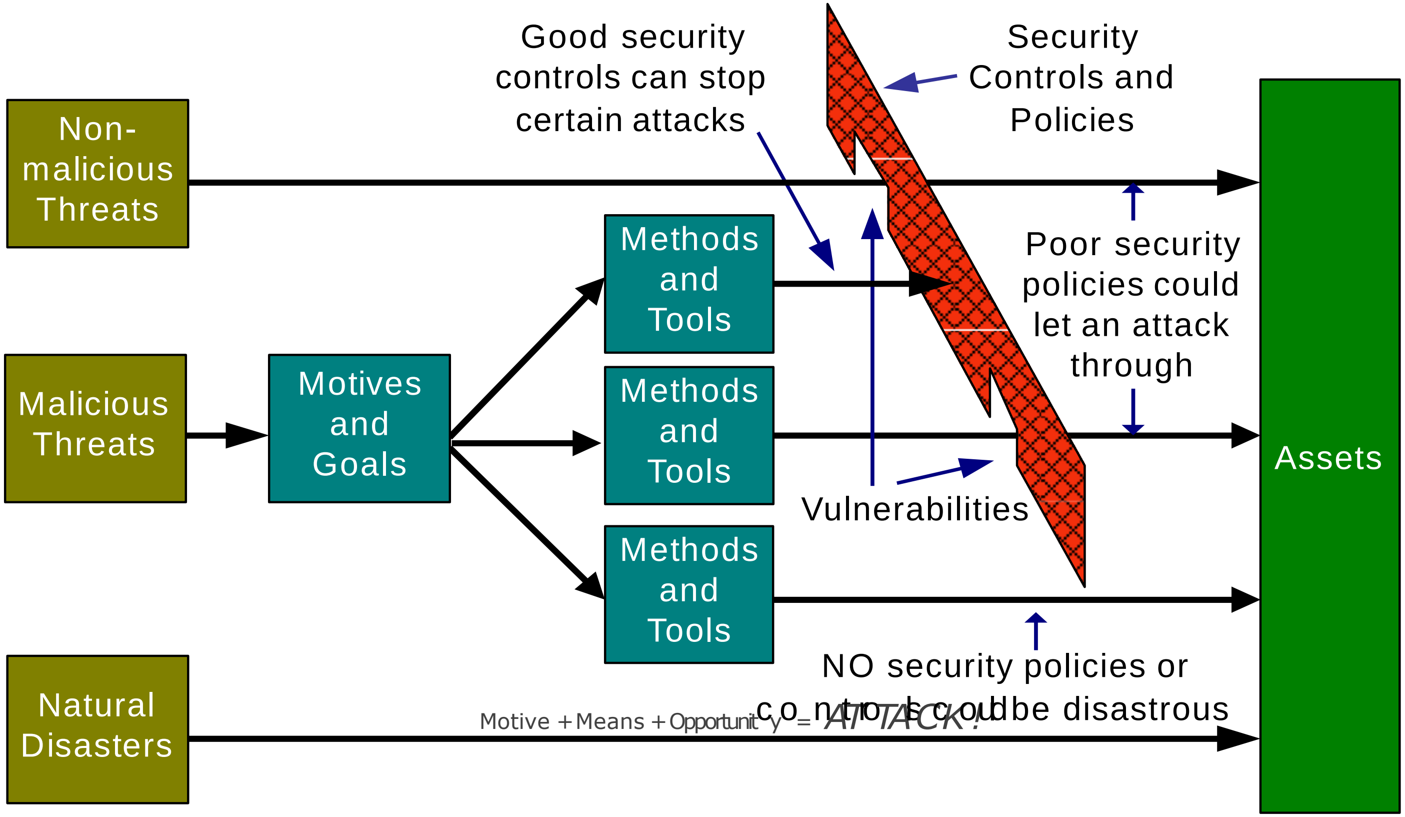
Other Relevant Terms (2)

- **Security Controls** - countermeasures used to prevent or respond to security threats and to reduce or avoid risk.
- **Security Mechanisms** - components comprising a defensive framework that protects IT resources, information, and services.
- **Security Policies** - a set of security rules and regulations that enforce security controls and mechanisms.

Figure 6.3. How security policies and security mechanisms are used to counter threats, vulnerabilities, and risks caused by threat agents.



The Ingredients of an Attack



Good security controls can stop certain attacks

Security Controls and Policies

Poor security policies could let an attack through

NO security policies or controls could be disastrous

Motive + Means + Opportunity = *ATTACK!*

6.2. Threat Agents
Common Threat Agents

- A treat agent?
  - an entity that poses a threat because it is capable of carrying out an attack.
- Originated from?
  - either internally or externally, from humans or software programs.
- Relationship?

