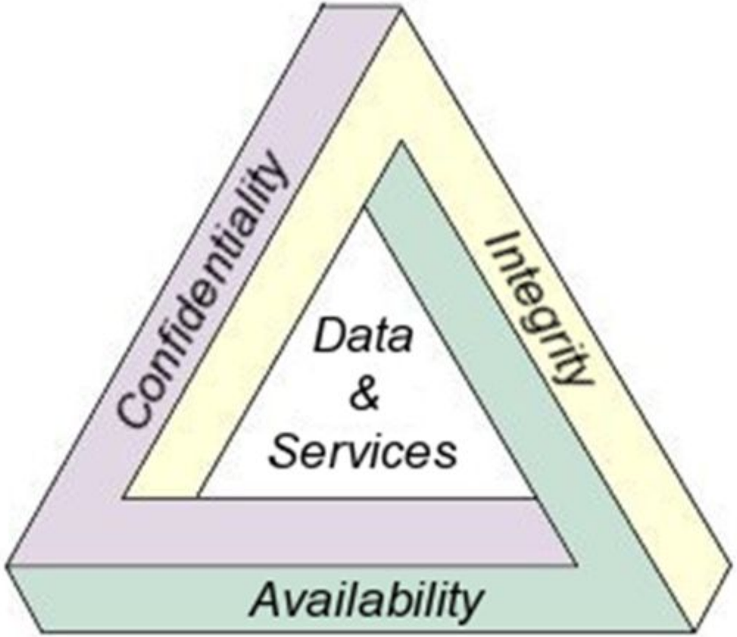
Cyber Risk Management

Review Time



- Confidentiality
- Integrity
- Availability

Everything revolves around Data! We ensure these principles through proper Risk Management.

What is Risk?

So Many Definition(s):

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. FIPS 200 under RISK

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. See Information System-Related Security Risk. NIST SP 800-30 Rev. 1 under Risk CNSSI 4009

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.] NIST SP 800-137 under Risk FIPS 200 - Adapted NIST SP 800-37 Rev. 1 under Risk FIPS 200 - Adapted NIST SP 800-53A Rev. 4 under Risk CNSSI 4009

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. NIST SP 800-18 Rev. 1 under Risk NIST SP 800-30

Risk is the possibility or likelihood that a threat will exploit a vulnerability to cause harm to an asset. (ISC)2 CISSP Eighth Edition

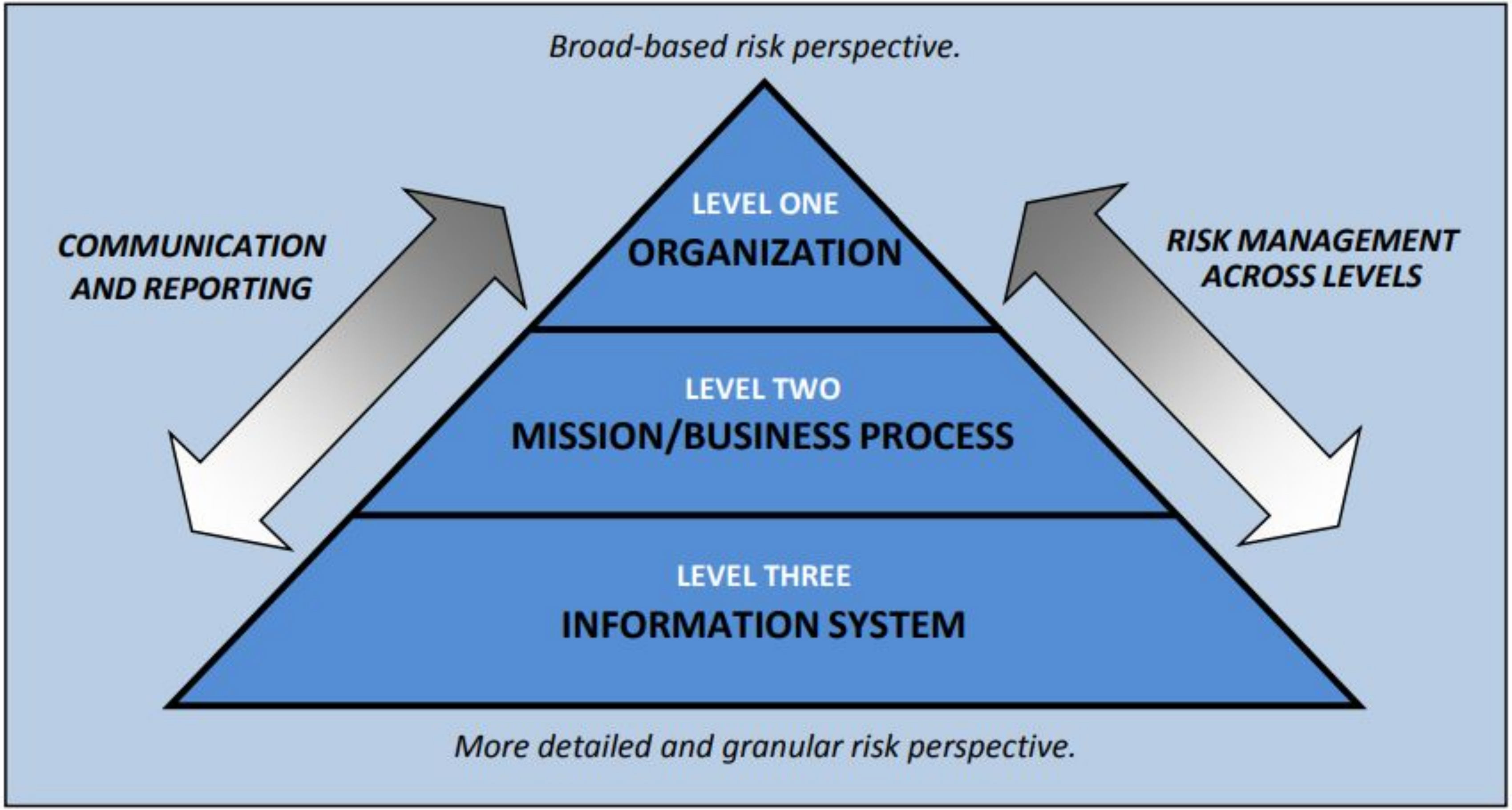

Broad-based risk perspective.
COMMUNICATION AND REPORTING
LEVEL ONE
ORGANIZATION
RISK MANAGEMENT ACROSS LEVELS
LEVEL TWO
MISSION/BUSINESS PROCESS
LEVEL THREE
INFORMATION SYSTEM
More detailed and granular risk perspective.

