1. Complying with PCI DSS (Payment Card Industry – Data Security Standard)
   1. Related to payment card industry
   2. PCI SSC (Payment Card Industry – Security Standard Council) determines the PCI DSS.
   3. Council members comprise of Visa, Mastercard, American Express, Diners & JCB.
   4. PCI encompasses 3 different standards:
      1. For manufacturers of ATM machines: PCI PTS (Pin Transaction Security) for physical security of cards
      2. For software developers: PCI PA-DSS (Payment Application Vendors)
      3. For Merchants and Service Providers: PCI DSS
   5. Key requirements of PCI DSS:
      1. Build & maintain secure network
      2. Protect cardholder data
      3. Maintain vulnerability management program
      4. Implement strong access control measures
      5. Regularly monitor and test networks
      6. Maintain an information security policy
   6. Levels of PCI DSS:
      1. Level 1: Annual card transactions greater than 6 million
      2. Level 2: Annual card transactions between 1 million to 6 million
      3. Level 3: Annual card transactions between 20k to 1 million
      4. Level 4: Annual card transactions less than 20k
   7. Consequences of Non-compliance:
      1. Higher fees charged by acquiring bank
      2. Higher/longer hold on fund settlement
      3. Daily non-compliance fines
      4. Restrictions on services
      5. Legal action for breach of contract
2. GDPR (General Data Protection Regulation):
   1. Law since 2018 in EU.
   2. 7 Principles of GDPR:
      1. Lawful, fair, transparent collection of data
      2. Limited usage of data as per agreement with the person
      3. Data Minimization – gathering only enough data required for the process
      4. Accurate – Data is accurate
      5. Limited Time Storage – Not to keep data post usage
      6. Integrity and Confidentiality (Security) – safeguarding the data
      7. Accountability – orgs collecting data are held accountable for upholding all the principles of GDPR.
   3. Legal Basis for Collecting data:
      1. Consent of associate
      2. Contract with associate about the collected data
      3. Info needed for Legal obligation
      4. Info needed for vital interest
      5. Info needed for Public tasks/interest
      6. Legitimate interest – i.e. why the data is needed by orgs.
   4. GDPR rights of individual (not absolute based on case to case, except for right to object processing data for direct marketing):
      1. Right to be informed about the data being collected
      2. Right to access info
      3. Right to rectification – rectify incorrect data
      4. Right to erasure – deleting the data
      5. Right to restrict processing
      6. Right to data portability
      7. Right to object
      8. Rights in relation to automated decision making and profiling.
   5. Where does GDPR apply:
      1. Applicable in Europe
      2. Applicable to all companies whose services/goods are used by Europeans
   6. Consequences for non-compliance:
      1. Reputation
      2. Financial Fines
      3. Business impact
      4. Legal action
3. ISO27000 Standards (focus on ISO27001):
   1. ISO27001 – focuses on Info Sec Management System.
      1. 114 controls grouped in 14 domain areas.
      2. Created by ISO (Int. Org. for Standardization) and IEC (Int. Electrotechnical Comission)
   2. ISO27005 – focuses on Risk Management
   3. ISO 27018 – rules for hosting services (eg. MS, AWS)
   4. Consequences for non-compliances:
      1. Revocation of certificate
      2. No financial penalties
      3. Business impact
4. HIPAA (Health Insurance Portability and Accountability Act):
   1. Federal Law applicable in USA
   2. Focuses on privacy & security of medical info & people involved.
   3. Non-compliance may lead to civil and criminal litigation.
5. Complying with SOX (Sarbanes-Oxley Act, 2002) and GLBA:
   1. SOX is Federal Law
   2. Known as

Corporate and Auditing Accountability, Responsibility and Transparency Act (US Congress) &

Public Company Accounting Reform and Investor Protection Act (US Senate)

* 1. Applicability:
     1. Overseen by SEC (Securities and Exchange Commission)
     2. To all businesses operating in & from USA and auditors
     3. CEO and CFO certify financial statements and effectiveness of internal controls in the annual report & to the SEC.
     4. Internal Controls incluse:
        + Access control,
        + Segregation of duties,
        + Attribution of actions on Info Systems,
        + Tampering/Modification of Financial Data
        + Fraud
        + Audit trails
  2. Non-compliance may lead to negative publicity, lawsuits, legal penalties with fines and imprisonment.
  3. GLBA (Gramm Leach Bailey Act, 1999)
  4. Financial Modernizer
  5. Applicable to Banks & Insurance companies
  6. 3 points in the GLBA:
     1. Financial Privacy Rule: orgs must provide consumers info collection and sharing practices
     2. Safeguards Rule: Need to have written security plan on how the company protects PIIs of clients
     3. Pretexting Rule: Safeguards and controls around Phishing & Impersonation of account holders.
  7. Non-compliance may lead to negative publicity, lawsuits, legal penalties with fines and imprisonment.

1. UK Cyber Essentials:
   1. Applicable in UK.
   2. Orgs do their own auditing based on the guidelines
   3. Cyber Essentials Plus – Same procedure but auditing is done by the external agency.