

Protecting Information Assets

- Week 2 -

Understanding an Organization's Risk Environment

MIS5206 Week 2

- In the News
- Readings
- Week 1 Review
- Understanding an Organization's Risk Environment
- Test Taking Tip
- Quiz

In the News

Anatomy of a Social Media Attack

“Social media threats are at an all-time high, ranging from account hijacking to impersonation attacks, scams, and new ways of distributing malware and executing phishing attacks...

Adversaries traditionally target a corporate network using two phases: reconnaissance and exploitation.

When attackers use social media, their strategy is similar, but the methods of attack are quite different. In social media, targeting an organization and corporate network involves footprinting, monitoring and profiling, impersonating or hijacking, and, finally, attacking....

By impersonating a key executive, an attacker can quickly establish trust to befriend other employees.”

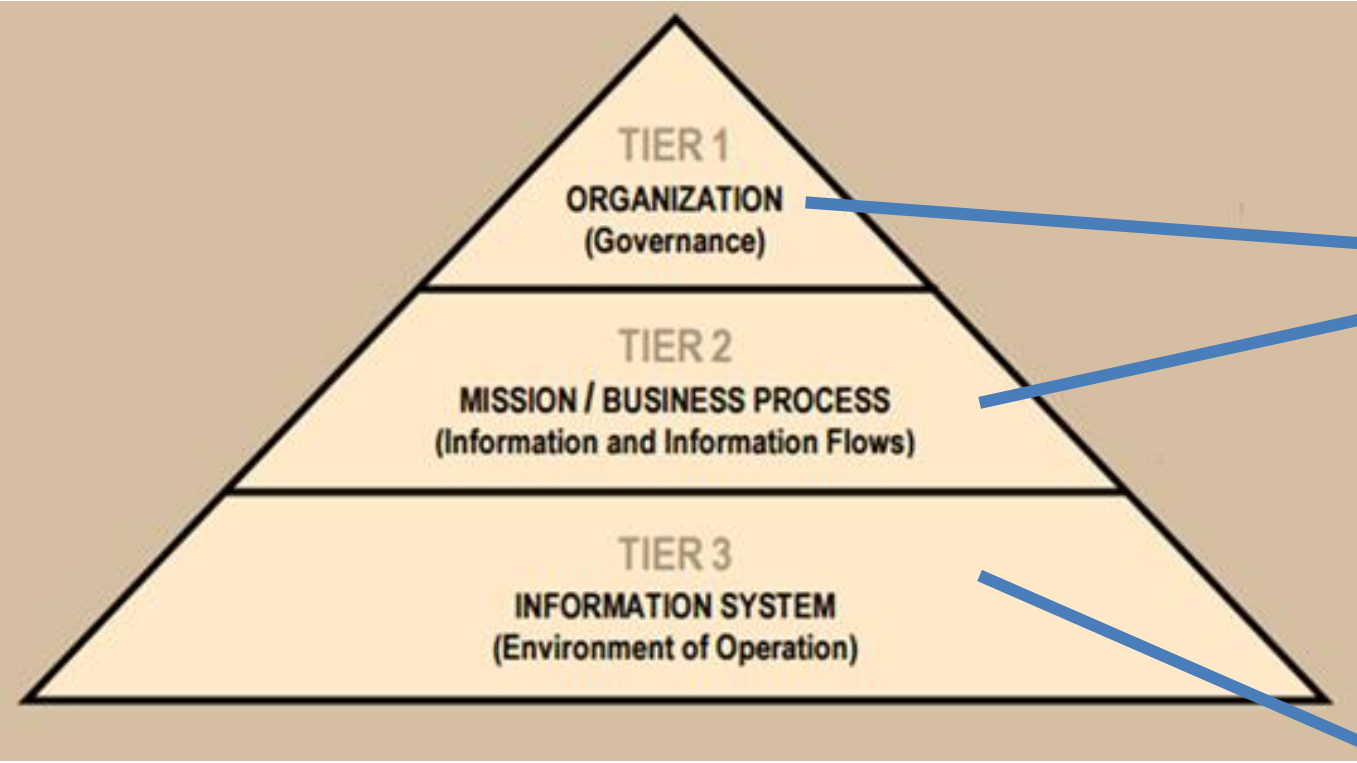
<http://www.darkreading.com/analytics/anatomy-of-a-social-media-attack/a/d-id/1326680>

Reading

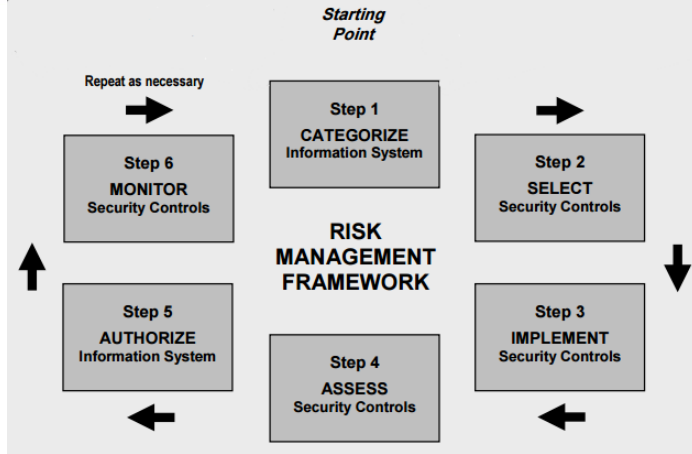
- Vacca Chapter 1
- ISACA RiskIT Framework pp. 1 - 42
- NIST Reading 1: “Framework for Improving Critical Infrastructure Cybersecurity”

Last time...

