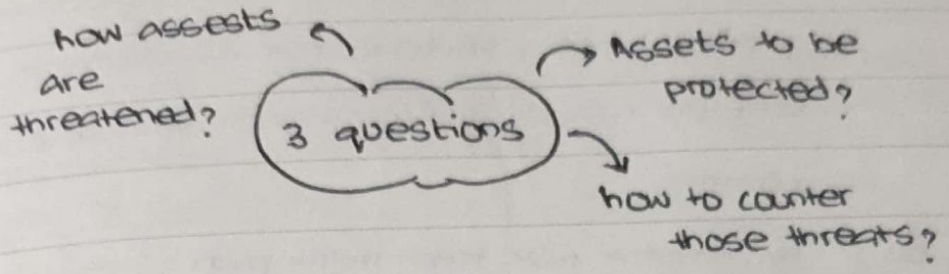
Chapter 14: IT security Management & Risk assessment.



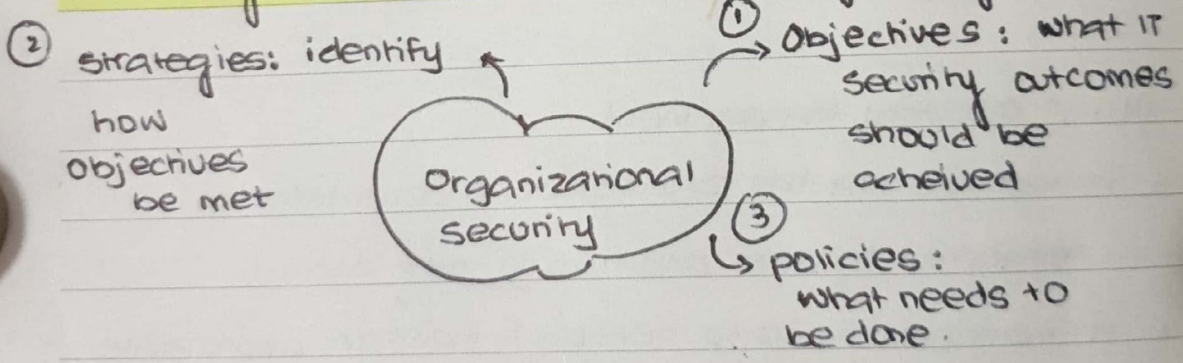
* IT security management is a formal way of answering these questions, in a cost effective way.
* Identify objectives of an organization.
  Perform risk assessment.
  Select suitable controls to write plans & procedures.
  Monitor implementation &
  Whole process iterated to be up to date

14.1: Security Management

* IT management has evolved due to dependence on networked system and rise in their risks.
* IT management is to develop & maintain appropriate levels of security to maintain CIA, accountability, authenticity & reliability.
* Important for senior management to be on board to achelve objectives.
* IT management is a cyclic process.

* Process Model to manage information security:
  - Plan: establish policies, objectives, processes & procedures. Perform risk assessment. Develop risk assessment plan with selection controls.
  - DO: Implement risk treatment plan
  - Check: Monitor & maintain risk treatment plan
  - Act: Maintain & improve plan in response to incidents, review & identify changes.
* Outcome of process security needs of managed party is met.

14.2: Organizational context & Security policy



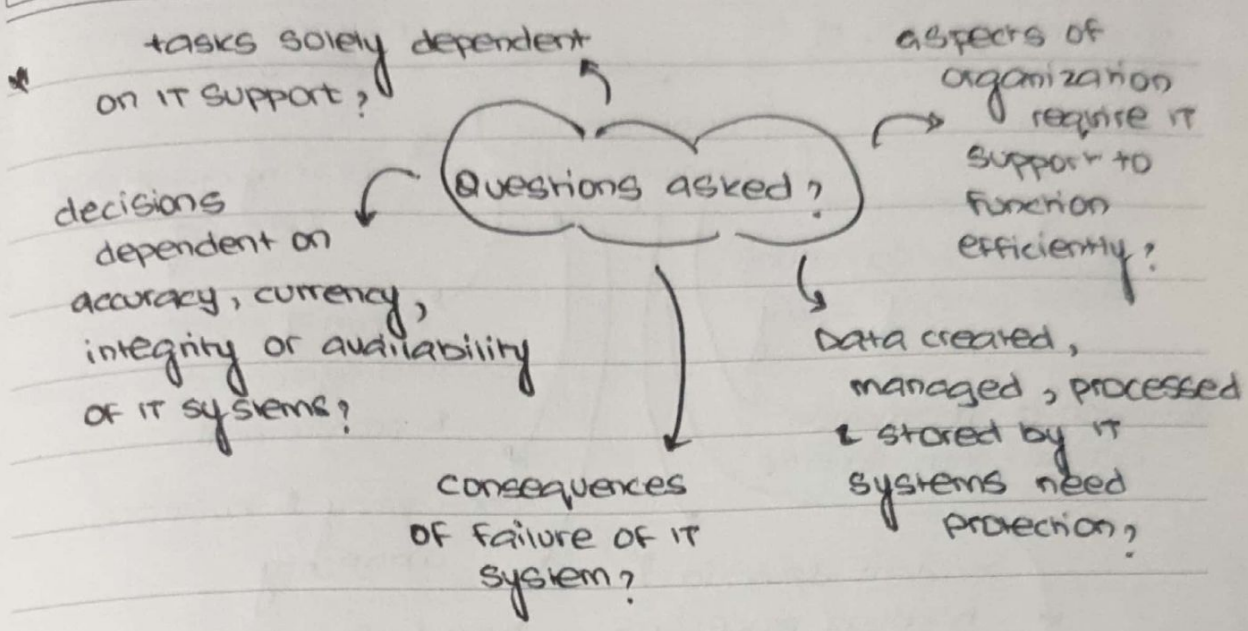
* Objectives need to consider individual rights, legal requirements & standards.
* To identify objectives, roles & importance of systems are examined, both by value & cost.