FIGURE 1: ORGANIZATION-WIDE RISK MANAGEMENT APPROACH

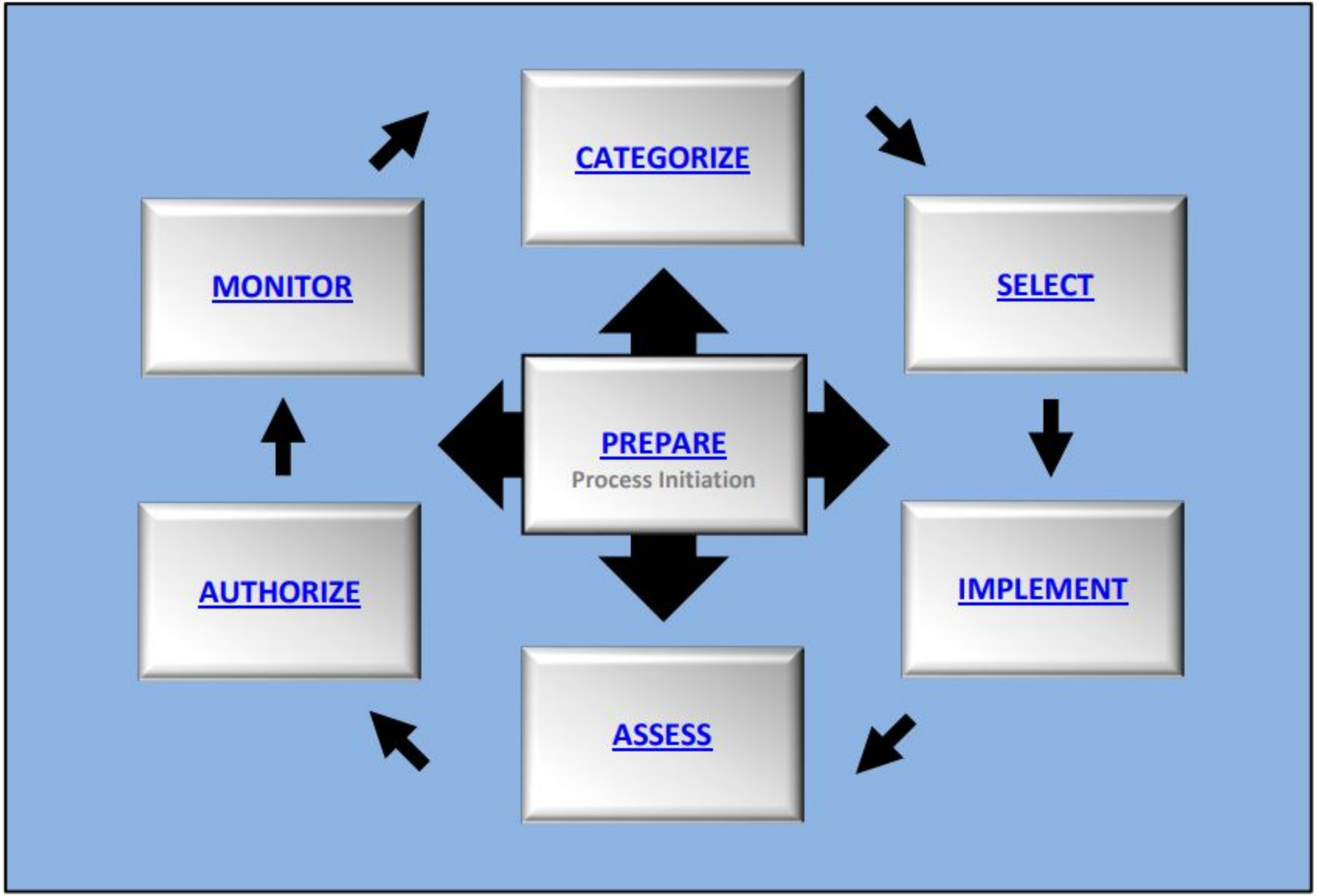
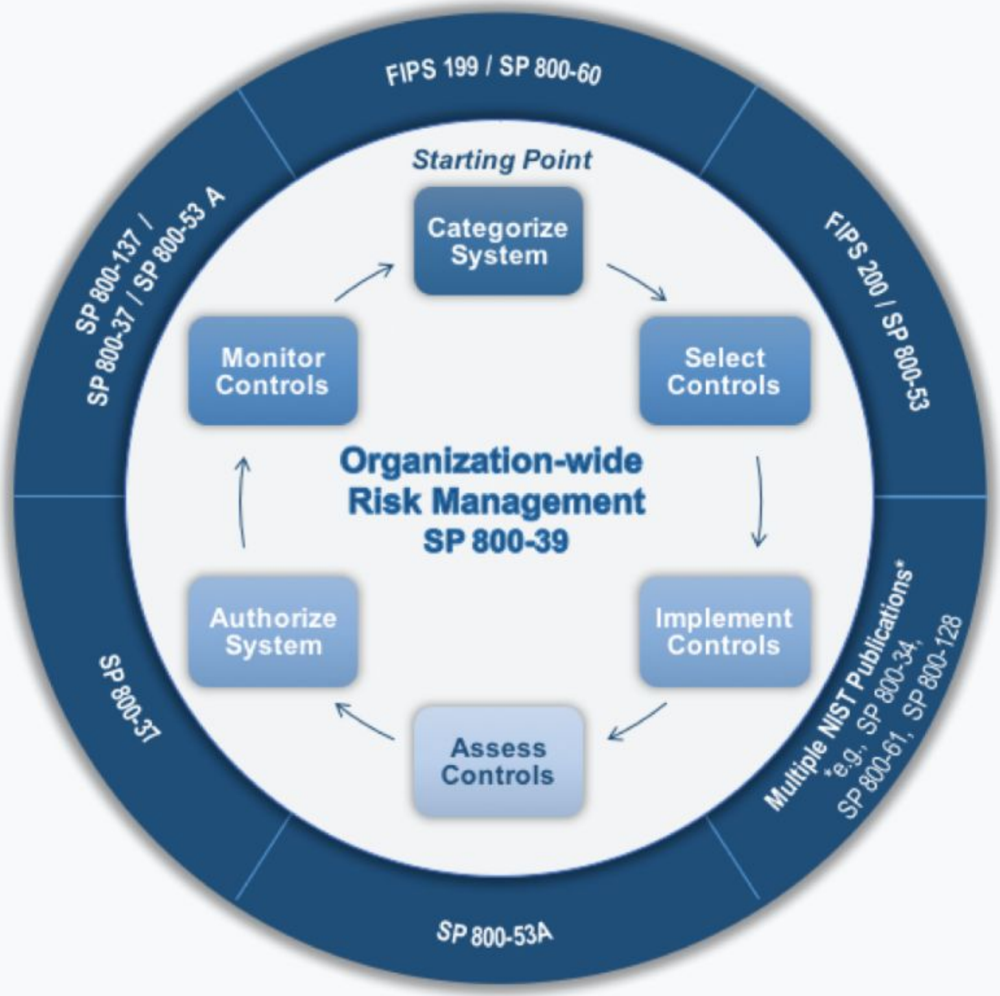


FIGURE 2: RISK MANAGEMENT FRAMEWORK


FIPS 199 / SP 800-60
Starting Point
Categorize System
FIPS 200 / SP 800-53
Select Controls
Organization-wide Risk Management SP 800-39
Multiple NIST Publications*
*e.g., SP 800-34, SP 800-61, SP 800-128
Implement Controls
SP 800-53A
Assess Controls
SP 800-37
Authorize System
SP 800-137 / SP 800-37 / SP 800-53 A
Monitor Controls

Risk - Keep it Simple

Risk = Impact * Likelihood

Impact = aka Severity and/or Consequence. The after effect of an event that can be measured in some way such as cost

Likelihood = what is the probability the impact will happen

Simple “Cyber Risk”

“Cyber Risk” = Impact * Vulnerability * Threat

Likelihood = Vulnerability * Threat

Impact: aka Severity, Consequence, Asset, and more

Costs, Value (monetary and nonmonetary), Opportunity Cost, etc.
CIA Triad/Triangle