The RiskIT Framework



NIST Risk Management Framework



Understanding an Organization's Risk Environment

Information security means protecting information and information systems from:

- *Unauthorized access, use, disclosure* **(Confidentiality)**
- *Modification* **(Integrity)**
- *Disruption and destruction* **(Availability)**

Key concepts

Threat



Potential for the occurrence of a harmful event such as an attack

Vulnerability



Weakness that makes targets susceptible to an attack

Risk



Potential of loss from an attack

Risk Mitigation

Strategy for dealing with risk



What is a threat?

Any thing that has the potential to lead to:

- ***Unauthorized access, use, disclosure***
- ***Modification***
- ***Disruption or Destruction***

of an enterprises' information

Physical



Technical



Administrative



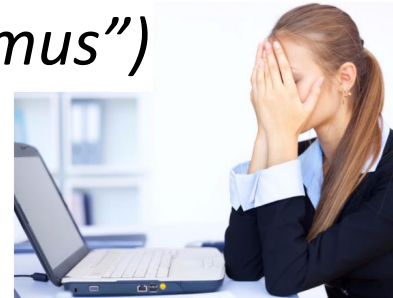
What is a threat...

Threats to information and information systems include:

- Purposeful attacks (*“Human malicious”*)



- Human errors (*“Human ignoramus”*)



- Structural Failures



- Environmental disruptions



Threats to information and information systems include:

Purposeful attacks

- Cyber attacks “are often aggressive, disciplined, well-organized, well-funded, and in a growing number of documented cases, very sophisticated
- Successful attacks on private and public sector information systems can result in serious or grave damage to organizations, and the national and economic security...” of the Nation
- “Given the significant and growing danger in these threats, it is imperative that leaders at all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks.”

Taxonomy of threat sources

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66

| Type of Threat Source | Description | Characteristics |
|---|--|-------------------------------|
| ADVERSARIAL <ul style="list-style-type: none"> - Individual <ul style="list-style-type: none"> - Outsider - Insider - Trusted Insider - Privileged Insider - Group <ul style="list-style-type: none"> - Ad hoc - Established - Organization <ul style="list-style-type: none"> - Competitor - Supplier - Partner - Customer - Nation-State | <p>Individuals, groups, organizations, or states that seek to exploit the organization’s dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).</p> | Capability, Intent, Targeting |
| ACCIDENTAL <ul style="list-style-type: none"> - User - Privileged User/Administrator | Erroneous actions taken by individuals in the course of executing their everyday responsibilities. | Range of effects |
| STRUCTURAL <ul style="list-style-type: none"> - Information Technology (IT) Equipment <ul style="list-style-type: none"> - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls <ul style="list-style-type: none"> - Temperature/Humidity Controls - Power Supply - Software <ul style="list-style-type: none"> - Operating System - Networking - General-Purpose Application - Mission-Specific Application | Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters. | Range of effects |
| ENVIRONMENTAL <ul style="list-style-type: none"> - Natural or man-made disaster <ul style="list-style-type: none"> - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage <ul style="list-style-type: none"> - Telecommunications - Electrical Power | <p>Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.</p> <p>Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).</p> | Range of effects |

Taxonomy of cybersecurity threat sources

| Type of Threat Source | Description | Characteristics |
|--|--|--------------------------------------|
| <p>ADVERSARIAL</p> <ul style="list-style-type: none"> - Individual <ul style="list-style-type: none"> - Outsider - Insider - Trusted Insider - Privileged Insider - Group <ul style="list-style-type: none"> - Ad hoc - Established - Organization <ul style="list-style-type: none"> - Competitor - Supplier - Partner - Customer - Nation-State | <p>Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).</p> | <p>Capability, Intent, Targeting</p> |

NIST SP 800-30r1 "Guide for Conducting Risk Assessments", page 66



Human malicious threat examples

- Accessing public material (80 percent unclassified and open to public)
- Black-hat hackers (lightweights to heavyweights)
- Bombing
- Career criminals
- Computer viruses (stealth, polymorphic, macro; over 6,500 different viruses identified)
- Corporate espionage (spies)
- Crackers/scriptkiddies (amateurs, novices; considerably less skilled than hackers)
- Cybercrime/fraud
- Data diddling
- Denial-of-service attacks
- Dumpster diving
- Employees, management (greed, vices, financial pressure, extravagant lifestyle, real or imagined grievances, workplace pressure/stress)
- High-energy radio frequency attacks (laser-like device aimed at buildings housing computers; high-frequency radio waves melt computer chips)
- Impersonation/spoofing (e-mail spoofs, anonymous eMailers, use of someone's login and password)
- Intelligence agencies
- Looping Internet Protocol ISP address (always-on Internet connections vulnerable)
- Password crackers (such as Cracker and LoPht Crack software)
- Physical attacks
- Remote access control software (examples include PCAnywhere, Timbuktu, NetBus, BackOrifice)
- Sabotage
- Social engineering (attacks against persons; using fake badges, blackmail, threat, harassment, bribery and impersonation)
- Surveillance (shoulder surfing, high-powered photography)
- Terrorists
- Trojan horses
- Unshredder software
- Van Eck receptors
- Vendors/suppliers/customers
- Vulnerability scanning software (such as Nessus, CyberCop software)
- War dialing
- Web crawlers

Anatomy of an Attack

Threat landscape

I. Social engineering techniques target specific individuals

Spear-phishing is a common technique used to lure targeted users into downloading initial-stage malware.

