Week 2

MIS-5903

Security & Risk Management

https://community.mis.temple.edu/mis5903sec711summer2022/

1

”The CIA Triad”

- Confidentiality – necessary level of secrecy; prevent unauthorized disclosure
- Integrity – unauthorized modification is prevented
- Availability – reliability and timely access to data and resources to authorized individuals.

- Key – Balanced Security

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

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.

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
  - Nonrepudiation – cannot disavow the action
- 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

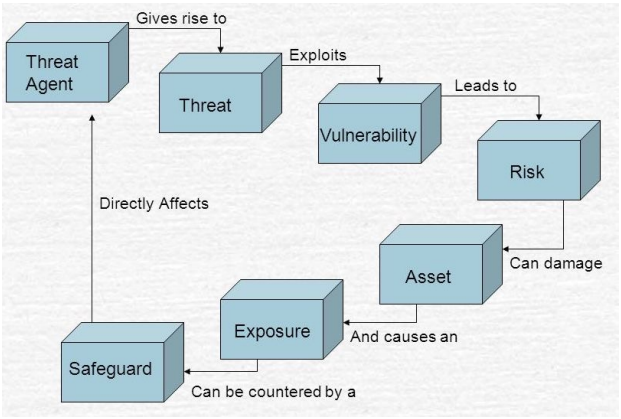
Protection Mechanisms

- 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

Threats-Safeguards

- 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



Control Types

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

- "Defense in Depth"

Control Functionalities

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

11

Security Frameworks

- Security Program:
  - ISO/IEC 27000 series (BS7799) includes:
    - 27001 – ISMS requirements
    - 27002 – Code of practice for Information Security Controls
    - 27005 – Information Security Risk Management
- Security Controls:
  - Control Objectives for Information and Related Technology (COBIT v5)
  - NIST SP 800-53 rev 5 – U.S. Federal Systems
  - NIST SP 800-171 rev 2 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - COSO Internal Control – Integrated Framework: developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.
- Metrics (SMART)

12

Enterprise Architecture Frameworks

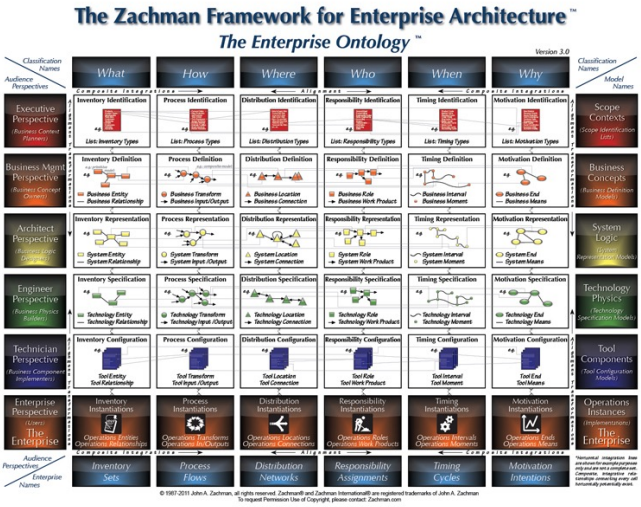
- SABSA – Sherwood Applied Business Security Architecture
  - Interrogatories – "What, Why, How, Who, Where, When"?
  - Perspective – Contextual, Conceptual, Logical, Physical, Component Operational
  - Model and a Method

Table 2: SABSA Architecture Matrix™ 2018

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
	Business Value; Taxonomy of Business Assets, including Goals & Objectives , Success Factors, Targets	Opportunities & Threats Inventory	Business Value Chain; Business Capabilities	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
	Business Attributes Taxonomy & Profile (with integrated performance targets)	Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support.	Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Security Domain Concepts & Framework	Through-Life Risk Management Framework; Attribute Performance Targets
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Trust Relationships	Domain Maps	Calendar & Timetable
	Inventory of Information Assets; Information Model of the Business	Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Domain Definitions; Inter-domain Associations & Interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
	Data Dictionary & Data Storage Devices Inventory	Risk Management Rules & Procedures; Risk Metadata	Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	User Interface to Business Systems; Identity & Access Control Systems	Workspaces; Host Platforms, Layout of Devices & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards
	Products and Tools, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery; Application Products	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators; Component Configuration	Time Schedules; Clocks, Timers & Interrupts
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Enterprise Architecture Frameworks - Zachman

- Zachman – development of enterprise architectures
  - Interrogatories – "What, How, Where, Who, When, and Why"?
  - Perspective – Conceptual, Architectural, Technological, Implementation, Enterprise



