**Module 1 Basics**

**1.2 Laws EH**

**Laws**

1. HIPAA
2. PCI-DSS
3. SOX
4. DMCA
5. FISMA
6. ISO/IEC 27001:2013

**HIPAA (Health Insurance Portability & Accountability Act**

1. Safeguarding private medical info
2. Strict violations for securing medical/health care info

**PCI-DSS**

1. Protect Credit Card info
2. High lvl overview
   1. Build & maintain secure network & systems
      1. Install & maintain firewall config to protect cardholder data
      2. Don’t use vendor supplied defaults for system pwds & other security params
   2. Protect cardholder data
      1. Protect stored cardholder data
      2. Encrypt transmissions of cardholder data across open, public networks
   3. Maintain Vulnerability Management Program
      1. Protect all systems against malware & regularly update anti-virus software/programs
      2. Develop & maintain secure systems & apps
   4. Implement strong Access Control Measures
      1. Restrict access to cardholder data by business need to know
      2. Identify & authenticate access to system components
      3. Restrict physical access to cardholder data
   5. Regularly monitor & test networks
      1. Track & monitor all access to network resources & cardholder data
      2. Regularly test security systems & processes
   6. Maintain an Info Security Policy
      1. Maintain policy that addresses info security for all personnel

**SOX (Sarbanes-Oxley Act)**

1. Protect investors – ensure financial records and upheld and accurate
2. SOX Section 404 Internal Controls/Requirements
   1. Management document controls & access effectiveness of internal controls over financial reporting
   2. External auditors to test internal controls over financial reporting

**DMCA (Digital Millennium Copyright Act)**

1. Send requests to remove data
   1. Can ask google to remove your stuff from search results if you prove its yours

**FISMA (Federal Info Security Management Act)**

1. Requires annual reviews of info security programs

**ISO/IEC 27001:2013**

1. Management needs to
   1. Examine info security risks
   2. Design/implement security controls
   3. Monitor controls
      1. If not working adapt them/improve