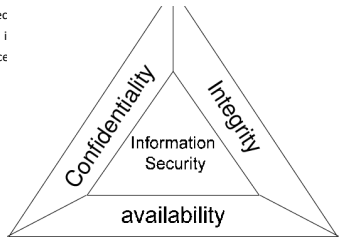
Week 2

MIS-5903
Security & Risk Management
https://community.mis.temple.edu/mis5903sec711summer2021/

1

”The CIA Triad”

- Confidentiality – necessary level of sec
- Integrity – unauthorized modification i
- Availability – reliability and timely acce



2

Examples

- Confidentiality:
  - Encryption for data at rest, in transit.
  - Access Control (physical and technical)
- Integrity:
  - Hashing, Digital Signatures, CRC
  - Change Control
  - Access Control (physical and technical)
- Availability:
  - Backups, Shadowing, Rollback,
  - Co-Location, Failover, Load Balancing, Redundancy, Clustering

3

Confidentiality

- Sensitivity – could cause harm if disclosed
- Discretion – influence or control disclosure to minimize harm or damage
- Criticality – mission-critical
- Concealment – hiding or preventing disclosure (cover, obfuscation, distraction)
- Secrecy – preventing disclosure of information
- Privacy – could cause harm, embarrassment, or disgrace
- Seclusion – out-of-the-way locations
- Isolation – separated from others; prevent commingling.

4

Integrity

- Accuracy – being correct and precise
- Truthfulness – true reflection of reality
- Authenticity – authentic or genuine
- Validity – factually or logically sound
- Nonrepudiation – cannot deny having performed an action
- Accountability – obligated for actions and results
- Responsibility – In charge or having control over something/someone
- Completeness – all needed and necessary components/parts

5

Availability

- Usability – easy to use or learn, able to be understood or controlled
- Accessibility – wide range of subjects can interact regardless of capabilities or limitations
- Timeliness – prompt, on-time, within reasonable timeframe, or low latency response

6

Authentication, Authorization, Accounting (AAA)

- Identification – claiming to be an identity
- Authentication – Proving the identity
- Authorization – Permissions (allow/grant/deny) based on authenticated identity
- Auditing – Log of events and activities related to subjects and objects
  - Subject – Wants access to an object. (e.g. end user, or process)
  - Object – Resource the Subject wants access to. (e.g. server, or "data")
- Accounting (accountability) – log files allow to check for compliance and violations. Subjects held accountable for their actions.

7

Protection Mechanisms

- Layering – no single checkpoint
- Abstraction – groups, classes, or roles
- Data Hiding – positioning data (object) in logical storage not accessible/seen by subject.
- Encryption – hiding the meaning or intent of communication from unintended recipients.

8

Definitions

- Vulnerability – inherent weakness or flaw
- Threat – potential danger associated with the exploitation of a vulnerability
- Threat agent – performs the action
- Risk – evaluates the
  - Likelihood the event will happen (uncertainty, occurrence, frequency)
  - Impact of the event when it happens
- Exposure – an instance of being exposed to loss
- Control (countermeasure) – mitigate or reduce the potential risk

9

Control Types

- Administrative (soft)
- Technical (logical)
- Physical

- "Defense in Depth"

10

Control Functionalities

- Preventive
- Detective
- Corrective
- Deterrent
- Recovery
- Compensating

11

Security Frameworks

- Security Program:
  - ISO/IEC 27000 series (BS7799)
- Security Controls:
  - Control Objectives for Information and Related Technology (COBIT v5)
  - NIST SP 800-53 – U.S. Federal Systems
  - COSO Internal Control – Integrated Framework: developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.
- Metrics (SMART)

12

Enterprise Architecture Frameworks

- Zachman – development of enterprise architectures
  - Interrogatories – "What, How, Where, Who, When, and Why"?
  - Perspective – Conceptual, Architectural, Technological, Implementation, Enterprise
- SABSA – Sherwood Applied Business Security Architecture
  - Interrogatories – "What, Why, How, Who, Where, Where"?
  - Perspective – Contextual, Conceptual, Logical, Physical, Component, Operational
- TOGAF – developed by "The Open Group"
  - Four layers: Business, Data, Applications, Technologies
  - Uses the "Architecture Development Model"