II. Establish a beachhead

Initial-stage malware executes shellcode and calls home for further instructions.

III. Infiltration

Custom executables with objective-specific malware is downloaded. Remote commands are executed according to attacker objectives.

IV. Persistence

Attackers wait for opportune attack times. "Sleep" commands are often executed between "run" commands to avoid detection.

V. Accomplish Objectives (data harvesting, sabotage, and more)

Remote commands issued to extract data, modify applications, or sabotage systems.

(McAfee, 2011)

Anatomy of an Attack

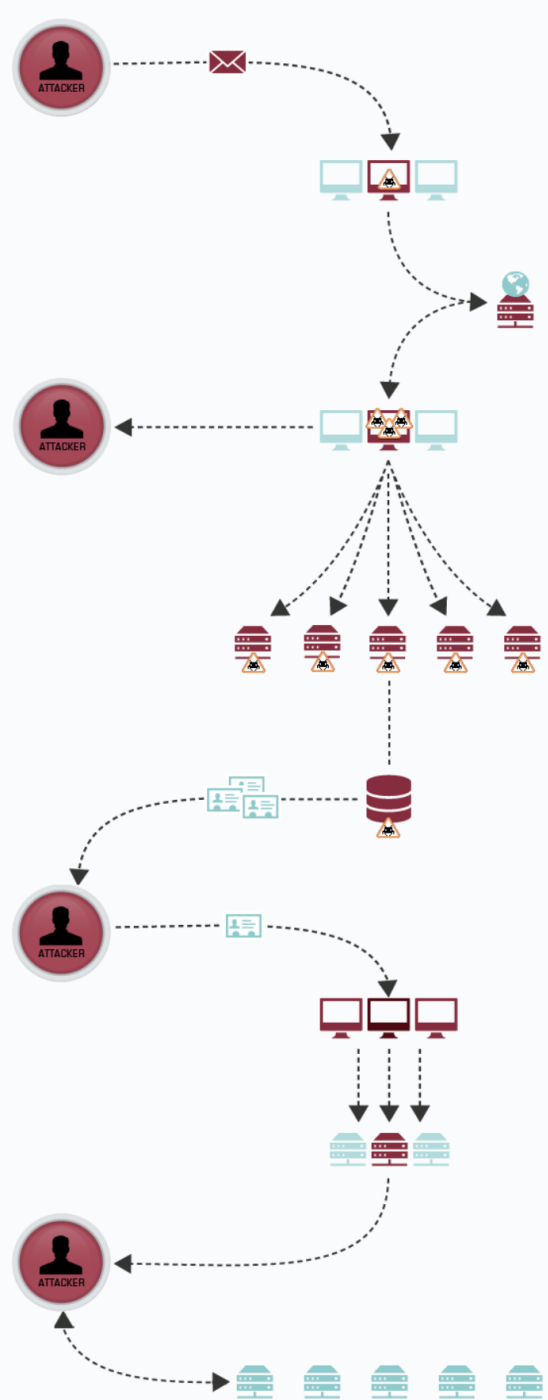
(MANDIANT, 2015)