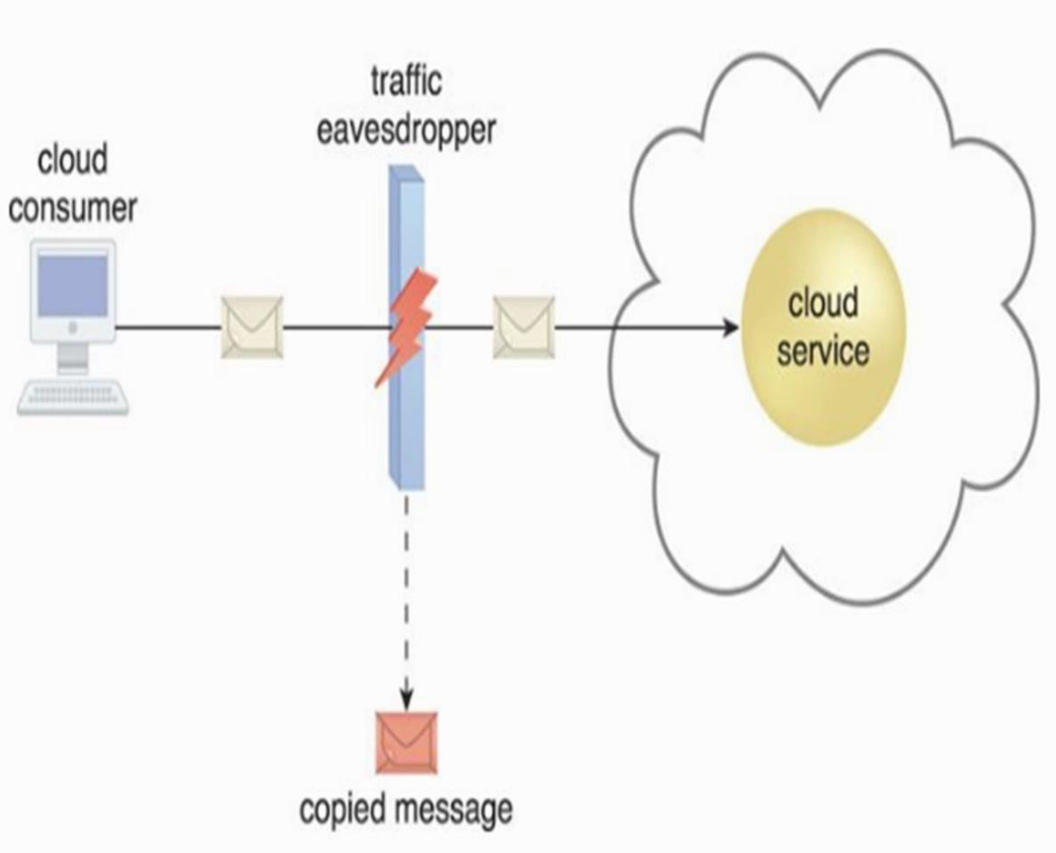
Types of Threat Agents/Attackers

- **Anonymous Attackers** - a non-trusted cloud service consumer without permissions in the cloud (typically external software programs).
- **Malicious Service Agent** - a service agent (or a program pretending to be a service agent) with compromised or malicious logic.
- **Trusted Attacker** - attacks from within a cloud's trust boundaries by abusing legitimate credentials.
- **Malicious Insider** - threat agents acting on behalf of or in relation to the cloud provider. They are typically current or former employees or third parties with access to the cloud provider's premises.