Enterprise Architecture Frameworks - TOGAF

- TOGAF – developed by "The Open Group"
  - Four layers: Business, Data, Applications, Technologies
  - Uses the "Architecture Development Model"

15

Military Architecture Frameworks

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

16

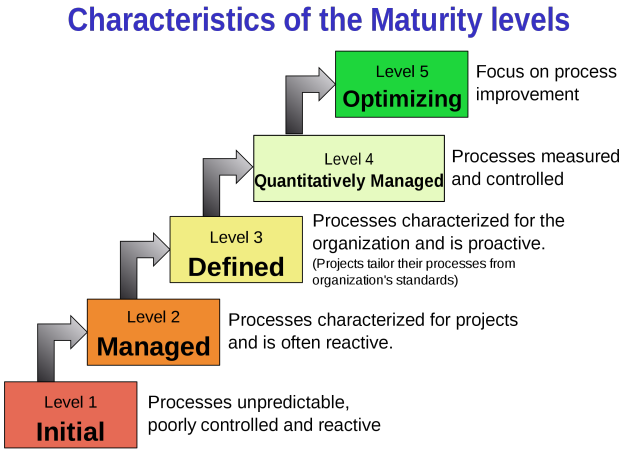
Process Management

- 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"
  - Reduce variation, defects

17

Process Management - CMMI

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



18

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

19

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

20

Classification Schemes

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

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

21

Executive Management

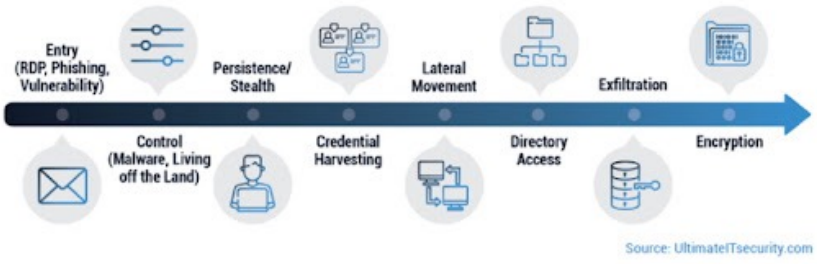
- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO) – focused on technology
- Chief Security Officer (CSO) – focused on convergence
- Chief Privacy Officer (CPO)

22

Organizational Roles

- Data Analyst – ensures data is stored correctly
- Data Owner – responsible to classify information
- Data Custodian – implements prescribed protection
- Security Administrator – implements security controls
- Supervisor – user manager – responsible for user activity
- System Owner – integrating security considerations
- User – any person who has access to system
- Auditor – Reviews and Verifies security policy is properly implemented

Cybercrime



- Digital Assets
- Evolution of Attacks
  - Script kiddies
  - Advanced Persistent Threat
  - Nation State Actors
  - Hacktivists
- Method of Entry:
  - Phishing and Zero-Day Attack
  - Back Door
  - Lateral Movement
  - Data Gathering
  - Exfiltrate (may encrypt)

Common Internet Crime Schemes

- Auction fraud
- Business E-mail Compromise
- Business Fraud
- Charity and Disaster Fraud
- Counterfeit prescription drugs
- Credit Card fraud
- Counterfeit cashier's check
- Debt elimination
- Election crimes and security
- Employment / Business Opportunities
- Escrow Services fraud
- Identity theft
- Illegal sports betting
- Investment Fraud
- Lotteries
- Nigerian letter "419"
- Parcel Courier
- Ponzi / Pyramid
- Ransomware
- Reshipping
- Sextortion
- Third-party receiver of funds

OECD Core Principles

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

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.

27

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

28

Civil/Tort

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

29

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

30

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)

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

Need for Privacy Laws

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

33

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)

34

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"

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)

Privacy – Regional

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

37

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

38

Security Plans

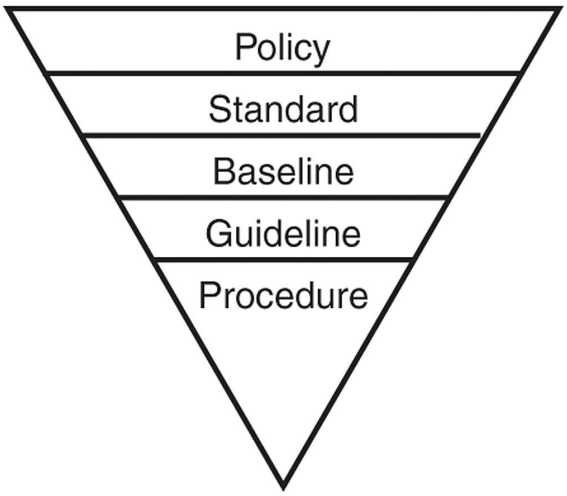
- Strategic – useful for five years
- Tactical – useful for one year; prescribes and schedules tasks
- Operational – updated monthly or quarterly.

