**Module 3 Architecture & Design**

**3.1 Frameworks**

**Types of Frameworks**

* Regulatory vs. Non-regulatory
* National vs. International
* Industry-specific frameworks

**Industry Standard Frameworks**

* International Organisation for Standardisation (ISO)
* National Institute of Standards & Technology (NIST)
* Payment Card Industry Data Security Standard (PCI-DSS)
* North American Electric Reliability Corporation (NERC)
* Centre for Internet Security (CIS)
* Open Web Application Security Project (OWASP)

**ISO Standards**

* ISO/IEC 27001:2013 – information security management systems requirements
* ISO/IEC 27002:2013 – code of practice for information security controls
* ISO/IEC 27003:2017 – information security management systems guidance
* ISO/IEC 27004:2016 – information security management monitoring, measurement, analysis & evaluation
* ISO/IEC 27005:2018 – information security risk management
* ISO/IEC 27017:2015 – code of practice for information security controls based on ISO/IEC 27002 for cloud services

**ISO 27001:2013**

* Specifies requirements for establishing, implementing, maintaining & continually improving an information security management system within the context of the organisation
* Includes requirements for assessment & treatment of information security risks tailored to needs of organisation
* Requirements set are generic & intended to be applicable to all organisations, regardless of type/size/nature

**ISO 27002:2013**

* Gives guidelines for organisational information security standards & information security management practices
* includes the selection, implementation & management of controls taking into consideration the organisation’s information security risk environment(s)
* Designed for organisations that intend to

1. Select controls within process of implementing Information Security Management System based on ISO/IEC 27001
2. Implement commonly accepted information security controls
3. Develop own information security management guidelines

**ISO 27002:2013 – Best Practices/Topic Areas**

* Information security policies
* Organisation of information security
* Human resource security
* Asset management
* Access control
* Cryptography
* Physical & environmental security
* Operation security – procedures & responsibilities
* Communication security
* System acquisition, development & maintenance
* Supplier relationships
* Incident management
* Business continuity management

**ISO/IEC 27017:2015**

* Gives guidelines for information security controls applicable to provision & use of cloud services by providing

1. Additional implementation guidance for relevant controls specified in ISO.IEC 27002
2. Additional controls with implementation guidance that specifically relate to cloud services

* Provides controls & implementation guidance for both cloud services providers & cloud services customers

**National Institute of Standards & Technology (NIST)**

* US National Standards
* Computer Security Resource Centre (CSRC) provides NIST’s cybersecurity & information security related projects, publications, news & events
* NIST Cybersecurity Framework (NIST CSF) is group of related standards designed to provide guidance on cybersecurity
* Each standard published as NIST SP (Special Publication)

**NIST Special Publications 800 Series (SP800)**

* SP 800-30 – Guide for conducting risk assessments
* SP 800-35 – guide to information technology security services
* SP 800-53 – security & privacy controls for federal information systems & organisations
* SP 80053A – assessing security & privacy controls in federal information systems & organisations – building effective assessment plans

**Payment Card Industry Data Security Standard (PCI-DSS)**

* Used by Visa, Mastercard, American Express & Discover to create common security controls for protection for Card Holder Data (CHD)
* Any organisation processing credit cards must be compliant
* Levels of compliance differ
* PCI-DSS control objectives

1. Build & maintain secure network
2. Protect cardholder data
3. Maintain vulnerability management program
4. Regularly monitor & test networks
5. Maintain vulnerability management program

**Benchmarks/Secure Configuration Guides – General Purpose Guides**

* DoD Security Technical Implementation Guides (STIGs) – contain technical guidance to “lock down” information systems/software that might be vulnerable to malicious computer risks
* Centre for Internet Security Benchmarks

1. Best practices for secure configuration of a target system
2. Available for more than 150 technologies, CIS Benchmarks are developed through unique consensus-based process comprised of cybersecurity professionals & subject matter experts globally

**Benchmark/Secure Configuration Guides – Platform/Vendor-specific Guides**

* Network – Cisco
* OS – Microsoft TechNet, Macintosh, Linux
* Web Server – Microsoft IIS (Internet Information Services), Apache

**Defence in Depth/Layered Security**

* Defence in Depth – coordinated use of multiple security countermeasures to information assets
* Segmentation – act/practice of splitting network into zones/subnetworks based on business function/security needs using

1. Physical devices – routers/switches
2. Virtual Local Area Network (VLANs)
3. Air Gaps

* Control Diversity – addressing security concern using multiple controls that don’t depend on another

1. Administrative/process
2. Technical

* Vendor Diversity – addressing security concern using multiple vendor products that don’t depend on each other
* User Training – reduces impact of threats & vulnerabilities