Anonymous Attacker

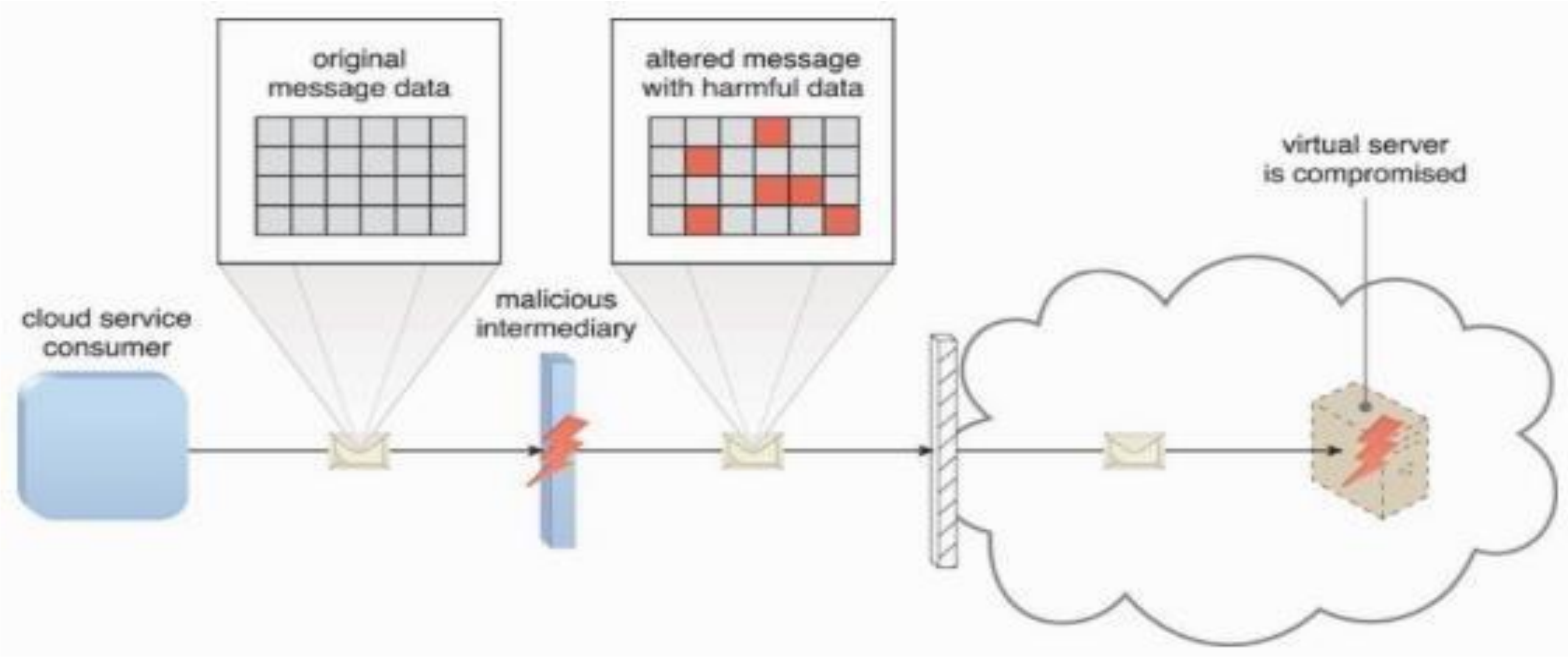
- An anonymous attacker is a non-trusted cloud service consumer without permissions in the cloud .
- It typically exists as an external software program that launches network-level attacks through public networks. When anonymous attackers have limited information on security policies and defenses, it can inhibit their ability to formulate effective attacks.
- Therefore, anonymous attackers often resort to committing acts like bypassing user accounts or stealing user credentials, while using methods that either ensure anonymity or require substantial resources for prosecution.

6.3. Cloud Security Threats



- **Traffic Eavesdropping** – data is passively intercepted by malicious service agents.
- Gather information to directly compromise confidentiality, e.g., username and password.