Vulnerability

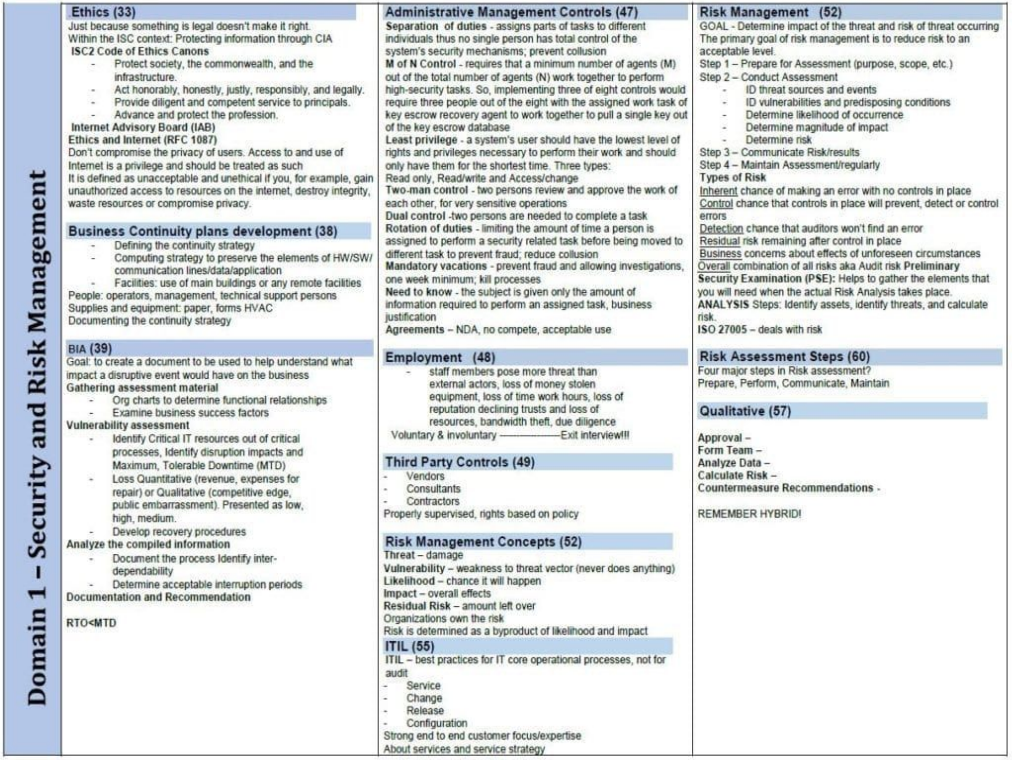
Exposure, Footprint, Weakness and/or susceptible to a threat

Threat

Actions or inaction that could cause damage, destruction, alterations, loss, etc. Intentional or accidental. From people, hardware, network, structure, nature.

What are some examples of threats?

Cybersecurity Risk Management



Domain 1 – Security and Risk Management

Ethics (33)

Just because something is legal doesn't make it right.
Within the ISC context: Protecting information through CIA
ISC2 Code of Ethics Canons

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

Internet Advisory Board (IAB)
Ethics and Internet (RFC 1087)
Don't compromise the privacy of users. Access to and use of Internet is a privilege and should be treated as such
It is defined as unacceptable and unethical if you, for example, gain unauthorized access to resources on the internet, destroy integrity, waste resources or compromise privacy.

Business Continuity plans development (38)

- Defining the continuity strategy
- Computing strategy to preserve the elements of HW/SW/ communication lines/data/application
- Facilities: use of main buildings or any remote facilities

People: operators, management, technical support persons
Supplies and equipment: paper, forms HVAC
Documenting the continuity strategy

BIA (39)

Goal: to create a document to be used to help understand what impact a disruptive event would have on the business
Gathering assessment material

- Org charts to determine functional relationships
- Examine business success factors

Vulnerability assessment

- Identify Critical IT resources out of critical processes, Identify disruption impacts and Maximum, Tolerable Downtime (MTD)
- Loss Quantitative (revenue, expenses for repair) or Qualitative (competitive edge, public embarrassment). Presented as low, high, medium.
- Develop recovery procedures

Analyze the compiled information

- Document the process Identify inter-dependability
- Determine acceptable interruption periods

Documentation and Recommendation

RTO<MTD

Administrative Management Controls (47)

Separation of duties - assigns parts of tasks to different individuals thus no single person has total control of the system's security mechanisms; prevent collusion
M of N Control - requires that a minimum number of agents (M) out of the total number of agents (N) work together to perform high-security tasks. So, implementing three of eight controls would require three people out of the eight with the assigned work task of key escrow recovery agent to work together to pull a single key out of the key escrow database
Least privilege - a system's user should have the lowest level of rights and privileges necessary to perform their work and should only have them for the shortest time. Three types:
Read only, Read/write and Access/change
Two-man control - two persons review and approve the work of each other, for very sensitive operations
Dual control -two persons are needed to complete a task
Rotation of duties - limiting the amount of time a person is assigned to perform a security related task before being moved to different task to prevent fraud; reduce collusion
Mandatory vacations - prevent fraud and allowing investigations, one week minimum; kill processes
Need to know - the subject is given only the amount of information required to perform an assigned task, business justification
Agreements – NDA, no compete, acceptable use

Employment (48)

- staff members pose more threat than external actors, loss of money stolen equipment, loss of time work hours, loss of reputation declining trusts and loss of resources, bandwidth theft, due diligence

Voluntary & involuntary ————————Exit interview!!!

Third Party Controls (49)

- Vendors
- Consultants
- Contractors

Properly supervised, rights based on policy

Risk Management Concepts (52)

Threat – damage
Vulnerability – weakness to threat vector (never does anything)
Likelihood – chance it will happen
Impact – overall effects
Residual Risk – amount left over
Organizations own the risk
Risk is determined as a byproduct of likelihood and impact

ITIL (55)

ITIL – best practices for IT core operational processes, not for audit

- Service
- Change
- Release
- Configuration

Strong end to end customer focus/expertise
About services and service strategy

Risk Management (52)

GOAL - Determine impact of the threat and risk of threat occurring
The primary goal of risk management is to reduce risk to an acceptable level.
Step 1 – Prepare for Assessment (purpose, scope, etc.)
Step 2 – Conduct Assessment

- ID threat sources and events
- ID vulnerabilities and predisposing conditions
- Determine likelihood of occurrence
- Determine magnitude of impact
- Determine risk

Step 3 – Communicate Risk/results
Step 4 – Maintain Assessment/regularly
Types of Risk
Inherent chance of making an error with no controls in place
Control chance that controls in place will prevent, detect or control errors
Detection chance that auditors won't find an error
Residual risk remaining after control in place
Business concerns about effects of unforeseen circumstances
Overall combination of all risks aka Audit risk **Preliminary Security Examination (PSE):** Helps to gather the elements that you will need when the actual Risk Analysis takes place.
ANALYSIS Steps: Identify assets, identify threats, and calculate risk.
ISO 27005 – deals with risk