13

Military Architecture Frameworks

- DoDAF – U.S. Department of Defense, focused on interoperability to meet military mission goals
- MoDAF – British Ministry of Defense, military support
- SABSA – "Sherwood"

14

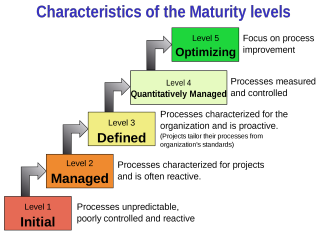
Process Management

- ITIL – best practice for service management
- ITSM – Information Technology Service Management
- ISO 20000-1:2018 – Information Technology Service Management System
- Six Sigma - successor to "Total Quality Management"

15

Process Management - CMMI

- Capability Maturity Model Integration
- Successor to Capability Maturity Model (CMM)
- Carnegie Mellon University – for US DoD



16

Process Management - CMMI

- Plan and organize (commitment, assessment, approval)
- Implement (Assign roles, Identify Data, Implement, Document, *Establish* SLAs)
- Operate and maintain (follow procedures, audit, manage SLAs)
- Monitor and evaluate

17

Data Classification

- Usefulness
- Timeliness
- Value or Cost
- Maturity or age
- Lifetime (when it expires)
- Association with personnel
- Data Disclosure Damage
- Data Modification Damage
- National Security Implications
- Authorized Access
- Restriction from Access
- Maintenance and Monitoring of Data
- Storage of Data

18

Classification Schemes

Government/Military
- Top Secret
- Secret
- Confidential
- Sensitive by Unclassified
- Unclassified

Commercial Business/Private
- Confidential / Private
- Sensitive
- Public

19

Organizational Roles

- Senior Manager – ultimately responsible for security
- Security Professional – ISO / CIRT role
- Data Owner – responsible to classify information
- Data Custodian – implements prescribed protection
- User – any person who has access to system
- Auditor – Reviews and Verifies security policy is properly implemented

20

Cybercrime

- Digital Assets
- Evolution of Attacks
  - Script kiddies
  - Advanced Persistent Threat
- Method of Entry:
  - Phishing and Zero-Day Attack
  - Back Door
  - Lateral Movement
  - Data Gathering
  - Exfiltrate

21

Common Internet Crime Schemes

- Auction fraud
- Counterfeit cashier's check
- Debt elimination
- Parcel courier
- Employment / Business opportunities
- Escrow services fraud
- Investment fraud
- Lotteries
- Nigerian letter "419"
- Ponzi / Pyramid
- Reshipping
- Third-party receiver of funds

22

OECD Core Principles

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

23

EU Safe Harbor

- Notice – informed how collected data to be used
- Choice – ability to opt-out
- Onward transfer limited – adequate security
- Security – reasonable efforts to prevent loss
- Data Integrity - relevant and reliable for the purpose
- Access – Individuals able to access, correct, or delete
- Enforcement – effective enforcement of these rules.

24

Types of Legal Systems

Civil (Code)
- Used in European countries such as France and Spain
- Based on State or Nations for Self-Regulation
- Most widespread in world
- Most common legal system in Europe
- Lower courts not compelled to follow higher court decisions

Common Law
- Developed in England
- Used in United States
- Based on Interpretation (judges)
- Broken down:
  - Criminal
  - Civil/Tort (breach of duty)
  - Administrative
- Lower courts compelled to follow higher court decisions

25

Civil/Tort

- Intentional
- Wrongs against property
- Wrongs against person
- Negligence
- Nuisance
- Dignitary wrongs
- Strict Liability (product manufacturing or design)

26

Other Legal Systems - Customary

- Personal conduct and patterns of behavior
- Based on traditions and customs of the region
- Often where mixed legal systems (China, India)
- Restitution is commonly in form of fine or service

27

Other Legal Systems - Religious

- Jurists and clerics have high degree of authority
- Divided into:
  - Responsibilities, obligations to others
  - Religious duties
- Knowledge and rules revealed by God, defines and governs human affairs
- Lawmakers and scholars don't create laws; they discover truth of law.
- Includes codes of ethics and morality
- Examples: Hindu, Sharia (Islamic - based on rules of Koran), Halakha (Jewish Law)