Threat landscape

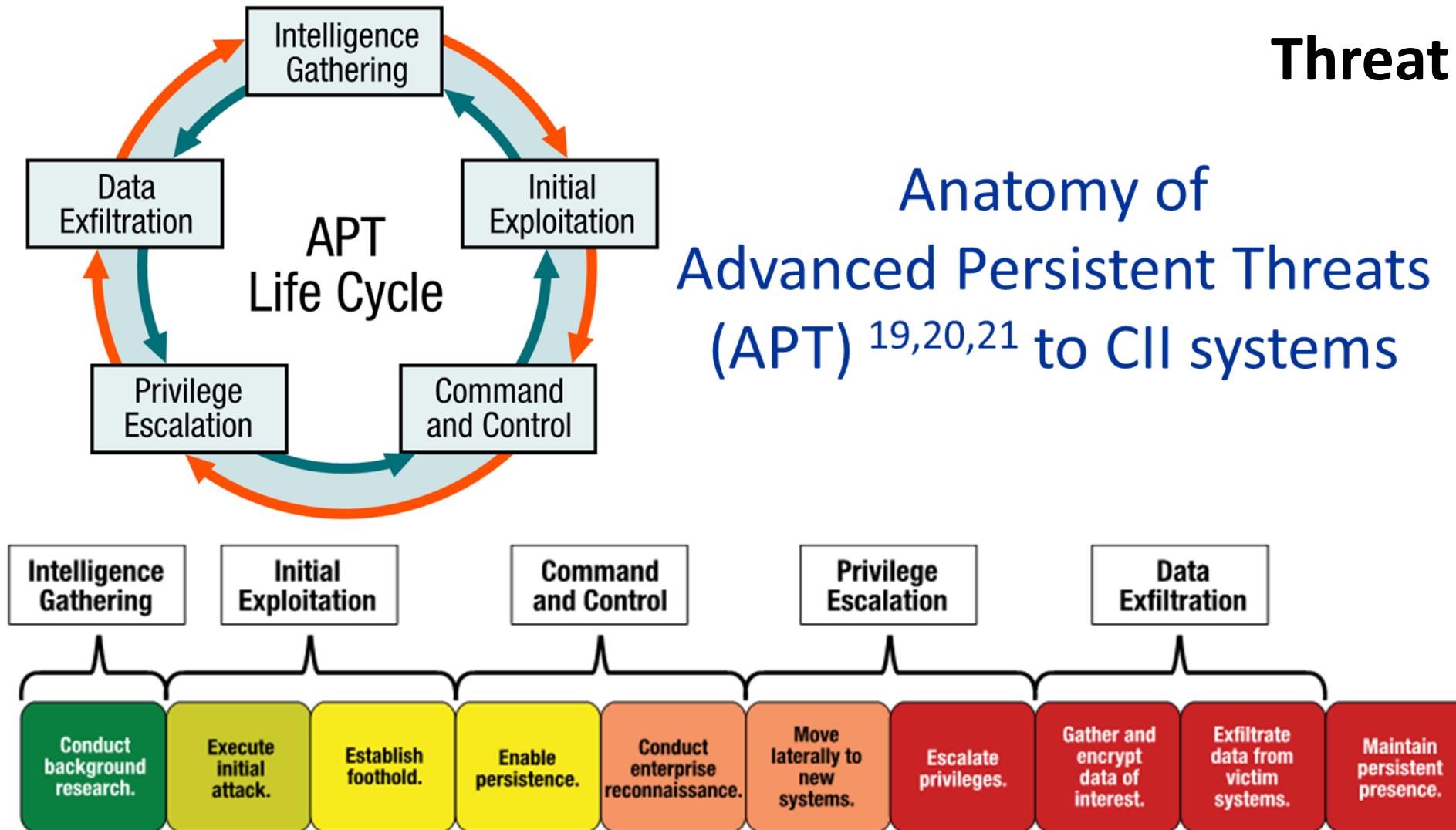
1. Attacker sends spear fishing e-mail
 - Custom malware is installed
2. Victim opens attachment
 - Custom malware communicates to control web site
3. Custom malware communicates to control web site
 - Pulls down additional malware
4. Attacker establishes multiple backdoors
5. Attacker accesses system
 - Dumps account names and passwords from domain controller
6. Attacker cracks passwords
 - Has legitimate user accounts to continue attack undetected
7. Attacker reconnaissance
 - Identifies and gathers data
8. Data collected on staging server
9. Data exfiltrated
10. Attacker covers tracks
 - Deletes files
 - Can return any time

Assets

Advanced threats usually maintain remote access to target environments for 6-18 months before being detected (i.e. they are persistent)
(Holcomb & Stapf, 2014)



Anatomy of Advanced Persistent Threats (APT) ^{19,20,21} to CII systems



Advanced threats usually maintain remote access to target environments for 6-18 months before being detected ²²

Taxonomy of cybersecurity threat sources

| Type of Threat Source | Description | Characteristics |
|---|--|------------------|
| ACCIDENTAL - User - Privileged User/Administrator | Erroneous actions taken by individuals in the course of executing their everyday responsibilities. | Range of effects |

NIST SP 800-30r1 "Guide for Conducting Risk Assessments", page 66



Human non-malicious threat examples

- Computer operator errors
- Data entry (input) errors
- Inadequate access controls
- Inadequate training
- Inadequate human resource policies
- Inadequate program testing/controls incorporated into computer programs
- Inadequate risk analysis undertaken
- Inadequate supervision
- Lack of ethics
- Mislaid disk files
- Physical damage to disk
- Poor management philosophy/attitude
- Unlocked trash containers
- Update of wrong file
- Weak internal controls

Taxonomy of cybersecurity threat sources

| Type of Threat Source | Description | Characteristics |
|--|--|-------------------------|
| <p>STRUCTURAL</p> <ul style="list-style-type: none"> - Information Technology (IT) Equipment <ul style="list-style-type: none"> - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls <ul style="list-style-type: none"> - Temperature/Humidity Controls - Power Supply - Software <ul style="list-style-type: none"> - Operating System - Networking - General-Purpose Application - Mission-Specific Application | <p>Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.</p> | <p>Range of effects</p> |

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66

MIS 5206 Protecting Information Assets



Structural Threat Examples

- Air conditioning failure
- Building collapse
- Destruction of data, disks, documents, reports
- Destruction of water mains, sewer lines
- Failure of hardware
- Failure of fire alarms, smoke detectors
- Failure of computer programs
- Freak accidents
- Gas line explosions
- Power outages (brownouts, blackouts, transients, spikes, sags and power surges)
- Product failure
- Software failure (operating system, database software)