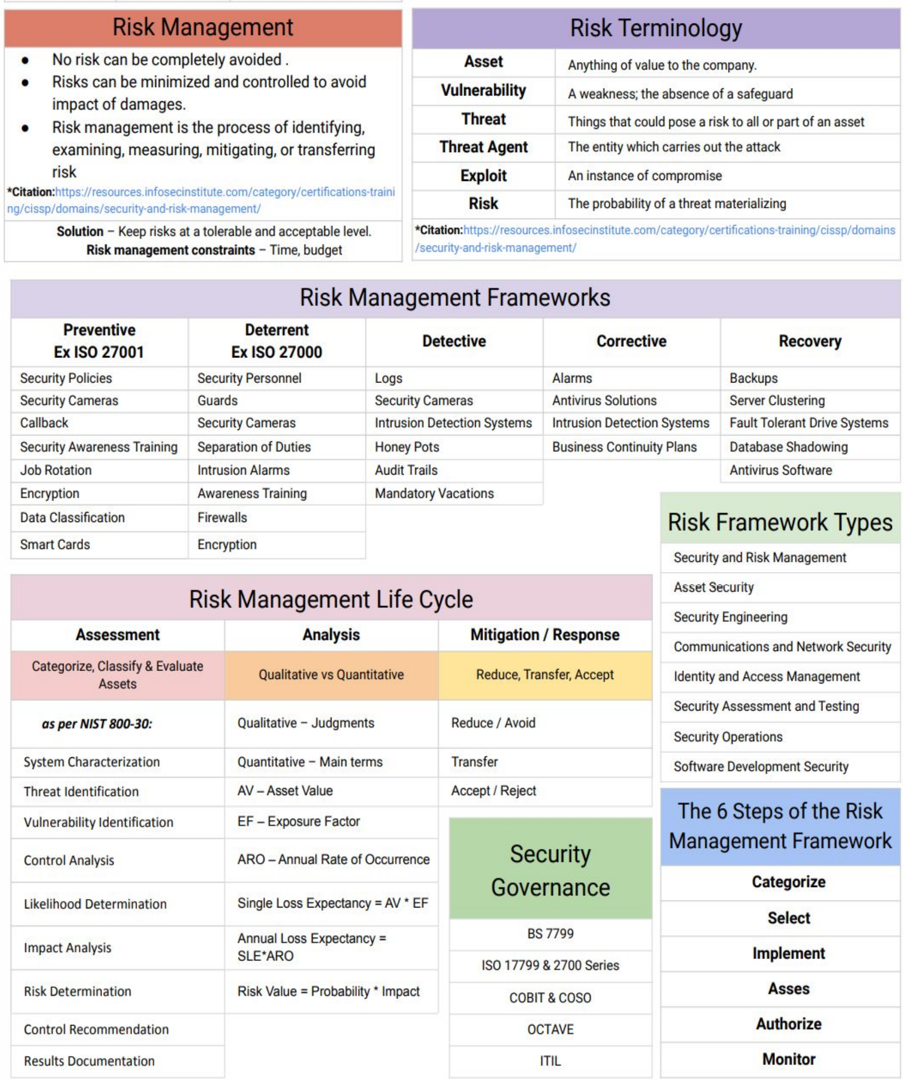
Risk Assessment Steps (60)

Four major steps in Risk assessment?
Prepare, Perform, Communicate, Maintain

Qualitative (57)

Approval –
Form Team –
Analyze Data –
Calculate Risk –
Countermeasure Recommendations -

REMEMBER HYBRID!



Risk Management

- No risk can be completely avoided .
- Risks can be minimized and controlled to avoid impact of damages.
- Risk management is the process of identifying, examining, measuring, mitigating, or transferring risk

*Citation:https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Solution – Keep risks at a tolerable and acceptable level.
Risk management constraints – Time, budget

Risk Terminology

Asset	Anything of value to the company.
Vulnerability	A weakness; the absence of a safeguard
Threat	Things that could pose a risk to all or part of an asset
Threat Agent	The entity which carries out the attack
Exploit	An instance of compromise
Risk	The probability of a threat materializing

*Citation:https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Risk Management Frameworks

Preventive Ex ISO 27001	Deterrent Ex ISO 27000	Detective	Corrective	Recovery
Security Policies	Security Personnel	Logs	Alarms	Backups
Security Cameras	Guards	Security Cameras	Antivirus Solutions	Server Clustering
Callback	Security Cameras	Intrusion Detection Systems	Intrusion Detection Systems	Fault Tolerant Drive Systems
Security Awareness Training	Separation of Duties	Honey Pots	Business Continuity Plans	Database Shadowing
Job Rotation	Intrusion Alarms	Audit Trails		Antivirus Software
Encryption	Awareness Training	Mandatory Vacations		
Data Classification	Firewalls			
Smart Cards	Encryption			

Risk Framework Types

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Risk Management Life Cycle

Assessment	Analysis	Mitigation / Response
Categorize, Classify & Evaluate Assets	Qualitative vs Quantitative	Reduce, Transfer, Accept
as per NIST 800-30:	Qualitative – Judgments	Reduce / Avoid
System Characterization	Quantitative – Main terms	Transfer
Threat Identification	AV – Asset Value	Accept / Reject
Vulnerability Identification	EF – Exposure Factor	
Control Analysis	ARO – Annual Rate of Occurrence	
Likelihood Determination	Single Loss Expectancy = AV * EF	
Impact Analysis	Annual Loss Expectancy = SLE*ARO	
Risk Determination	Risk Value = Probability * Impact	
Control Recommendation		
Results Documentation		

Security Governance

- BS 7799
- ISO 17799 & 2700 Series
- COBIT & COSO
- OCTAVE
- ITIL

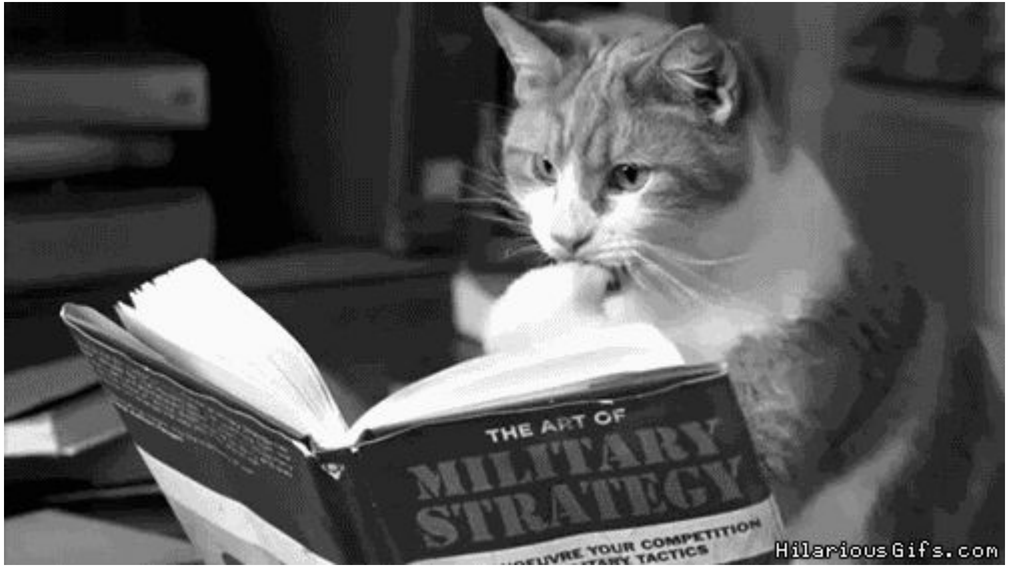
The 6 Steps of the Risk Management Framework

Categorize
Select
Implement
Asses
Authorize
Monitor

Risk Management Guidance

- ISO 27000 Series
  - 27001
  - 27002

- NIST Special Publications – Risk Management
  - SP 800-30: Risk assessment standard
  - SP 800-37: Guide for Risk Management Framework Implementation
  - SP 800-39: Managing information security risk



Risk Management Framework (RMF)

