IT Governance

1. NIST Key frameworks
   * + Cyber Security Framework (CSF)
     + Risk Management Framework (RMF)
     + Is an audit standard for SOC reports
2. (NIST) Statements on Standards Attestation Engagements (SSAE):
   * + SSAE 18 is an audit standard to enhance the quality and usefulness of Service Organization Control (SOC) reports.
       - SOC Type 1: These reports measure your security suitability of the design of controls
       - SOC Type 2: These reports are about data management the effectiveness of the controls
       - SOC Type 3: These are general use reports. They are less detailed and can be freely distributed.
3. Cloud Control Matrix (CCM) & CSA Reference Architecture
   1. CSA CCM helps potential customers measure the overall risk of a CSP
   2. ISO 17789:2014
      * Specifies the cloud computing reference architecture (CCRA)
        + Cloud computing roles
        + Cloud computing activities
        + Cloud computing functional components and their relationships
4. ISO – International Organization for Standardization
   * + ISO 27001 – Security techniques for Information Security Management Systems:
     + ISO 27002 – Code of Practice for Information Security Controls. The aim of this standard is to improve the management of information
     + ISO/IEC 27005:2018 -- Information technology — Security techniques — Information security risk management
     + ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
     + ISO 27701 – An extension to 27001/27002 for Privacy Information Management – Requirements and Guidelines
     + ISO 31000 – About managing risk for company organizations and management in general; information can be found on its website
5. Regulations, standards, and legislation
   * + GDPR- General Data Protection Regulation
       - Developed by the EU (European Union)
       - It deals with data privacy and data sharing while maintaining the privacy and rights of an individual
       - Outline the roles and responsibilities of data controllers and data processors
     + **Gramm-Leach Bliley Act (GLBA)**
       - Requires financial institutions to provide consumers with a privacy notice
     + **Sarbanes-Oxley Act (SOX)**
       - requires that executives within an organization take individual responsibility for the accuracy of financial reports
     + **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
       - Mandates that organizations protect PHI
6. **Payment Card Industry Data Security Standard (PCI DSS)**
   * Regulations for the handling and storage of financial information
     + Deals with credit card purchases and financial transactions
     + The 12 requirements of PCI DSS are:
     + Install and maintain a firewall configuration to protect cardholder data
     + Do not use vendor-supplied defaults for system passwords and other security parameters
     + Protect stored cardholder data
     + Encrypt transmission of cardholder data across open, public networks
     + Use and regularly update anti-virus software or programs
     + Develop and maintain secure systems and applications
     + Restrict access to cardholder data by business need to know
     + Assign a unique ID to each person with computer access
     + Restrict physical access to cardholder data
     + Track and monitor all access to network resources and cardholder data
     + Regularly test security systems and processes
     + Maintain a policy that addresses information security for all personnel