Taxonomy of cybersecurity threat sources

| Type of Threat Source | Description | Characteristics |
|---|--|-------------------------|
| <p>ENVIRONMENTAL</p> <ul style="list-style-type: none"> - Natural or man-made disaster - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage <ul style="list-style-type: none"> - Telecommunications - Electrical Power | <p>Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.</p> <p>Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).</p> | <p>Range of effects</p> |

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66



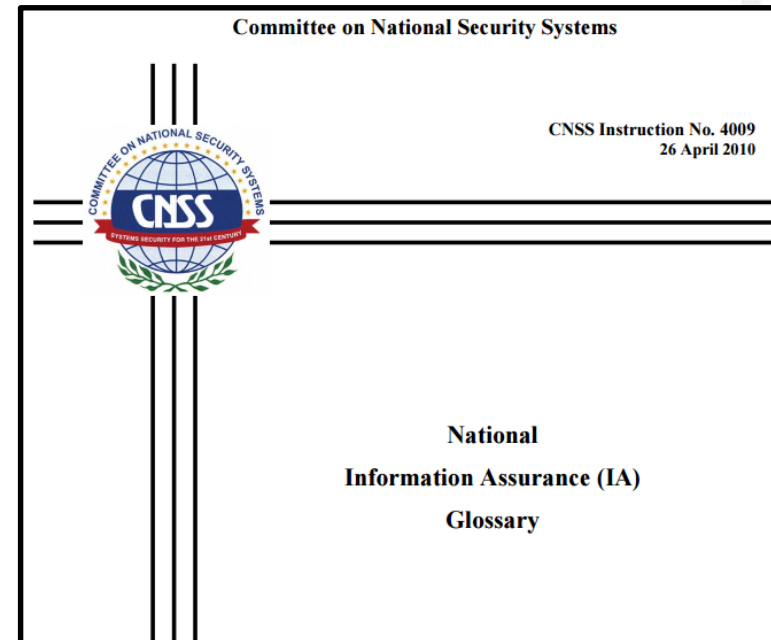
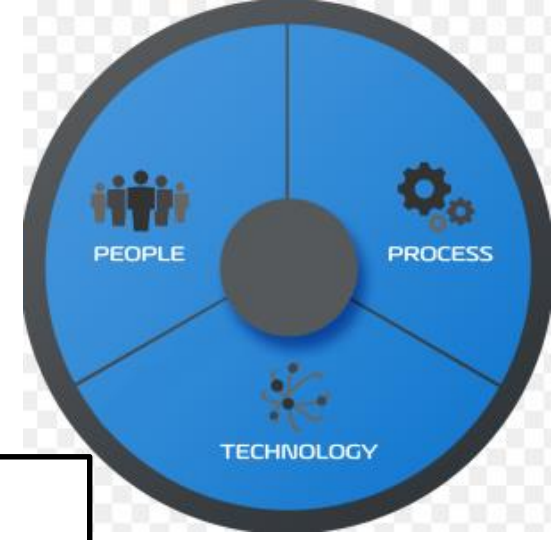
What is a Vulnerability?

Physical

Technical

Administrative

Any unaddressed susceptibility to a Physical, Technical or Administrative information security threat



Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

What is a Risk?

A measure of threat

Potential loss resulting from unauthorized:

- *Access, use, disclosure*
- *Modification*
- *Disruption or destruction*

...of an enterprises' information

Can be expresses in quantitative and qualitative terms

Physical

Technical

Administrative
(organizational,
governance)