Date 17 / 12 / 22

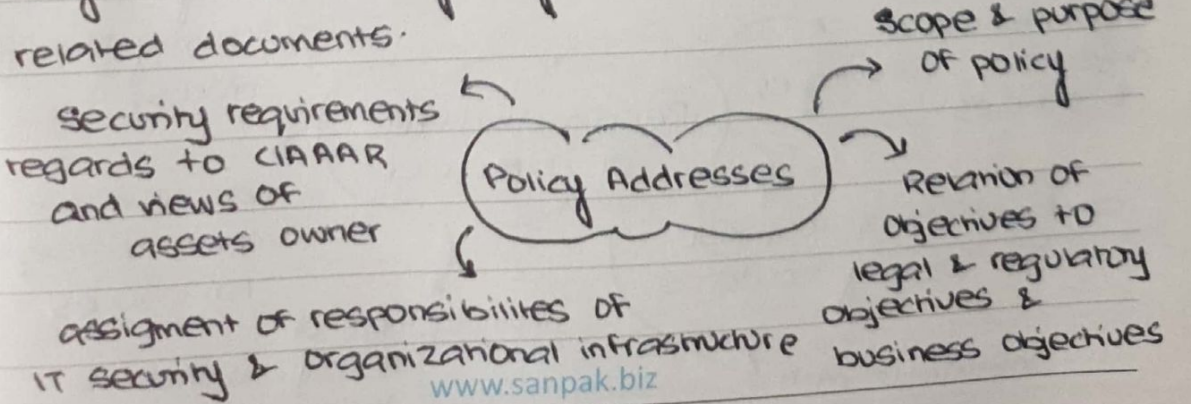
MON TUE WED THU FRI SAT SUN

CIAAAR - confidentiality, availability, integrity, authenticity, accountability & reliability

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.