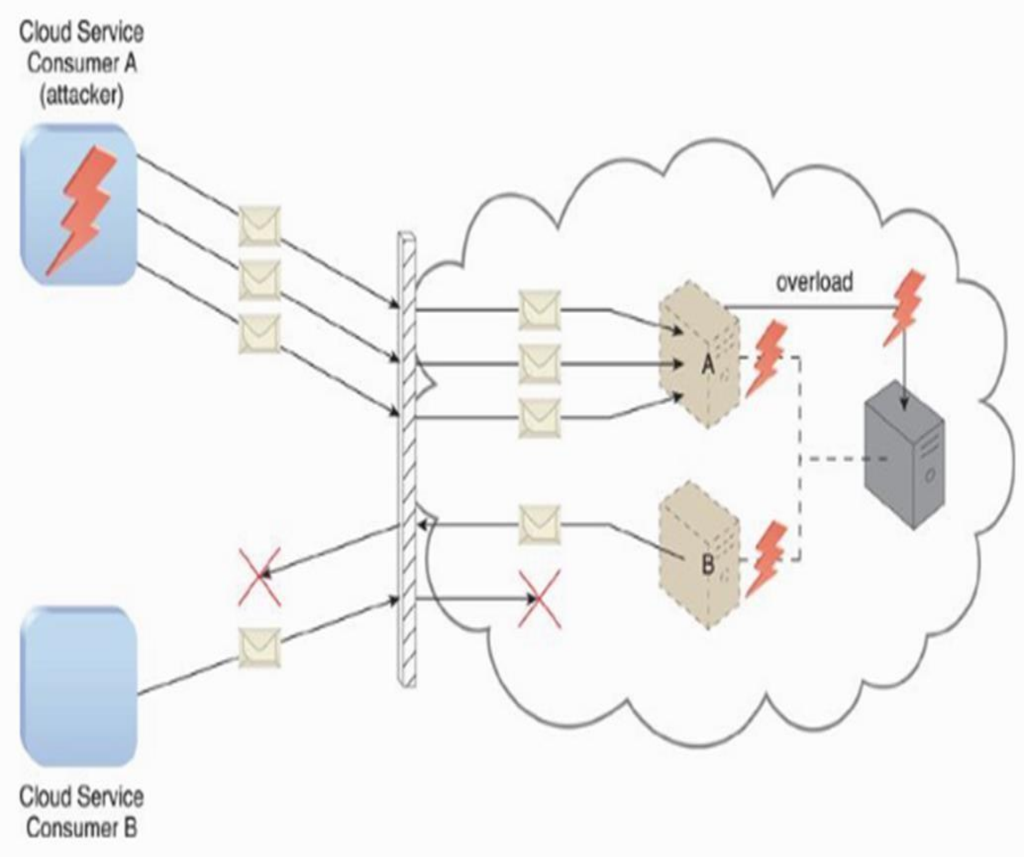
Malicious Intermediary



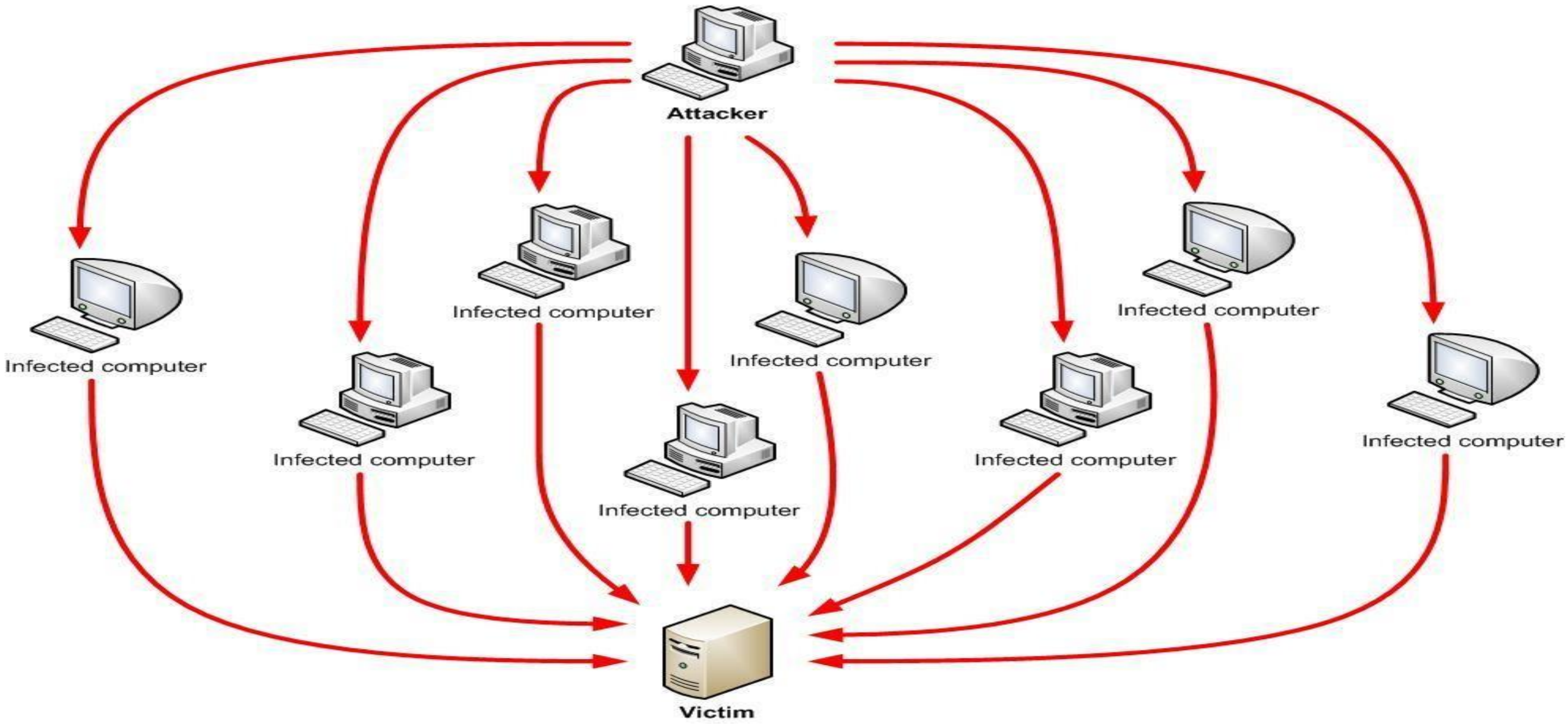
- This attack arises when messages are intercepted and altered by a malicious service agent.

Denial of Service

- To overload IT resources to the point where they cannot function properly.
  - Workload increased (CPU, memory loads)
  - Network traffic increased
- Successful DoS attacks produce server degradation and/or failure.