Information security risks

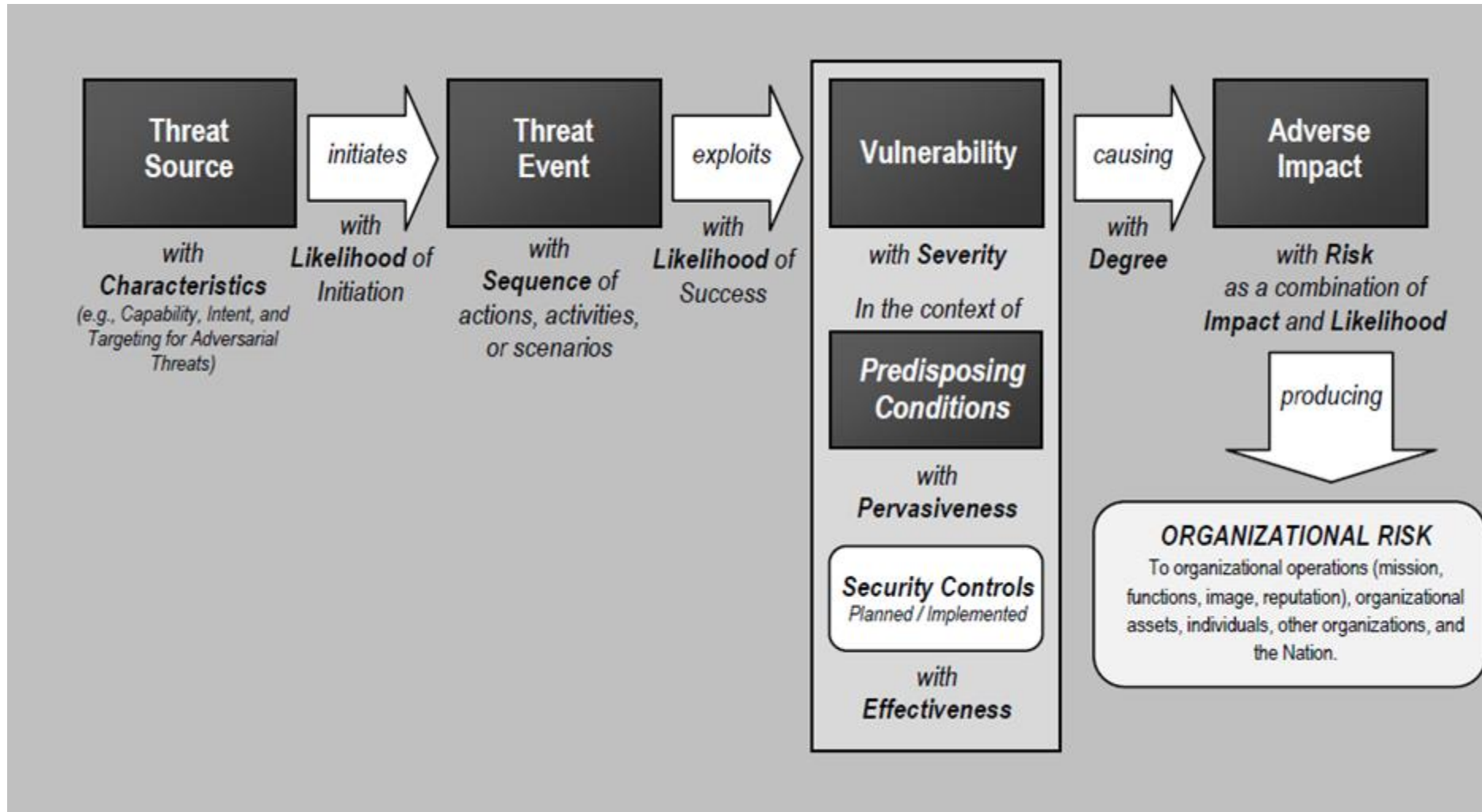
- Replacement costs (software, hardware, other)
- Backup restoration and recovery costs
- Reprocessing, reconstruction costs
- Crime (non-computer, computer)
- Loss of life
- Economic impact and financial loss
- Losses due to fraud, theft, larceny, bribery
- Impact of
 - lost competitive edge
 - lost data
 - lost time
 - lost productivity
 - lost business
- Bankruptcy
- Business interruption
- Frustration
- Ill will
- Injury
- Impacts of inaccurate data

Examples of types of information security risk

1. Safety
2. Compliance and regulatory
3. Financial
4. Legal
5. Reputational
6. Political
7. Strategic planning
8. Program/acquisition risk (cost, schedule, performance)
9. Project
10. Operational (mission/business)
11. Supply chain