28

Intellectual Property

- Trade Secret – proprietary to a company (formula for drink)
- Copyright – owners of original work
- Trademark – word, name, symbol, sound, shape, color (or combination)
  - E.g. Intel or T-Mobile sounds
- Patent – legal ownership and exclusion of others from copying an invention:
  - Novel, useful, not obvious
- Software Piracy

29

Need for Privacy Laws

- Data aggregation and retrieval (Big Data)
- Loss of Borders (Globalization)
- Convergence
  - Gather
  - Mining
  - Distribution

30

Privacy Laws

- Federal Privacy Act of 1974 – "big brother"
- Federal Information Security Management Act of 2002 FISMA)
  - Federal agencies must create, document, and implement agency-wide security program to achieve "risk-based policy for cost-effective security."
- Development of Veterans Affairs Information Security Protection Act (2006)
  - Response to stolen laptop
- Uniting and Strengthening America for Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)

31

Privacy Laws – Healthcare

- Health Insurance Portability and Accountability Act (HIPAA)
  - Protected Health Information
- Health Information Technology for Economic and Clinical Health Act (HITECH – 2009)
  - Part of American Recovery and Reinvestment Act
  - Promoted "Meaningful Use"

32

Privacy – Financial

- Fair Credit Reporting Act
- Gramm-Leach-Bliley Act (GLBA, 1999)
  - Financial Privacy Rule – privacy notice
  - Safeguards Rule
  - Pretexting Protection (social engineering)
- Payment Card Industry Data Security Standard (PCI-DSS)

33

Privacy – Regional

- Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)
- States (Massachusetts, California, Texas, etc.)
- General Data Protection Regulation (EU)

34

Security Governance – Alignment

- Business Strategy – Business Case
- Goals, Mission, Objectives
- Top-Down Approach
  - Senior Management defined policies
    - ISO/CISO
  - Middle Management - Document standards, baselines, guidelines, procedures
  - Operational Managers implement
  - End Users comply

35

Security Plans

- Strategic – useful for five years
- Tactical – useful for one year; prescribes and schedules tasks
- Operational – updated monthly or quarterly.

36

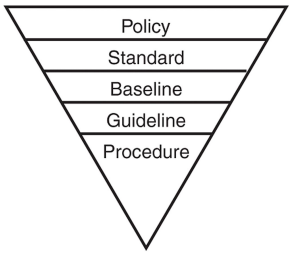
Security Policy

- Types
  - Organizational
    - Relevant to all aspects
  - Issue-Specific
    - Service
    - Department
    - Function
  - System-Specific
    - Type of system(s)
    - Methods to lock-down
    - Mandates specific security controls
- Categories
  - Regulatory
    - Industry, or
    - Legal standards
  - Advisory
    - acceptable behaviors
    - consequences
  - Informative – provides
    - Knowledge about subject (goals, mission statements, partner or customer interaction)
    - Support, research, background information

37

Supporting Elements

- Policies
- Standards
- Baseline
- Guidelines
- Procedures



38

Security Frameworks

- Open Source Security Testing Methodology Manual (OSSTMM)
- ISO/IEC 27002 (replaced ISO 17799)
- Information Technology Infrastructure Library (ITIL)
- Control Objectives for Information and Related Technology (COBIT)

1. Meeting Stakeholder Needs
2. Covering Enterprise End-to-End
3. Applying Single, Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance from Management

39

Threat Modeling

- Focus on Assets
- Focus on Attackers
- Focus on Software

40

Microsoft STRIDE

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

41

Process for Attack Simulation and Threat Analysis (PASTA)

1. DO – Definition of the Objectives
2. DTS – Definition of Technical Scope
3. ADA – Application Decomposition and Analysis
4. TA – Threat Analysis
5. WVA – Weakness and Vulnerability Analysis
6. AMA – Attack Modeling & Simulation
7. RAM – Risk Analysis & Management

42

Visual, Agile, and Simple Threat (VAST)

- Built on Agile project management and programming
- Integrate threat and risk management into programming environment

43

Risk Management

- Physical damage
- Human interaction
- Equipment malfunction
- Inside and outside attacks
- Misuse of data
- Loss of data
- Application data