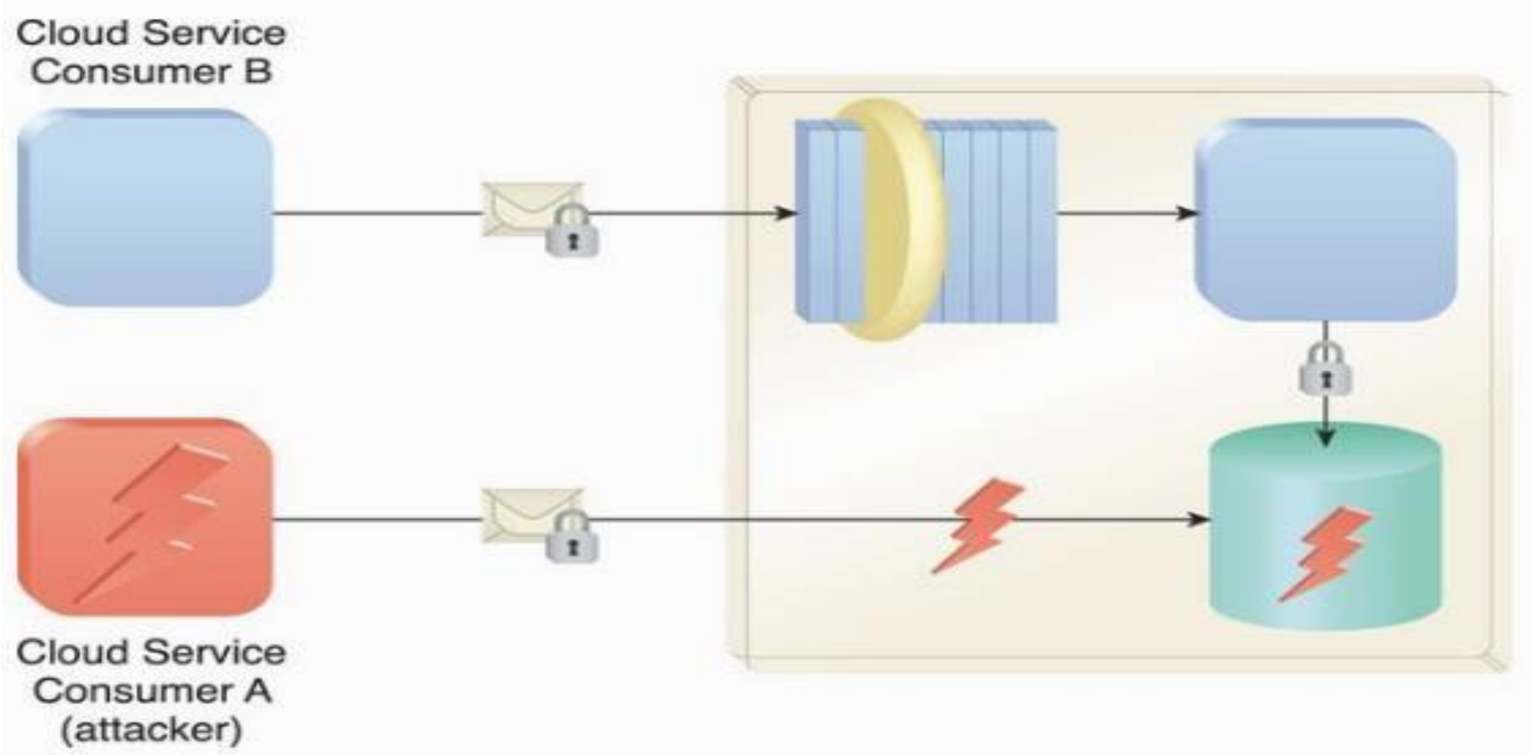


Distributed DoS (DDoS)



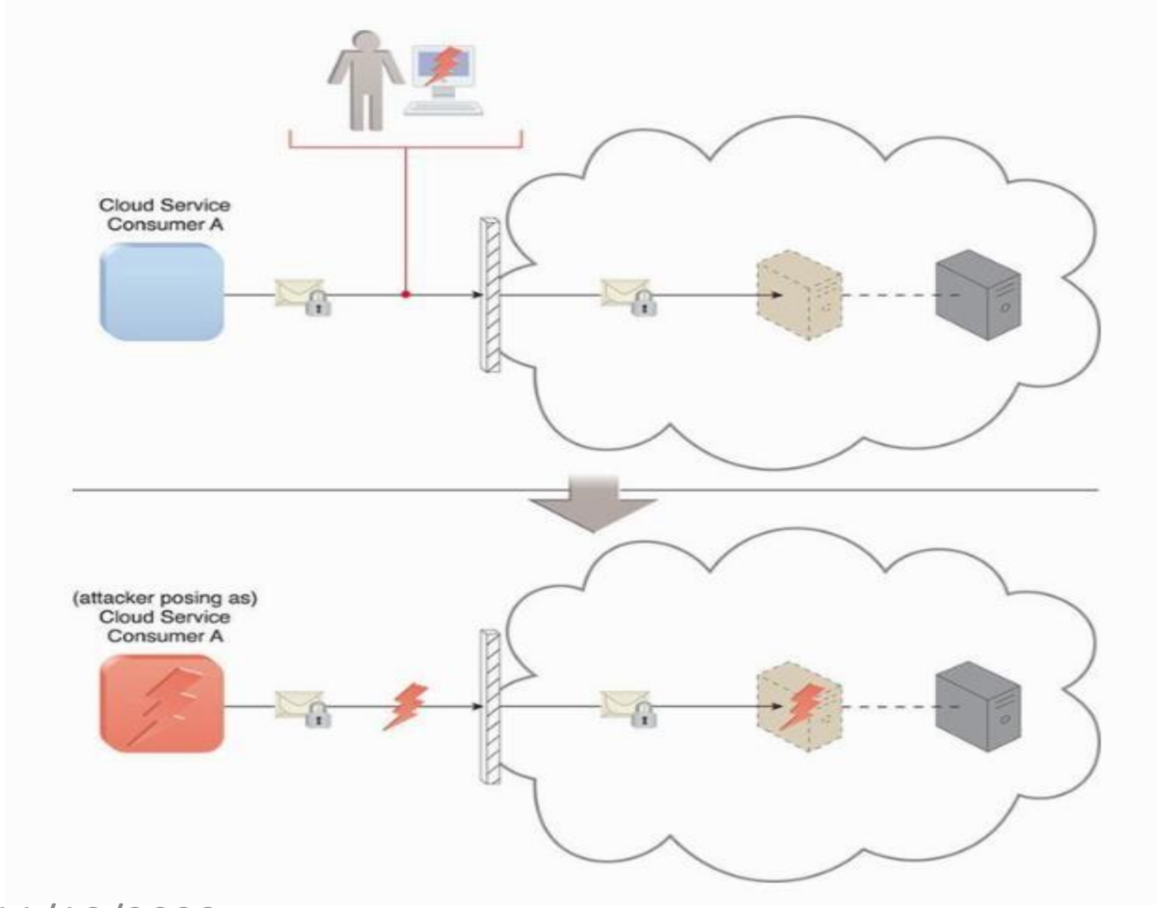
- DoS is easy to detect (trace back) and mitigate.