- Align risk tolerance with security strategy
- Define an appropriate response to threats
- Reduce operational losses from realized threats
- Improve deployment of protective resources

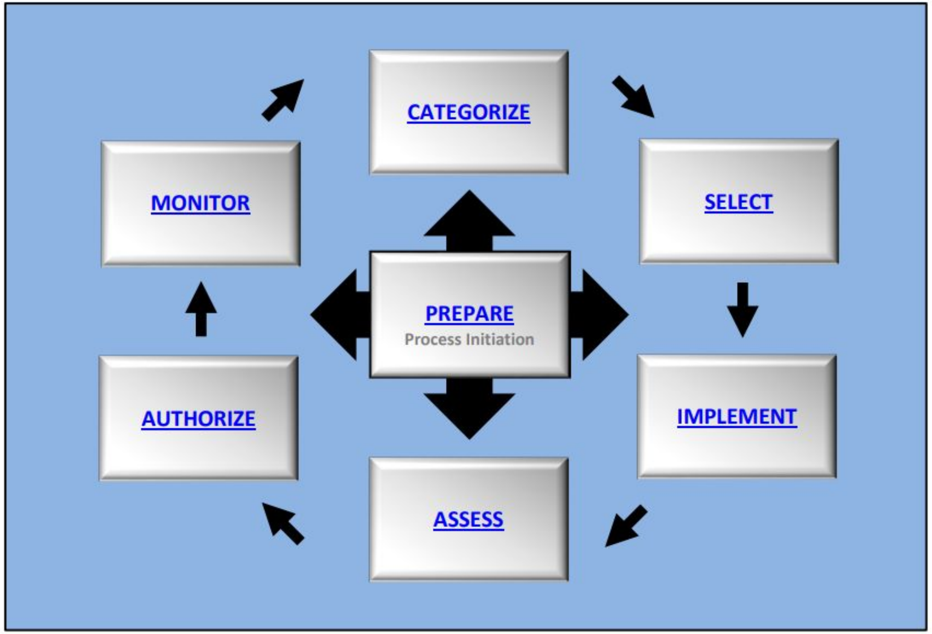


FIGURE 2: RISK MANAGEMENT FRAMEWORK

Cybersecurity Risk Management

Current State

1. Highest Value First
2. Asset Focused; Some Organizational
    - Inconsistency, silo’d, separated costs, high overhead
3. System Centric
4. Vulnerability-based
5. Qualitative and Anecdotal
6. Some Quantitative

Cybersecurity is a function of IT Department

Desired State

1. Highest Value First
2. Enterprise-Wide (including Third Parties)
    - Consistency, holistic, synergy costs and less overhead
3. Business/Mission Centric
4. Predictive and Holistic-based
5. Standardized Qualitative
6. Data Science Quantitative

Cybersecurity is part of Enterprise Risk Management

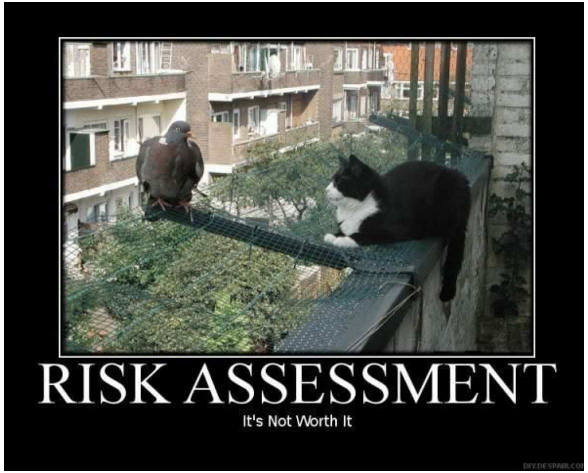
Quantitative vs. Qualitative Risk Analysis

- There are different methods to determine the risk exposure to an asset

- Qualitative Analysis
    - Relies on prioritization of threats based upon their severity

- Quantitative Analysis
    - Uses financial measures and dollar values to determine risk exposure

- Organizations typically rely on combining the two techniques to perform risk analysis



Qualitative vs Quantitative

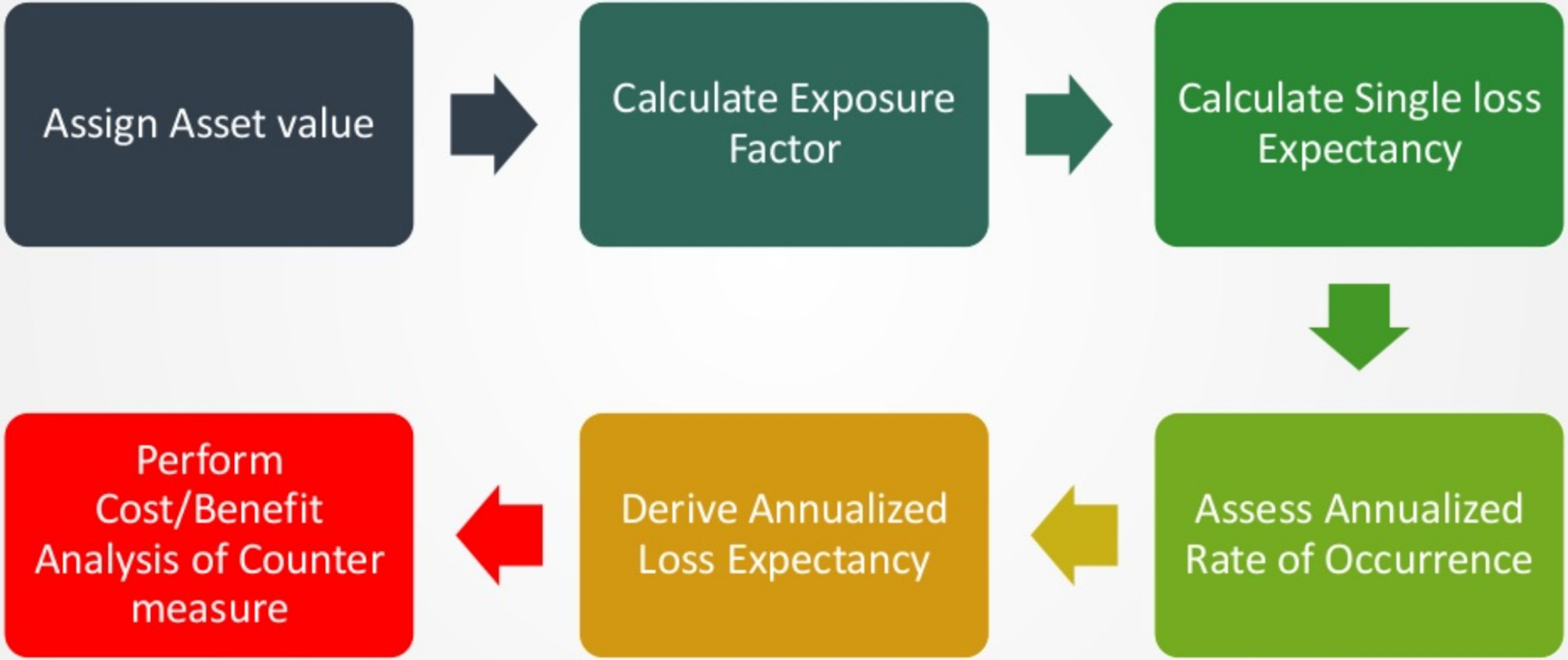
Qualitative

- Requires no calculations
- Involves high degree of guess work
- Provides general areas and indications of risk
- Does not allow Cost/benefit analysis
- Based on opinions of individuals
- Eliminates the opportunity to create a dollar value for Cost/benefit analysis
- Hard to develop a security budget from the results