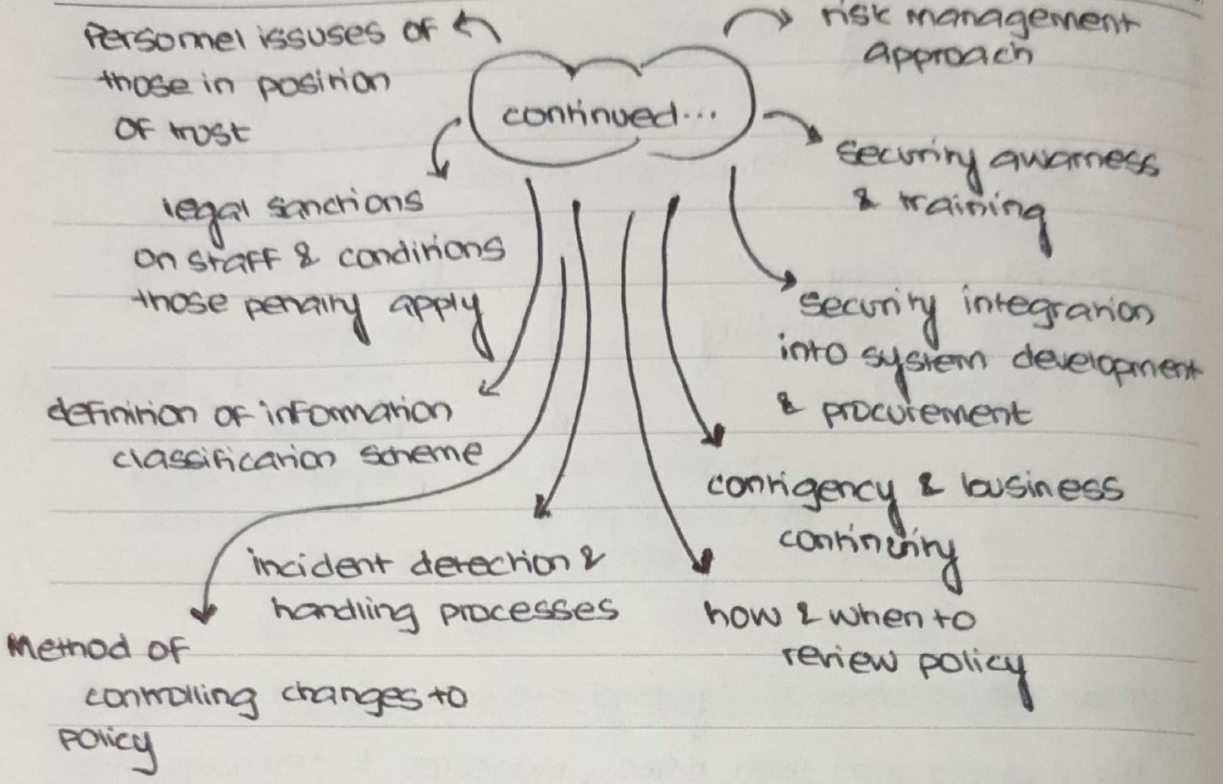
* If answers show IT systems are crucial for functioning of the organization then risks, measures & defencies are identified.
* Topics & details of strategy depends on objectives, size of organization & importance of IT systems in an organization.
* Strategy address approaches to be taken to manage security of IT systems.
* Organizational policy maybe a large document or set of related documents.



Date ____ / ____ / ____

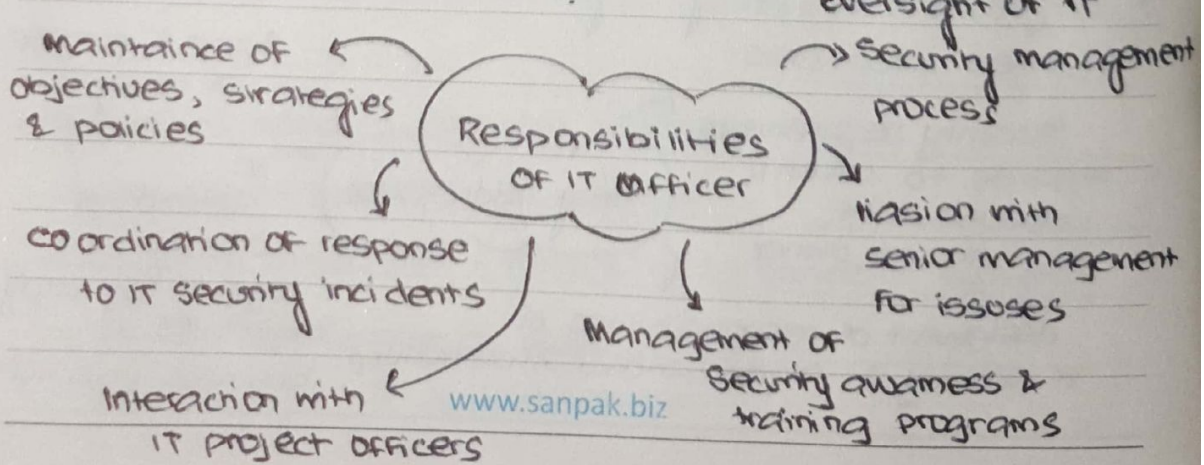
MON TUE WED THU FRI SAT SUN

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.



* Policy provides an overview how IT infrastructure supports business objectives & what security requirements are needed to be effective.

