CLOUD SECURITY DESIGN

- **Ideas of simplicity and restriction**
  - Simplicity makes designs and mechanisms easy to understand.
  - Less can go wrong with simple designs.
  - Minimizing the interaction of system components minimizes the number of sanity checks on data being transmitted from one component to another.
  - Simplicity also reduces the potential for inconsistencies within a policy or set of policies.
  - Restriction minimizes the power of an entity. The entity can access only information it needs.
  - Entities can communicate with other entities only when necessary and in as few and narrow ways as possible. Communications is used in its widest possible sense, including that of imparting information by not communicating.

CLOUD SECURITY DESIGN PRINCIPLES

- **Least Privilage**
  - A subject should be given minimum privileges & time that it needs in order to complete its task.
  - The function of a subject should control the assignment of rights, not the identity of the subject.
  - This means that if your boss demands root access to a UNIX system that you administer, he/she should not be given that privilege unless he/she requires such level of access.
  - If possible, the elevated rights of an identity individual should be removed as soon as those rights are no longer required.
  - e.g. sudo
  - su programs
  - set uid only when needed

CLOUD SECURITY DESIGN PRINCIPLES

- **Defense in depth**
  - Architected the protection system having multiple layers
  - If one layer is breached for security then internal layer can defend the attack
- **Fail safe**
  - A system should be safe for any security threats
  - System failure sometimes causes scope for breaching the security.
  - Difficult to maintain all the access control principles while recovery
  - This principle restricts how privileges are initialized when a subject or object is created.
  - Basically, this principle is similar to the “Default Deny” principle.
  - Whenever access, privilege, or some other security related attribute is not granted, that attribute should be denied by default.

CLOUD SECURITY DESIGN PRINCIPLES

- **Economy of Mechanism**
  - Security mechanisms should be as simple as possible.
  - This principle simplifies the design and implementation of security mechanisms.
  - If the design and implementation are simple, fewer possibilities exist for errors.
  - The checking and testing process is less complex.
  - Interfaces between security modules are suspect area and should be as simple as possible.
- **Open Design**
  - The security of a mechanism should not depend on the secrecy of its design or implementation.
  - This principle suggests that complexity does not add security. This concept captures the term “security through obscurity”.
  - E.g. undisclosed algorithms makes it difficult to break vs more chance of uncovering flows

CLOUD SECURITY DESIGN PRINCIPLES

- **Complete Mediation**
  - All accesses to objects should be checked to ensure that they are allowed.
  - This principle restricts the caching of information, which often leads to simpler implementations of mechanisms.
  - Every time that someone tries to access an object, the system should authenticate the privileges associated with that subject.
  - What happens in most systems is that those privileges are cached away for later use. The subject's privileges are authenticated once at the initial access.
  - For subsequent accesses the system assumes that the same privileges are enforce for that subject and object. This may or may not be the case.
  - The operating system should mediate all and every access to an object.
  - e.g. DNS information is cached , What if it is poisoned?

CLOUD SECURITY DESIGN PRINCIPLES

- **Least Common Mechanism**
  - Discourage the sharing of similar security mechanism among different components
  - If Common Mechanism are used then whole system becomes unsafe, if security of any one is cracked
- **Separation of privilege**
  - Break single privilege to multiple
  - A system should not grant permission based on a single condition.
  - Thus before privilege is granted two or more checks should be performed.
- **Weakest Link**
  - Detect and resolve weakest part
  - Attackers try to identify the most fragile part

CLOUD SECURITY DESIGN PRINCIPLES

- **Psychological Acceptability**
  - Security mechanisms should not make the resource more difficult to access than if the security mechanism were not present.
  - If security-related software or systems are too complicated to configure, maintain, or operate, the user will not employ the requisite security mechanisms.
  - For example, if a password is rejected during a password change process, the password changing program should state why it was rejected rather than giving a cryptic error message.
  - At the same time, programs should not impart unnecessary information that may lead to a compromise in security.
  - In practice, the principle of psychological acceptability is interpreted to mean that the security mechanism may add some extra burden, but that burden must be both minimal and reasonable.
  - e.g. When you enter a wrong password, the system should only tell you that the user id or password was wrong. It should not tell you that only the password was wrong as this gives the attacker information

CLOUD SECURITY MANAGEMENT FRAMWORKS

Blueprint for building a cloud security program to manage the risk and reduce vulnerabilities

- Information Technology Infrastructure Library (ITIL)
  - Globally accepted security guidelines
- ISO 27001/27002
  - Mandatory requirement of information security management system (ISMS)
  - Two complementary directives
  - 27001 for management
  - 27002 providing necessary control

ITIL

- Ten ways ITIL can improve information security
  - ITIL keeps information security service and business focused.
  - ITIL can enable organizations to develop and implement information security in a structured, clear way based on best practices.
  - With its requirement for continuous review, ITIL can help ensure that information security measures maintain their effectiveness as requirements, environments and threats change.
  - ITIL establishes documented processes and standards (such as SLAs and OLAs) that can be audited and monitored.
  - ITIL provides a foundation upon which information security can build. It requires a number of best practices - such as Change Management, Configuration Management and Incident Management - that can significantly improve information security.

ITIL

- ITIL enables information security staff to discuss information security in terms other groups can understand and appreciate.
- The organized ITIL framework prevents the rushed, disorganized implementation of information security measures.
- The reporting required by ITIL keeps an organization's management well informed about the effectiveness of their organization's information security measures.
- ITIL defines roles and responsibilities for information security.
- ITIL establishes a common language for discussing information security.

ISO 27001

- ISO 27001 is the central framework of the ISO 27000 series, which is a series of documents relating to various parts of information security management.
- The Standard contains the implementation requirements for an ISMS. These are essentially an overview of everything you must do achieve compliance.
- This is particularly useful at the start of your project, or if you're looking for general advice but can't commit to a full-scale implementation project.
- To meet these requirements, organizations must:
  - Assemble a project team and initiate the project;
  - Conduct a gap analysis;
  - Scope the ISMS;
  - Initiate high-level policy development;
  - Perform a risk assessment;
  - Select and apply controls;
  - Develop risk documentation;
  - Conduct staff awareness training;
  - Assess, review and conduct an internal audit; and
  - Opt for a certification audit.

ISO 27002

- ISO 27002 is a supplementary standard that focuses on the information security controls that organizations might choose to implement.
- These controls are listed in Annex A of ISO 27001, which is what you'll often see information security experts refer to when discussing information security controls.
- However, whereas Annex A simply outlines each control in one or two sentences, ISO 27002 dedicates an average of one page per control.
- This is because the Standard explains how each control works, what its objective is, and how you can implement it.

ISO 27002

- Annex A of ISO 27001 lists 114 security controls divided into 14 control sets
- Each of which is expanded upon in Clauses 5–18 of ISO 27002
- https://www.itgovernanceusa.com/iso27002

References

1. *Cloud Computing*, Sandeep Bhowmik
2. https://www.givainc.com/wp/ten-ways-it-infrastructure-library-itil-improve-information-security.cfm
3. https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002