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

Supporting Elements

- Policies
- Standards
- Baseline
- Guidelines
- Procedures



41

Security Frameworks

- NIST SP800-53 rev 5
- NIST CyberSecurity Framework (CSF) – implementation groups
- ISO/IEC 27000 series (replaced ISO 17799)
- Center for Internet Security – implementation groups
  - 7.1 – 20 controls
  - 8.0 – 18 controls
- 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

42

Threat Modeling

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

43

Microsoft STRIDE

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

44

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

Visual, Agile, and Simple Threat (VAST)

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

Risk Management

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

- Cybercriminals
- Nation-State Actors
- Hacktivists
- Internal Actors
- Nature

47

Prioritization

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

48

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

Risk Management Process

- Frame
- Assess
  - Qualitative, Quantitative, or Hybrid
  - NIST SP800-30r1
  - ISO 27005
  - Facilitated Risk Analysis Process (FRAP)
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - Factor Analysis of Information Risk (FAIR)
  - Failure Modes and Effect Analysis (FMEA)
  - Central Computing and Telecommunications Agency Risk Analysis and Management Method (CRAMM, UK)
- Respond
- Monitor

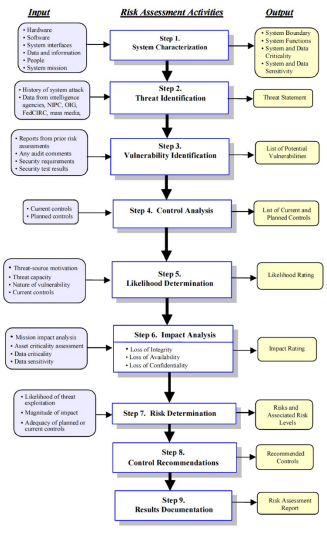


Figure 3-1. Risk Assessment Methodology Flowchart

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

51

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

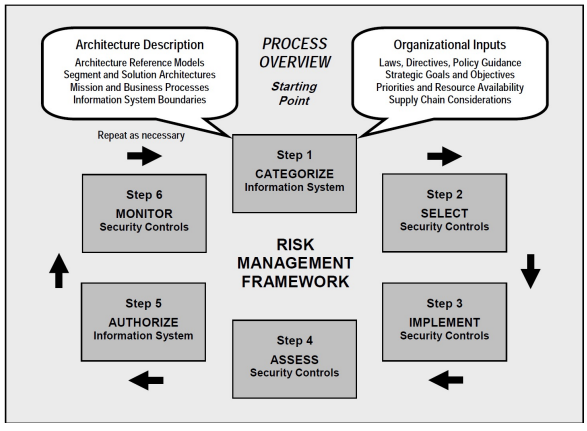
52

Risk Management – Decision

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

Risk Management Frameworks

- NIST
  - 800-37 rev 2 – Risk Management Framework for Information Systems and Organizations
  - 800-39 – Managing Information Security Risk
  - 800-30 rev 1 – Guide for Conducting Risk Assessments
- ISO 31000:2009 (organization)
- ISACA RiskIT
- COSO Enterprise Risk Management – Integrated Framework (2004)



Supply Chain / Third Parties

- Service Level Agreement (SLA) – specified in contract
  - Data Protection
  - Incident Response
  - Verification means
- ISO/IEC 27001 certification
- US Department of Defense Cybersecurity Maturity Model Certification (CMMC)
- Payment Card Industry Digital Security Standard (PCI-DSS)
- Service Organization Control 1 (SOC1) or 2 (SOC2) report
- U.S. Federal Risk and Authorization Management Program (FedRAMP)

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 22301:2019 – Business Continuity Management Systems, replaced BS 25999-2
- Business Continuity Institute's Good Practice Guidelines (GPG)

Business Continuity Institute's Good Practice Guidelines (GPG)

1. Policy and Program Management – governance
2. Embedding Business Continuity – embedding within culture, awareness and training
3. Analysis – review, assessment, business impact analysis (BIA)
4. Design – identifying and selecting solutions
5. Implementation – BC Plan development
6. Validation – exercising, maintaining, reviewing the program

57

Personnel Security

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

58

Termination

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

59

Awareness, Training, Education

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

60

Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Though shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Though shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Though shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

61

Next Steps

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

62