44

Prioritization

- Probability x Damage Potential (1-10)x(1-10)
- High/Medium/Low
- DREAD
  - Damage Potential
  - Reproducibility
  - Exploitability
  - Affected Users
  - Discoverability

45

Information Systems Risk Management Policy

- Objectives of the ISRM team
- Level of risk the organization will accept
- Formal process of risk identification
- Connection between ISRM policy and organizational strategic planning processes
- Responsibilities and roles
- Mapping of risk to internal controls
- Approach toward changing staff behavior and resource allocation
- Mapping of risks to performance targets and budgets
- Key indicators to monitor effectiveness of controls

46

Risk Management Process

- Frame
- Assess
  - Qualitative
  - Quantitative
  - NIST SP800-30
  - Facilitated Risk Analysis Process
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (CMM)
  - Failure Modes and Effect Analysis
  - Central Computing and Telecommunications Agency Risk Analysis and Management Method (CRAMM, UK)
- Respond
- Monitor

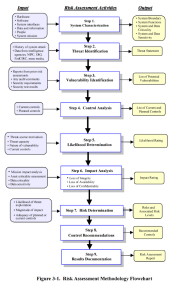


Figure 3-1. Risk Assessment Methodology Flowchart

47

Risk Calculation

- Inherent Risk (Total, Overall)
  - Threats x Vulnerability x Asset Value = Total Risk
- Residual Risk
  - (Threats x Vulnerability x asset value) x Controls Gap = Residual Risk
  - (total risk) – countermeasures = Residual Risk
- SLE = Single Loss Exposure
- ARO = Annual Rate of Occurrence
- ALE = Annual Loss Expectancy
  - SLE x ARO = ALE

48

Risk Management

- Mitigation – control selection, implementation, monitoring
- Transfer
  - Insurance transfers the financial liability
  - Outsourcing reduces the variability
- Acceptance
  - Requires senior management approval
- Avoidance – discontinue the activity leading to the risk

49

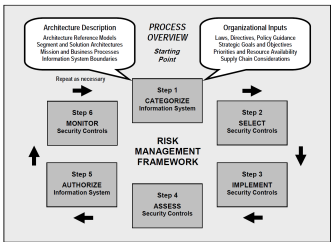
Risk Management – Decision

- Return on Security Investment (ROSI)
- Cost-Benefit Analysis
- Legal Requirements

50

Risk Management Frameworks

- NIST RMF 800-37 (information systems)
- ISO 31000:2009 (organization)
- ISACA RiskIT
- COSO Enterprise Risk Management – Integrated Framework (2004)



51

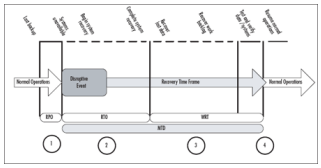
Business Continuity Planning (BCP)

- NIST SP800-34
  - Developing the continuity planning policy statement
  - Conduct the Business Impact Assessment (BIA)
  - Identify preventive controls
  - Create contingency strategies
  - Develop and Information System Contingency Plan
- ISO/IEC 27031:2011
- ISO 22301:2012 – Business Continuity Management Systems, replaced BS 25999-2

52

Disaster Recovery Planning

- RPO – Recovery Point Objective
- RTO – Recovery Time Objective
- WRT – Work Recovery Time
- MTD – Maximum Tolerable Downtime
  - Maximum Acceptable Outage
  - Maximum Allowable Outage



53

Personnel Security

- Hiring Practices
- Non-Disclosure Agreements
- Background Checks
  - Criminal, Sex Offender
  - Employer, Education
  - Immigration / SSN
  - Professional license/certification
  - Credit report(s)
  - Drug screening

54

Termination

- Disable access
- Surrender badges, keys, equipment
- Exit Interview
- Escort off premises
- Shared passwords changed

55

Awareness, Training, Education

- Awareness – “What”, Information, Recognition, Short-Term Impact
- Training – “How”, Knowledge, Skill, Intermediate Impact
- Education – “Why”, Insight, Understanding, Long-Term Impact

56

Next Steps

- Complete Discussion Questions / Participation
- Complete online quiz – Domain #1 (graded)
- Begin Reading Domain #2 Chapter(s)

57