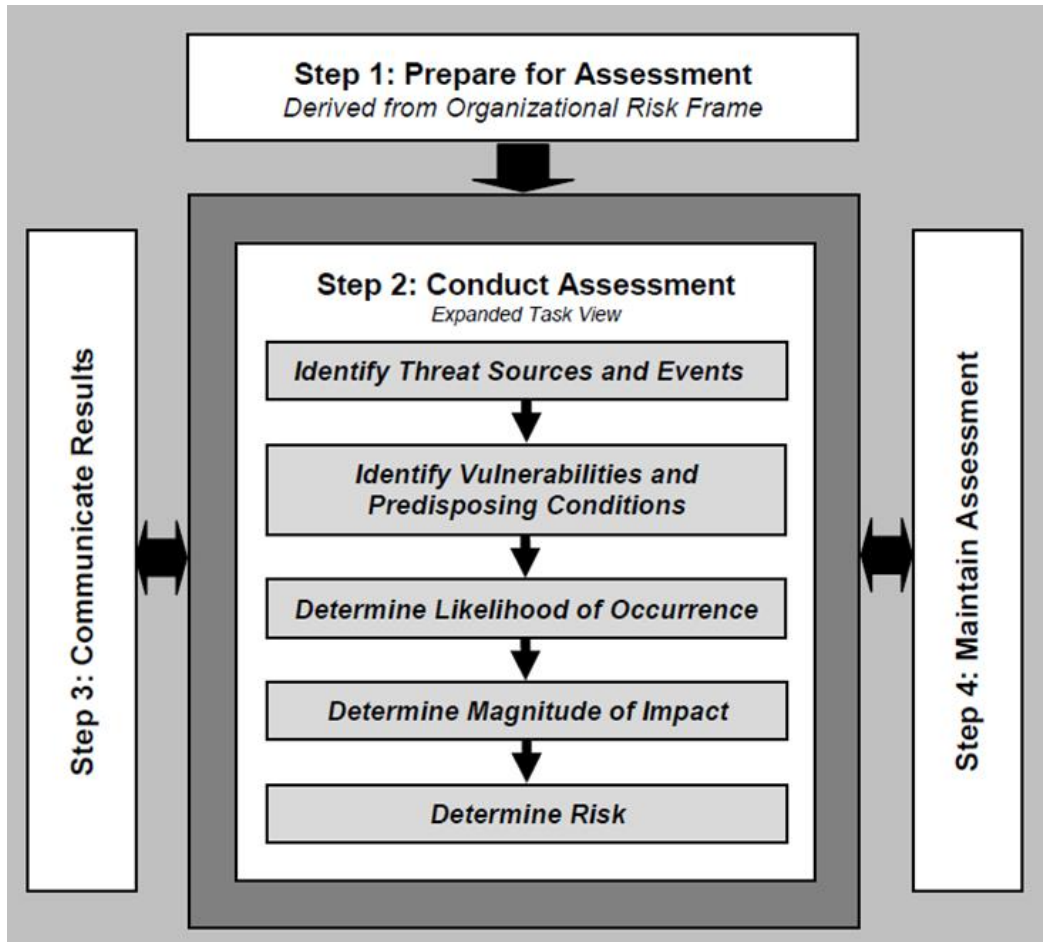


Example of a risk model



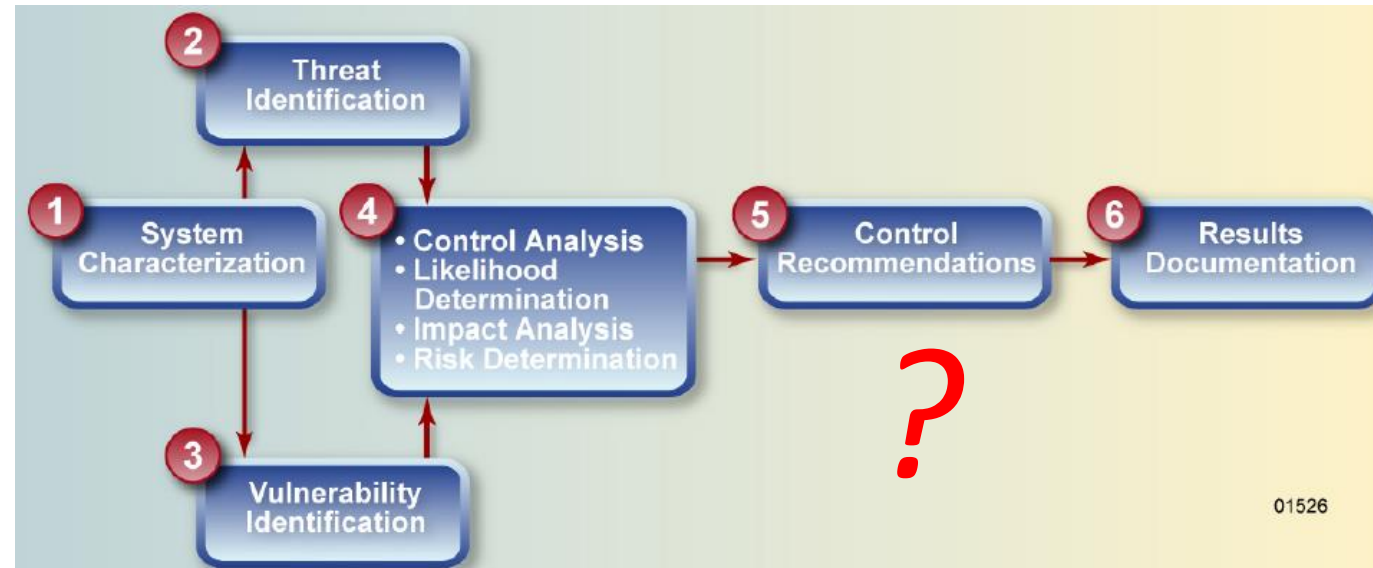
NIST SP 800-30r1 "Guide for Conducting Risk Assessments", page 21 and page 32

Risk assessment process



NIST SP 800-30r1 "Guide for Conducting Risk Assessments", page 32

MIS 5206 Protecting Information Assets



NIST SP 800-100 "Information Security Handbook: A Guide for Managers", page 95

NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Table of Contents

| | |
|------------------------------------|----|
| Executive Summary | 1 |
| 1.0 Framework Introduction | 3 |
| 2.0 Framework Basics..... | 7 |
| 3.0 How to Use the Framework | 13 |
| Appendix A: Framework Core..... | 18 |
| Appendix B: Glossary..... | 37 |
| Appendix C: Acronyms | 39 |