Quantitative

- Does more complex calculations
- Mathematical and statistical calculations
- Uses independently verifiable and objective metrics
- Allows cost/benefit analysis
- It is easier to automate
- Used in Risk management performance tracking
- Without automated tools, the process is very difficult
- More preliminary work is needed to gather detailed information about the environment

Quantitative Risk Analysis – 6 Steps



Assign Asset value

Calculate Exposure Factor

Calculate Single loss Expectancy

Assess Annualized Rate of Occurrence

Derive Annualized Loss Expectancy

Perform Cost/Benefit Analysis of Counter measure

Key Terms in Quantitative Analysis

Exposure Factor (EF)

- % loss the organization would suffer if a risk materializes
- Also referred to as loss potential

Single Loss Expectancy (SLE)

- Cost associated with a single realized risk against a specific asset
- SLE = AV * EF
- It is calculated in $ value

Annualized Rate of Occurrence (ARO)

- Frequency with which a specific threat will occur within a single year
- Range from 0 (threat will not occur) to very large numbers
- It is also known as probability determination

Annualized Loss Expectancy (ALE)

- Possible yearly cost of all instances of a specific threat realized against a specific asset
- ALE = SLE * ARO

Annual Cost of Safeguard (ACS)

- It’s the cost associated in procuring, developing, maintaining a control against a potential threat
- The ACS should not exceed the ALE

Quantitative Analysis

- **Single Loss Expectancy (SLE)**
- Asset Value (AV) x Exposure Factor (EF) = SLE
- The exposure factor represents the percentage of loss a realized threat could have on a certain asset

- **Annualized Loss Expectancy (ALE)**
- SLE x Annualized Rate of Occurrence (ARO) = ALE
- The annualized rate of occurrence (ARO) is the value that represents the estimated possibility of a specific threat taking place

Example

- Tornado is estimated to damage 50% of a facility if it hits, and the value of the facility is $200,000. The probability is once every ten years.

  AV x EF = SLE = 200,000 x .50 = 100,000

  SLE x ARO = ALE = 100,000 x .10 = 10,000

  ALE is $10,000

- Management should not spend over $10,000 in countermeasures trying to protect against this risk

Cost-Benefit Analysis

- Return on Investment (ROI)
- Total Cost of Ownership (TCO)
- To demonstrate the financial benefits of deploying a control, a cost-benefit analysis calculation should be performed
- If the TCO is less than the ALE, then the ROI is positive

Cost-Benefit Analysis Example

$10K	ALE (before – per calculation)
- $1K	ALE (after – policy deductible)
- $2K	TCO (insurance premium)
$7K	ROI (financial benefit)
=======	

Qualitative Risk Analysis Methods

Brainstorming

- A group decision-making technique designed to generate a large number of creative ideas through an interactive process.

Delphi Technique

- Delphi is based on the principle that decisions from a structured group of individuals are more accurate than those from unstructured group
- The experts answer questionnaires in two or more rounds. After each round, a facilitator provides an **anonymous** summary of the experts' decision from the previous round as well as the reasons they provided for their judgments

Storyboarding

- Processes are turned into panels of images depicting the process, so that it can be understood and discussed

Focus Groups

- Panels of users evaluate the user impact and state their likes and dislikes regarding the safeguard being evaluated

Surveys

- Used as an initial information gathering tool. Results of each survey can influence the content of other evaluation methods

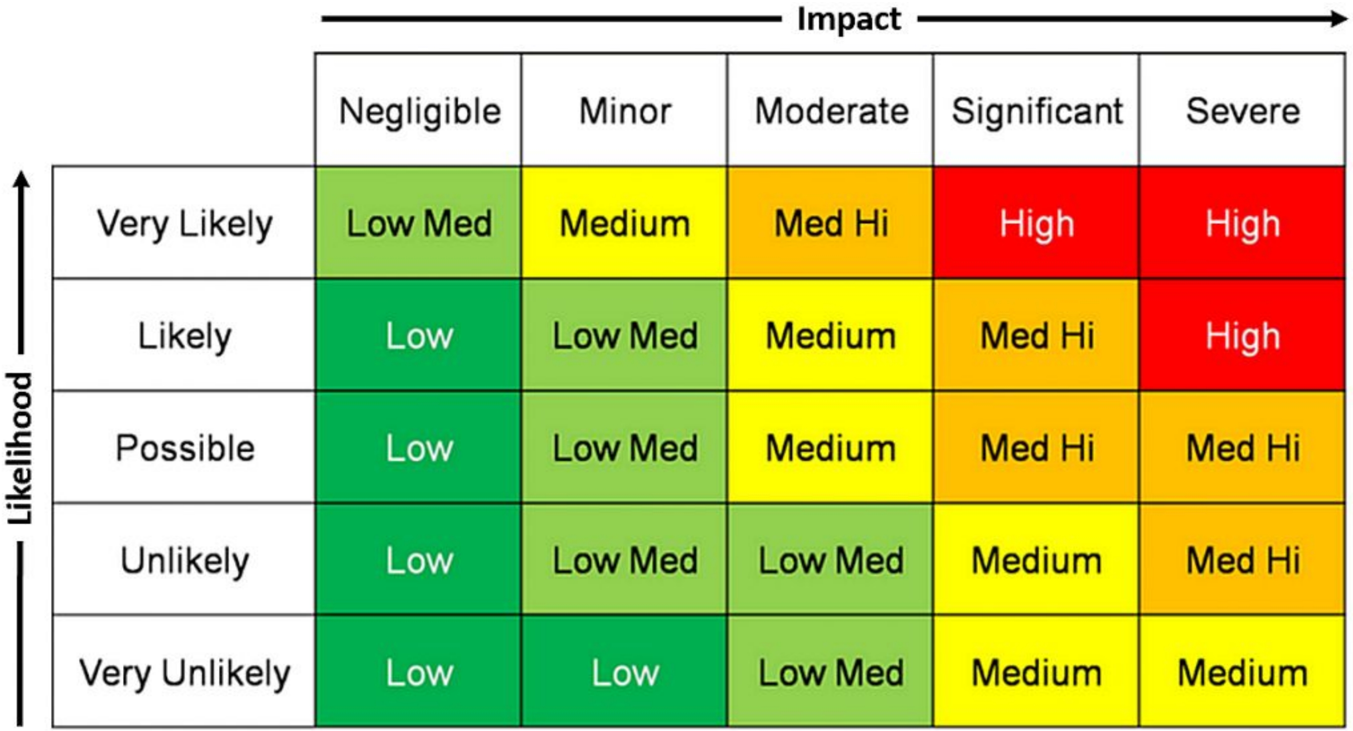
Questionnaires

- Limit the responses of participants more than surveys, so they should be used later in the process

Checklist

- Used to make sure safeguards being evaluated cover all aspects of the threats

Risk Matrix for Qualitative



Impact

Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Risk Handling

Avoid

Transfer/Share

Mitigate

Accept

Third Party Risk

Vendors (Supply Chain)

Business Partners

Contractors

Information & Data

Systems

Security Control (Countermeasures)

- Controls – technical or nontechnical risk mitigation mechanisms
    - Safeguards are preventative (proactive) controls
    - Countermeasures are detective (reactive) controls

- Security processes implemented to protect the confidentiality, integrity, and availability of an information system