Insufficient Authorization



- Attackers gain direct access to IT resources through poorly managed cloud API.

Weak Authentication

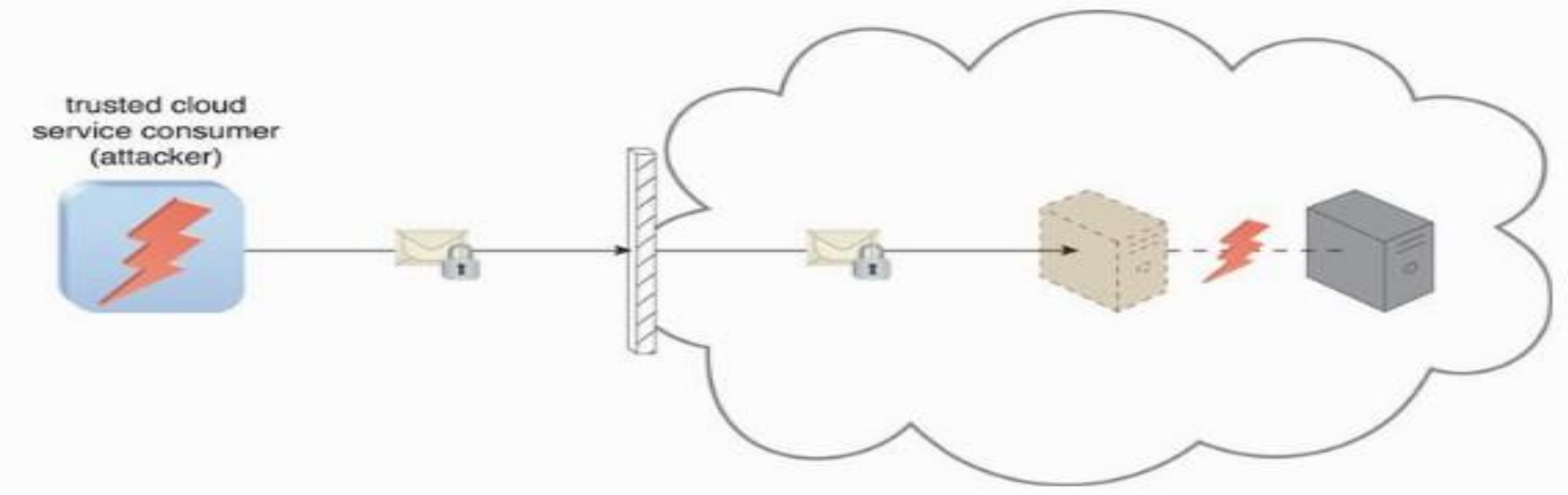


- Cloud consumer A uses a weak password enabling an attacker to easily crack it.

