Security & Risk Management | Ivan notes 2022

- **Alignment of security function to business strategy**
  - Corporate Governance
    - Security Governance
      - Focus of security
        - Enable business
        - increase value
      - Risk Mgmt
      - Clearly defined roles and responsibilities
        - accountability
        - responsibility
        - due care
        - due diligence
      - import/export controls
        - wassenaar arragnements
      - transborder data flow
      - privacy
      - ethics
      - Corporate laws
      - Orverarchinge security policy
      - functional security policies
        - standards
        - procedures
        - baselines
        - guildelines
      - procurement
        - contracts & SLAs

- Training, education, awareness

BCM

- 1. business impact assessment
- measurements of time
  - RPO
    - maximum acceptable amount of data loss measured in time
  - RTO
    - maximum tolerable amount of time needed to bring all critical systems back online
  - WRT
    - maximum tolerable amount of time that is needed to verify the system and/or data integrity
  - MTD
    - total amount of time that a business process can be disrupted without causing any unacceptable consequences
- types of plans
  - BCP
    - over all business plan to keep everything running
  - DRP
    - focus on recovering technology/system

Intellectual Property

- Trade secrets
  - Give exclusive control to the owners of valuable information as long as it remains secret
- patents
  - Patents protect the functionality & design of an invention
- copyright
  - Subtopic 1
    - Give owners the exclusive right to the circulation/distribution/access/control of their recorded artwork
- trademarks

- Trademarks protect the brand

Risk Mgmt

- 1. Asset valuation
  - quantitative
  - qualitative
- 2. Risk analysis
  - threats
    - STRIDE, PASTA (better risk centric)
  - vulns
    - vuln scans/pentest
  - likelihood
  - impact
  - quantitative
    - ALE = SLE X ARO
  - qualitative
- 3. Risk Treatment
  - avoid
  - transfer
  - Acceptance
  - mitigate (controls)
    - administrative
    - technical/logical
    - physical
    - safeguards (proactive)
      - directive
      - deterent
      - preventative
    - countermeasures (reactive)
      - detective
      - corrective

- recovery
- compensating

- Functional
  - what control is meant to do
- assurance
  - making sure controls are working properly