- Controls typically fall into three different categories

- Controls employ different techniques to protect resources

Security Control Categories

- Administrative
  - Policies and procedures, personnel security, hiring practices
- Technical
  - Network access, application access, malware control, encryption
- Physical
  - Locks, guards, fire suppression systems

Security Control Types

- Preventative
- Detective
- Corrective
- Deterrent
- Recovery
- Compensating

TYPES OF SECURITY CONTROLS

	CONTROL FUNCTIONS		
	PREVENTATIVE	**DETECTIVE**	**CORRECTIVE**
PHYSICAL CONTROLS	• Fences • Gates • Locks	• CCTV • Surveillance Cameras	• Repair physical damage • Re-issue access cards
TECHNICAL CONTROLS	• Firewall • IPS • MFA • Antivirus	• IDS • Honeypots	• Vulnerability patching • Reboot a system • Quarantine a virus
ADMINISTRATIVE CONTROLS	• Hiring & termination policies • Separation of duties • Data classification	• Review access rights • Audit logs and unauthorized changes	• Implement a business continuity plan • Have an incident response plan

Residual Risk

- Residual risk is that risk that exists after the organization deploys a management-approved security control

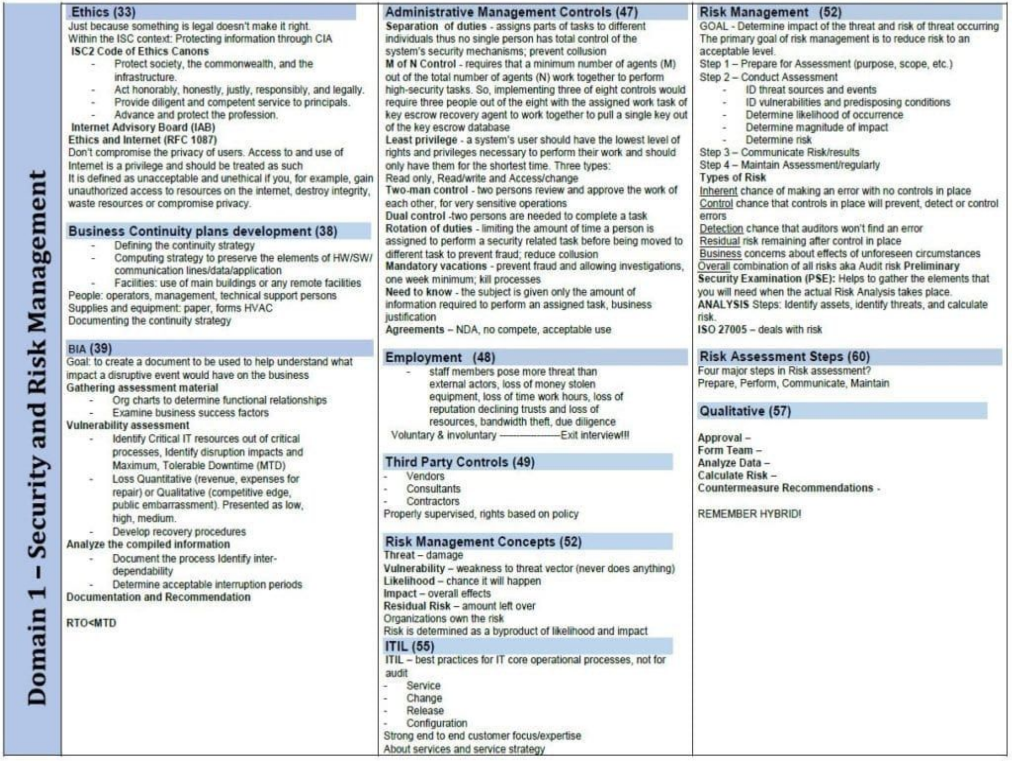
- It is understood that it is impossible to remove all risk exposure
  - Management should deploy security controls that will mitigate risk to an acceptable level

Residual Risk “Calculation”

Total Risk Exposure	X
(Controls Gap)	
Acceptable Risk Exposure	Y
	___________
Residual Risk	Z
0% Risk Exposure	===========

Class Exercise

Review: Cybersecurity Risk Management



Domain 1 – Security and Risk Management

Ethics (33)

Just because something is legal doesn't make it right.
Within the ISC context: Protecting information through CIA

ISC2 Code of Ethics Canons

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

Internet Advisory Board (IAB)

Ethics and Internet (RFC 1087)

Don't compromise the privacy of users. Access to and use of Internet is a privilege and should be treated as such
It is defined as unacceptable and unethical if you, for example, gain unauthorized access to resources on the internet, destroy integrity, waste resources or compromise privacy.

Business Continuity plans development (38)

- Defining the continuity strategy
- Computing strategy to preserve the elements of HW/SW/ communication lines/data/application
- Facilities: use of main buildings or any remote facilities

People: operators, management, technical support persons
Supplies and equipment: paper, forms HVAC
Documenting the continuity strategy

BIA (39)

Goal: to create a document to be used to help understand what impact a disruptive event would have on the business

Gathering assessment material

- Org charts to determine functional relationships
- Examine business success factors

Vulnerability assessment

- Identify Critical IT resources out of critical processes, Identify disruption impacts and Maximum, Tolerable Downtime (MTD)
- Loss Quantitative (revenue, expenses for repair) or Qualitative (competitive edge, public embarrassment). Presented as low, high, medium.
- Develop recovery procedures

Analyze the compiled information

- Document the process Identify inter-dependability
- Determine acceptable interruption periods

Documentation and Recommendation

RTO<MTD

Administrative Management Controls (47)

Separation of duties - assigns parts of tasks to different individuals thus no single person has total control of the system's security mechanisms; prevent collusion
M of N Control - requires that a minimum number of agents (M) out of the total number of agents (N) work together to perform high-security tasks. So, implementing three of eight controls would require three people out of the eight with the assigned work task of key escrow recovery agent to work together to pull a single key out of the key escrow database
Least privilege - a system's user should have the lowest level of rights and privileges necessary to perform their work and should only have them for the shortest time. Three types:
Read only, Read/write and Access/change
Two-man control - two persons review and approve the work of each other, for very sensitive operations
Dual control -two persons are needed to complete a task
Rotation of duties - limiting the amount of time a person is assigned to perform a security related task before being moved to different task to prevent fraud; reduce collusion
Mandatory vacations - prevent fraud and allowing investigations, one week minimum; kill processes
Need to know - the subject is given only the amount of information required to perform an assigned task, business justification
Agreements – NDA, no compete, acceptable use

Employment (48)

- staff members pose more threat than external actors, loss of money stolen equipment, loss of time work hours, loss of reputation declining trusts and loss of resources, bandwidth theft, due diligence

Voluntary & involuntary ——————Exit interview!!!

