Group members: Ijiehon, Ehis; Hussain, Areeb; Aboualnaga, Khaled

Assignment 1

The main role of universities is as repositories and generators of knowledge. Universities have the obligation to equip graduates so that they can obtain viable employment. The longer-term role of graduates is in creating cohesive and tolerant communities. The most important goal of a university is to hand out degrees/ certificates, at the end of the studies, which acts as a tool to showcase the graduates' standard of education and skillsets. The university enrolls students and keeps records of their personal data (names, grades, addresses, other scientific and software material etc.) in a data base. Therefore, there should be integrity and all data should be secured. This is where the need of **ISMS** (information security management systems) for a university comes in, to store all this data securely.

ISMS provide a secure processing of business to ensure improvement and continuity without interruption by malicious parties from internal and external sources. For departments such as finance, data confidentiality and integrity should be ensured. Goals of the Information Security Management are:

Goals of ISMS for University

- Privacy and protection of personal information of students and staff
- Complying with International laws of Information security to prevent e.g. (Copy right Infringement)
- Prevent physical access of unauthorized personnel from accessing sensitive locations (database)
- Ensure the Confidentiality, Integrity, and Authenticity of Information.

All goals of ISMS are achieved by following a set of security protocols and policies that must be developed by the CISO and ISO of the organization according to the Information Security standards of that said Organization. In the context of a university we can easily identify and assess risk by implementing the **CIA analysis**, which helps to prioritize the procedures that are required to develop an ISMS for a University.

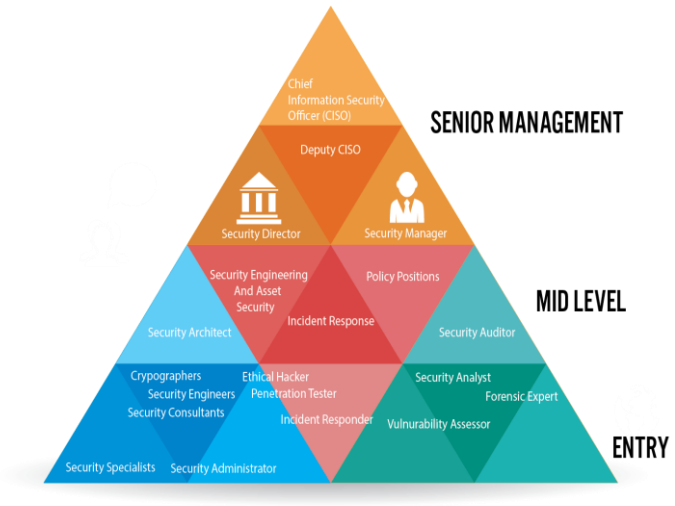
C: Confidentiality Refers to the impact of unauthorized access to information assets, such as client information, passwords, computer hardware, student grades, research data, etc. The recommended rating is **High**. Solution: One-time passwords (SecurID or similar); Intrusion Detection System, etc.+++

I: Integrity This addresses the impact if customer information such as student grades or account balances were incorrect or manipulated data is used in research or sent to a sponsoring agency. The release of inaccurate data to customers, regulators, shareholders, the public, etc. could lead to a loss of business, possible legal action or public embarrassment. The recommended rating is **High.** +++

A: Availability or business disruption risk considers the impact if the function or activity was rendered inoperative due to a system failure, or a disaster situation. Consideration is given to the impact on clients as well as the department. The recommended rating is **Medium.** Solution: Back up and recovery, Uninterrupted Power Source (UPS), Disaster recovery and business continuity ++

To implement an ISMS, a security committee under the supervision of a Chief Information Security Officer is set up, who is responsible for assigning roles for the rest of the security committee. There are many roles, but we have elaborated a few

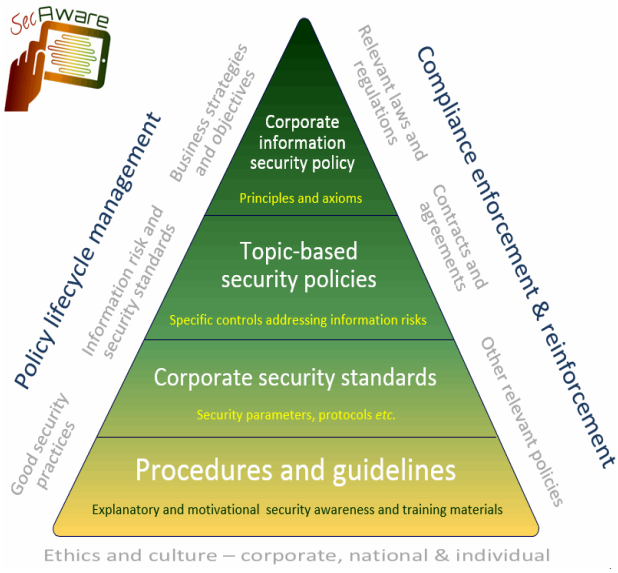
a) **CISO:** Head of Information Security. Responsible of controlling, documentation and making policy. Deals with the directive management.
b) **Information Security Officer (ISO):** ISO is responsible of actions to take care of the risk according to ISMS policy and shall report to the information security management. They also do risk analysis.
c) **IT Admin:** IT Administrator is responsible to manage personnel and to make sure they are obeying security policies



