# Cognizant Class 2

06 March 2020 16:09

Inf. Security Standards and Regulations

- Top-down approach of infosec responsibilites
- Data classification
  - Confidential : needs authority
  - Sensitive : secured and shared to limited people
  - Proprietary
  - Public
- 5 w's of infosec
- Data classif needs to take into account
  - Regulatory req.
  - Strategic or propr. Worth
  - Organization specific policies
  - Ethical and privacy considerations
  - Contractual agreements
- ACT:set of rules , law & policy, standard:level of quality
- Examples:(monitory authority of singapore)
  - SOX: records buisness should store and for how long
  - SSAE 16: data center security specific
  - GLB act: to protect consumer's financial information
  - FISMA: for federal agencies
  - HIPPA:
  - HITECH
- NIST Cyber sec framework ver 1.1
- CIS: center for internet security (non-profit organization), has standards for everything
- ISO/IEC 27000,1,2,5 , controls and control groups(114 controls in 14 groups)
- controls
  - Proactive
  - Reactive
  - Deterrent
- Cloud sec frameworks,cert. , guidelines : https://cloudsecurityalliance.org/
  - Cloud security guidance v4.0
  - Cloud control matrix v3.0.1
- CCSK
- Cloud security posture management
  - Policy enforcement
  - Threat protection
  - Risk & compliance Assessment
  - Operational Monitoring
  - API integration
- Cloud workload protection platforms
  - Native/ Complementary tools protecting the workloads hosted on Cloud
  - AV, HIPS, EDR
  - Memory protection,Exploit Prevention
  - Application control, System integrity assurance
  - Firewalls & Micro segmentation
- PCI : Payment Card Industry , a standard
  - PCI security standards council
    - VISA, MasterCard etc : payment processors
  - Splunk(SIEM)
  - Components
    - PA-DSS : payment app data sec. stndrd
    - P2PE: p2p encryption
    - PTS: pin transac. Sec.
  - PCI types
- HIPAA : health insurance portability and accountability act
- HITECH : health information tech. For economic and clinical health act
- Risk management life cycle

SOA :During Employment Information security awareness, educatio training

- A security clearence
- Simulating an attack to check if the employees are well aware

RTP : risk treatment plan

-