* Responsibility of IT security is shared organization to avoid ~~risk~~ risk of inconsistent implementation & loss of central monitoring, all of these should be managed by an IT officer

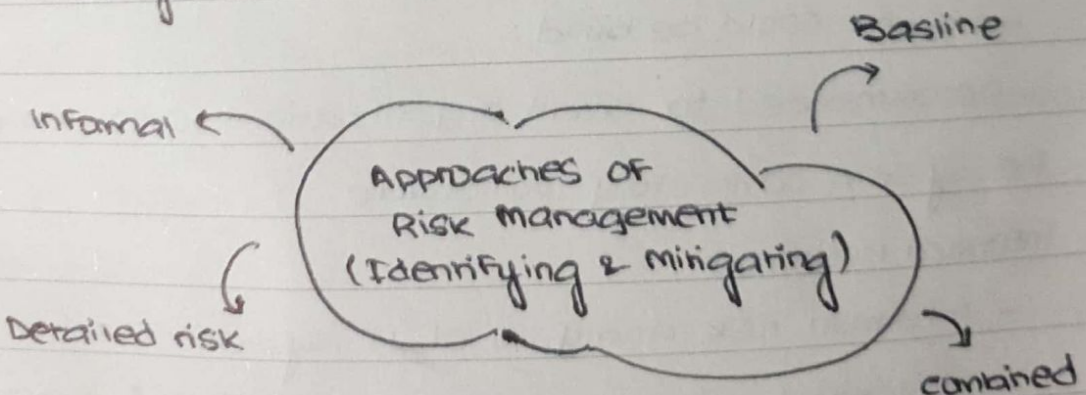


* Larger organizations require seperate IT project security to manage policies, develop & implement plans, handle monitoring & assist in investigation of events.

~~chapter~~ 14.3: Security Risk Assesment

* critical because decides where to deploy resources to be critical.
* Risks will not be addressed properly leaving organization vulnerable.
* If risk of a system is considered to be too great on assessment measures are taken to reduce it to an acceptable level.
* Evaluating each system is impossible in practical due to rapid changes in IT and takes longer time.
* Specifying acceptable levels of risks is based on how much can the organization afford the cost.

*



* Choice of approach is based on resources, valuability of IT systems to business objectives.

* Baseline Approach:
  - Implement basic general level of security controls using baseline documents, codes of pratice & industry best practice.
  - Does not require additional resources ~~of~~ for risk assessment, same measures can be used for range of systems.
  - No special consideration given to variation in organizational's risk exposure or working of their systems.
  - Baseline measure maybe set too high resulting in expensive restrictive measures or too low resulting in insufficient security leaving organization vulnerable.
  - Deals with protection against common threats.
  - Sets a good foundation on which additional security measures could be build.
  - Recommended for small organizations to not leave the system completely vulnerable.

* Informal Approach:
  - Informal risk analysis of IT systems, not a structured process, exploits knowledge & expertise of the person conducting ~~the~~ analysis.

$n = \frac{10}{100} = 0.1$

$n = \frac{3.2g}{1 \times 4} = 0.8$ CH_4

$\frac{10}{100} = \frac{g}{46}$

$\frac{10 \times 46}{100} = \frac{46}{10} = 4.6g$

Date ____/____/____

MON TUE WED THU FRI SAT SUN

- individual conducting analysis does not require additional skills.
- Performed quickly & cheaply. Organizational's personal vulnerabilities & risks are addressed.
- More specific targeted controls can be used.
- Due to no formal process some risks may not be identified leaving organization vulnerable.
- Results may be skewed by views & prejudice of person performing analysis. Resulting into insufficient ~~een~~ justification for suggested controls or their expenditure.
- Inconsistent results overtime due to different expertise.
- Recommended for small to medium sized organizations where it is not neccessary for meeting business objectives or additional risk analysis expenditure cannot be justified.

* Detailed Risk Analysis:
  - Uses a formal structured process, all risks identified along with their implications.
  - Includes steps:
    - Identification of assets.
    - Identification of ~~risks~~ threats & vulnerabilities.
    - likelihood of risks occuring & its consequences.

Level of risk organization is exposed.

- Allows for appropriate controls to be identified & implemented.
- Provides detailed identification & examinations of risks & justification on their expenditure.
- Better information to manage risks when they change & erave.
- costs significant time, resources & expertise
- Time taken during analysis causes delay in providing suitable levels of protection for systems.
- A legal requirement of government organizations to use this approach or business providing services to them. Recommended for organization whose IT systems are critical to meet their business objectives.

* Combined Approach:

- combines elements of all above approaches.
- To provide reasonable level of protection asap & then adjust these controls overtime.
- Perform baseline to establish a foundation, then informal to get a tailored and quick response to threats and lastly a structured analysis of systems.
- Results in appropriate & cost-effective controls.

Date ____/____/____

MON TUE WED THU FRI SAT SUN

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

- Easier to sell approach to management to perform analysis of some systems rather than detail of all.
- Exposes where major risks are likely to occur.
- Use of baseline ensures basic protection is implemented early on.
- Resources are applied to systems that need it and detailed analysis of these systems is carried out early on.
- If informal analysis results in inaccurate results during detailed risk analysis some systems may still be vulnerable.
- Recommended for almost all organizations.