Third Party Controls (49)

- Vendors
- Consultants
- Contractors

Properly supervised, rights based on policy

Risk Management Concepts (52)

Threat – damage
Vulnerability – weakness to threat vector (never does anything)
Likelihood – chance it will happen
Impact – overall effects
Residual Risk – amount left over
Organizations own the risk
Risk is determined as a byproduct of likelihood and impact

ITIL (55)

ITIL – best practices for IT core operational processes, not for audit

- Service
- Change
- Release
- Configuration

Strong end to end customer focus/expertise
About services and service strategy

Risk Management (52)

GOAL - Determine impact of the threat and risk of threat occurring
The primary goal of risk management is to reduce risk to an acceptable level.
Step 1 – Prepare for Assessment (purpose, scope, etc.)
Step 2 – Conduct Assessment

- ID threat sources and events
- ID vulnerabilities and predisposing conditions
- Determine likelihood of occurrence
- Determine magnitude of impact
- Determine risk

Step 3 – Communicate Risk/results
Step 4 – Maintain Assessment/regularly

Types of Risk

Inherent chance of making an error with no controls in place
Control chance that controls in place will prevent, detect or control errors
Detection chance that auditors won't find an error
Residual risk remaining after control in place
Business concerns about effects of unforeseen circumstances
Overall combination of all risks aka Audit risk **Preliminary Security Examination (PSE):** Helps to gather the elements that you will need when the actual Risk Analysis takes place.
ANALYSIS Steps: Identify assets, identify threats, and calculate risk.
ISO 27005 – deals with risk

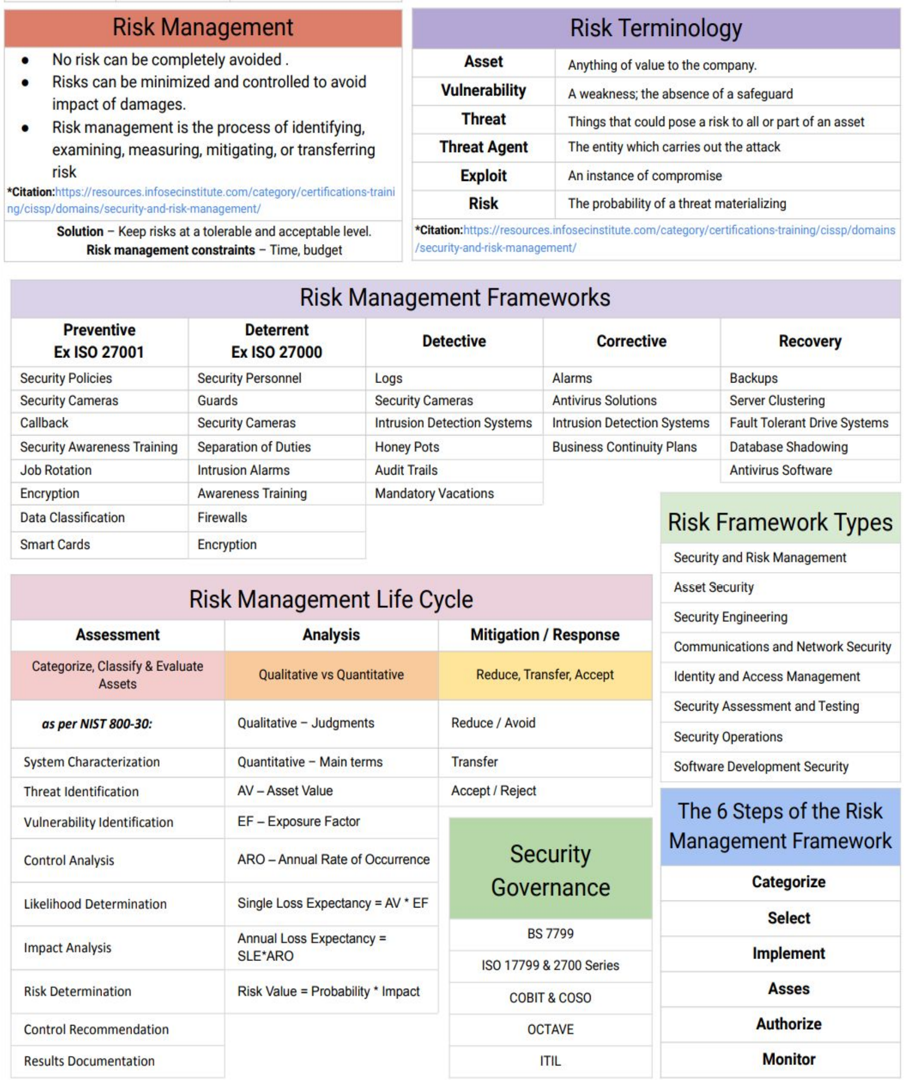
Risk Assessment Steps (60)

Four major steps in Risk assessment?
Prepare, Perform, Communicate, Maintain

Qualitative (57)

Approval –
Form Team –
Analyze Data –
Calculate Risk –
Countermeasure Recommendations -

REMEMBER HYBRID!



Risk Management

- No risk can be completely avoided .
- Risks can be minimized and controlled to avoid impact of damages.
- Risk management is the process of identifying, examining, measuring, mitigating, or transferring risk

***Citation:**https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Solution – Keep risks at a tolerable and acceptable level.
Risk management constraints – Time, budget

Risk Terminology

Asset	Anything of value to the company.
Vulnerability	A weakness; the absence of a safeguard
Threat	Things that could pose a risk to all or part of an asset
Threat Agent	The entity which carries out the attack
Exploit	An instance of compromise
Risk	The probability of a threat materializing

***Citation:**https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Risk Management Frameworks

Preventive Ex ISO 27001	Deterrent Ex ISO 27000	Detective	Corrective	Recovery
Security Policies	Security Personnel	Logs	Alarms	Backups
Security Cameras	Guards	Security Cameras	Antivirus Solutions	Server Clustering
Callback	Security Cameras	Intrusion Detection Systems	Intrusion Detection Systems	Fault Tolerant Drive Systems
Security Awareness Training	Separation of Duties	Honey Pots	Business Continuity Plans	Database Shadowing
Job Rotation	Intrusion Alarms	Audit Trails		Antivirus Software
Encryption	Awareness Training	Mandatory Vacations		
Data Classification	Firewalls			
Smart Cards	Encryption			

Risk Framework Types

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Risk Management Life Cycle

Assessment	Analysis	Mitigation / Response
Categorize, Classify & Evaluate Assets	Qualitative vs Quantitative	Reduce, Transfer, Accept
as per NIST 800-30:	Qualitative – Judgments	Reduce / Avoid
System Characterization	Quantitative – Main terms	Transfer
Threat Identification	AV – Asset Value	Accept / Reject
Vulnerability Identification	EF – Exposure Factor	
Control Analysis	ARO – Annual Rate of Occurrence	
Likelihood Determination	Single Loss Expectancy = AV * EF	
Impact Analysis	Annual Loss Expectancy = SLE*ARO	
Risk Determination	Risk Value = Probability * Impact	
Control Recommendation		
Results Documentation		

Security Governance

- BS 7799
- ISO 17799 & 2700 Series
- COBIT & COSO
- OCTAVE
- ITIL

The 6 Steps of the Risk Management Framework

- **Categorize**
- **Select**
- **Implement**
- **Asses**
- **Authorize**
- **Monitor**

Review: Cybersecurity Risk Management

Current State

1. Highest Value First
2. Asset Focused; Some Organizational
   - Inconsistency, silo’d, separated costs, high overhead
3. System Centric
4. Vulnerability-based
5. Qualitative and Anecdotal
6. Some Quantitative

Cybersecurity is a function of IT Department

Desired State

1. Highest Value First
2. Enterprise-Wide (including Third Parties)
   - Consistency, holistic, synergy costs and less overhead
3. Business/Mission Centric
4. Predictive and Holistic-based
5. Standardized Qualitative
6. Data Science Quantitative

Cybersecurity is part of Enterprise Risk Management https://www.csiac.org/wp-content/uploads/2021/03/2021-03-19-csiac-dod-cybersecurity-policy-chart.pdf