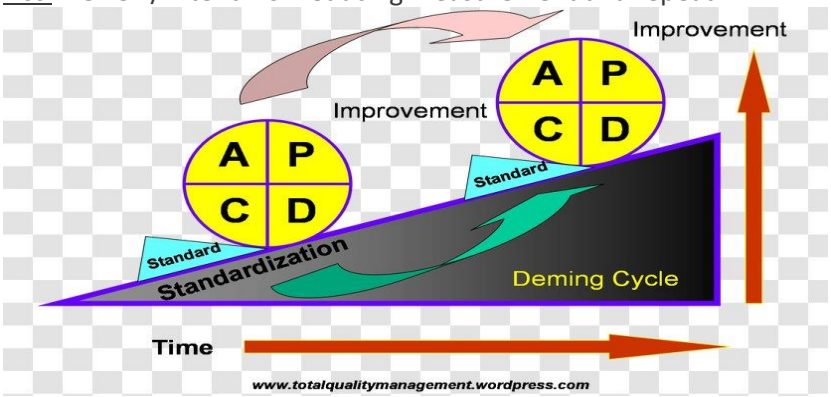
Components of ISMS

The CIA analysis is the first step towards an efficient SMS. Through CIA analysis the organization can assess the probability of occurrence of a certain "RISK" and then categorize it as HIGH, MEDIUM, or LOW, as we have shown above. The organization focuses on HIGH threat level first and take preventive measures accordingly, however if the Threat fall into a LOW category then it can be put at the end of the priority list. This classification of threat/risk can also be done through pictorial representation known as **Risk matrix.**

After the initial threat analysis, we can use more sophisticated techniques to make our ISMS more efficient for e.g. (**Risk treatment, and Security Documentation**). Risk Treatment is the process of selecting and implementing of measures to modify risk. Key takeaway of risk treatment is (Avoidance, Retention, Sharing, Transferring, Loss prevention and reduction). Security documentation is establishing a pyramid like hierarchy that illustrates how certain documents are important like Corporate information security policy, topic-based security policy, etc. Constantly changing data are put at the end of the pyramid and High priority Security policies are kept at the top



It is also important to keep on improving the ISMS; therefore, the PDCA cycle of continuous improvement processes **(CIP)** is often implemented. The PDCA cycle consists of 4 different processes:
Plan: Identify risks and risk reducing measurement
Do: implement risk reducing measurements
Check: Verify that measurements in fact reduces the identified risks
Act: Review/Extend risk reducing measurement and repeat



- **University** is not importantly dependent on Information Security. As it is mainly an Education facility, which aims to provide education in a physical manner more than a digital one. However, it of course depends on Information Security to protect its members' data such as but not limited to: students' grades, exams, sensitive information of the members, Organization or personal documents. So, we can say that the University is partly dependent on Information Security.

High-level Policies:

- The regulation and legislation must be followed
- Important laws must be followed such as Data protection
- Prevention of infringement of Copyright laws such as distribution of unlicensed Software
- Definition of Information Security guidelines and the consequences of the misuse or undermining
- The university must provide a safe and reliable environment for learning so as to protect the information and the sensitive data of its users
- The Information security threats must be taken into consideration

Topic-specific Policies:

- Assignment of Information Security management and the distribution of roles among them (Information Security Department)
- Determination of appropriate access control rules, access rights and restriction for specific user roles towards their assets; segregation of access control roles.
- Protection of sensitive or critical information processing facilities against unauthorized access
- Information classification in accordance to their value, sensitivity and criticality to prevent unauthorized manipulation or loss of information

Low-level Policies:

- An organization's data policy for privacy and protection of personally identifiable information should be developed and implemented.
- A timeline should be defined to react to notifications of potentially relevant technical vulnerabilities
- Implementation and development of Password policies and guiding the user to use it
- Splitting of the network into subnetwork, each being a network segment
- Registration of mobile devices, restriction of Software installation and the restriction of connection to information services
- Procedures designed to protect transferred information from being intercepted, copied or mis-routed
- Use of Cryptographic techniques to protect the confidentiality, integrity and authenticity of Data
- Protection against malware, spamming, cracking
- Sensitive or critical business information, on paper or digitally stored, should be locked away when not in need
- Computers and terminals should be left logged off or protected with a password or any user authentication mechanism
- Frequent update and installations of patches by authorized persons and trusted sources
- Patches should be tested and evaluated before they are installed to ensure that they are effective and do not result in any side effects that cannot be tolerant
- Backup of data to ensure data integrity and to protect against loss of data in case of a system failure or external attack
- Identifying and documenting the types of suppliers (IT services, IT infrastructure components, financial services) that will gain access to the organization information and facilities
- Ensuring that employees and contractors understand their responsibilities and security guidelines and are suitable for the roles they are selected for
- Awareness training for the organization's personnel in relation to the use of IT infrastructure and IT services
- Employees and external party users should be made aware of Information Security requirements and that such acts of information processing resources are carried under their responsibilities