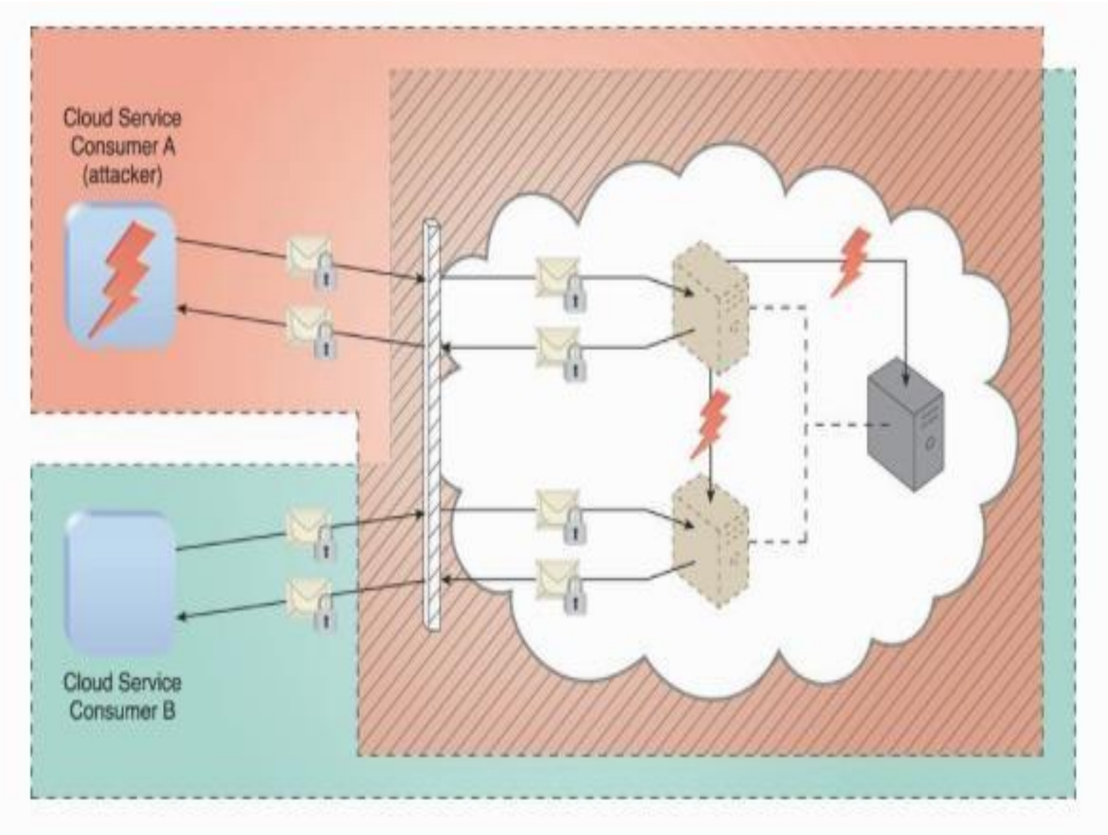
Virtualization Attack

to jeopardize its confidentiality, integrity, and/or availability.

- ❑ Accesses a virtual server to compromise its underlying physical server.
- ❑ This attack exploits vulnerabilities in the virtualization platform



Overlapping Trusted Boundaries



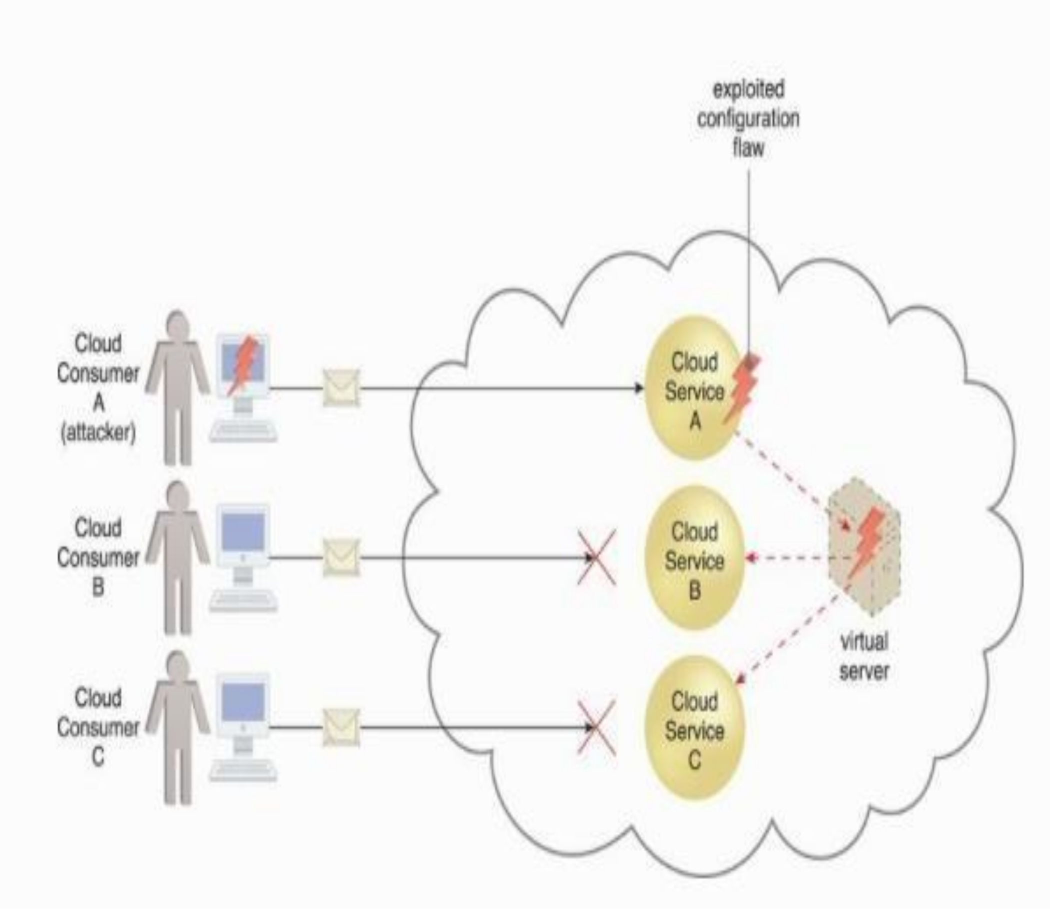
- Physical IT resources shared by multiple cloud consumers, resulting in overlapping trusted boundaries.
- Malicious cloud consumers target shared IT resources with the intention of compromising cloud consumers or other IT resources that share the same trust boundary.

6.4. Additional Considerations

- Flawed Implementation
- Security Policy Disparity
- Contracts
- Risk Management

Flawed Implementation

- Substandard design, implementation, or configuration of cloud service deployments may lead to undesirable consequences.
- Attackers can exploit these vulnerabilities to impair the integrity, confidentiality, and/or availability of cloud provider IT resources.



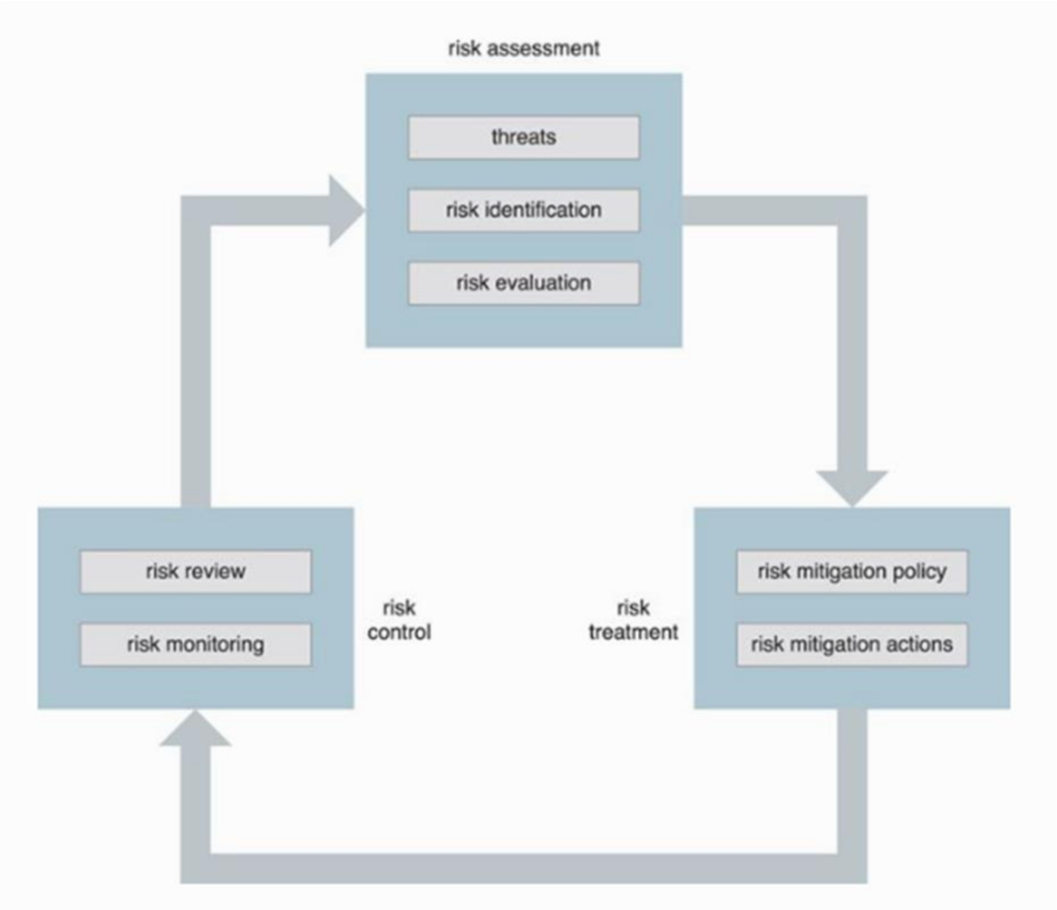
Security Policy Disparity

- ❑ Our own implemented security mechanisms are different from that provided by cloud providers.
- ❑ Assessments are needed to ensure our IT resources being migrated to a cloud are sufficiently protected.
- ❑ Cloud consumers may not be granted sufficient administrative control (of course we are not the owner of the cloud infra).
- ❑ Some public clouds, additional third parties, such as security brokers and certificate authorities, may introduce their own distinct set of security policies and practices (make things more complicated).

Contracts

- Examine contract and SLA.
- Use clear language that indicates the amount of liability assumed by the cloud provider and/or the level of indemnity the cloud provider may ask for.
- Contractual obligations is where the lines are drawn between cloud consumer and cloud provider assets. In case of security breach, who to be blamed (us or cloud provider).

Risk Management



Risk Management

- When assessing the potential impacts and challenges pertaining to cloud adoption, cloud consumers are encouraged to perform a formal risk assessment as part of a risk management strategy. Process comprises
  - Risk assessment – to identify potential vulnerabilities and shortcomings.
  - Risk treatment – mitigation policies and plans to treat risks.
  - Risk control – risk monitoring
- Risk management is an on-going process.

THANK YOU