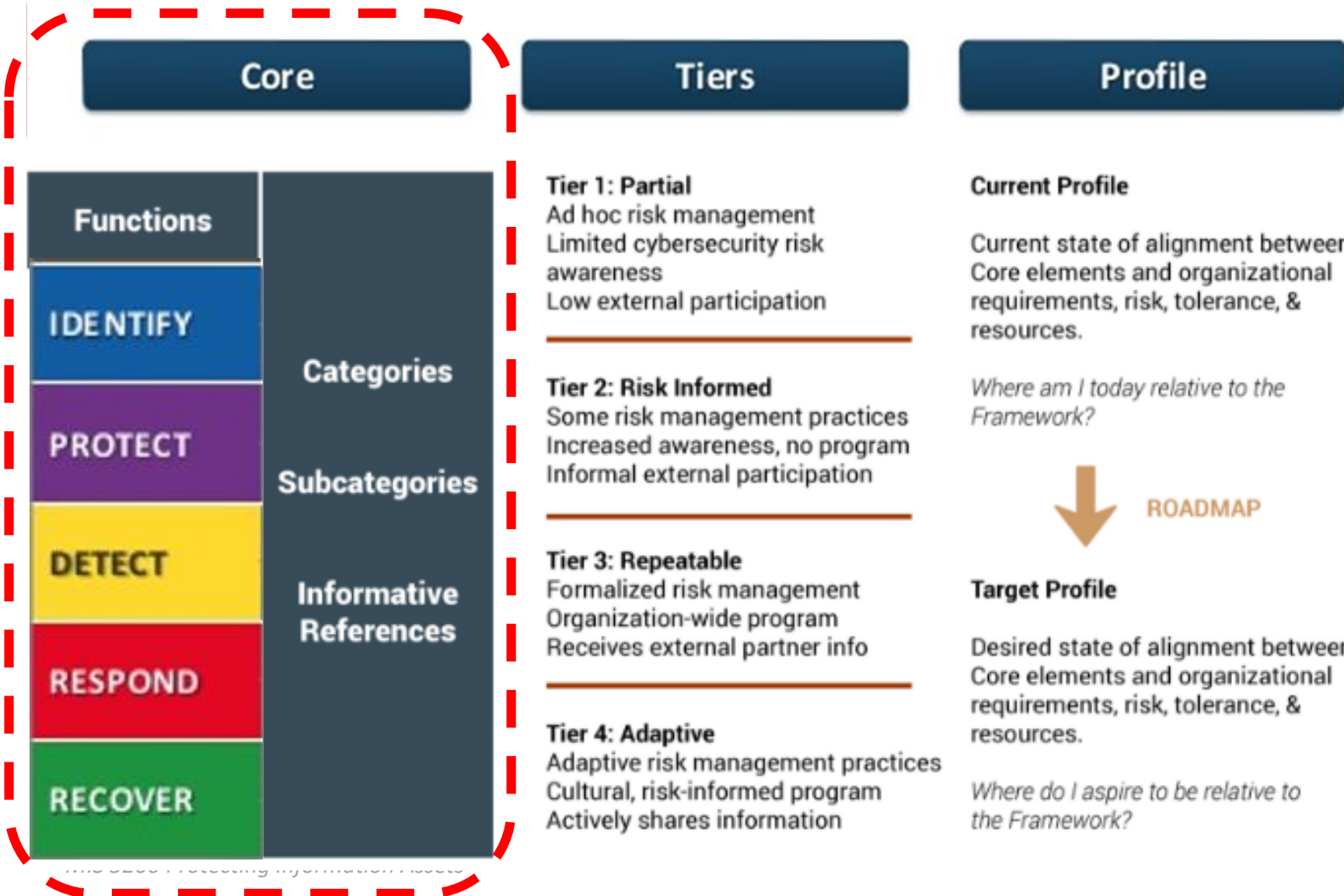
List of Figures

| | |
|--|----|
| Figure 1: Framework Core Structure | 7 |
| Figure 2: Notional Information and Decision Flows within an Organization | 12 |

List of Tables

| | |
|---|----|
| Table 1: Function and Category Unique Identifiers | 19 |
| Table 2: Framework Core | 20 |

NIST Cybersecurity Framework



Can be done at the:

- Organizational level
- Program level
- Project level



NIST Cybersecurity Framework's Core Functions

| | Functions | Categories | Subcategories | Informative References |
|---|-----------|------------|---------------|------------------------|
| What assets need protection? | IDENTIFY | | | |
| | | | | |
| What safeguards are available? | PROTECT | | | |
| | | | | |
| What techniques can identify incidents? | DETECT | | | |
| | | | | |
| What techniques can contain impacts of incidents? | RESPOND | | | |
| | | | | |
| What techniques can restore capabilities? | RECOVER | | | |
| | | | | |

NIST Cybersecurity Framework

functions and their categories

It is of paramount importance to first **identify**: what to protect, what to detect, what to respond to and recover from...

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|----------------------------|----------|----------------------------|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

NIST Cybersecurity Framework

Functions and their categories...

Identify (function): Develop the institutional understanding of which organizational systems, assets, data, and capabilities need to be protected, determine priority in light of organizational mission, and establish processes to achieve risk management goals.

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|----------------------------|----------|----------------------------|--------------------------|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |

NIST Cybersecurity Framework - Evaluate and profile your organization's capabilities

Profile

Current Profile

Current state of alignment between Core elements and organizational requirements, risk, tolerance, & resources.

Where am I today relative to the Framework?



ROADMAP

Target Profile

Desired state of alignment between Core elements and organizational requirements, risk, tolerance, & resources.

Where do I aspire to be relative to the Framework?

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|----------------------------|----------|----------------------------|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

Each category is rated

Tiers

Tier 1: Partial

Ad hoc risk management
Limited cybersecurity risk awareness
Low external participation

Tier 2: Risk Informed

Some risk management practices
Increased awareness, no program
Informal external participation

Tier 3: Repeatable

Formalized risk management
Organization-wide program
Receives external partner info

Tier 4: Adaptive

Adaptive risk management practices
Cultural, risk-informed program
Actively shares information

Can be done at the:

- Organizational level
- Program level
- Project level

Evaluation of an organization's cybersecurity capabilities

Profile

Current Profile

Current state of alignment between Core elements and organizational requirements, risk, tolerance, & resources.

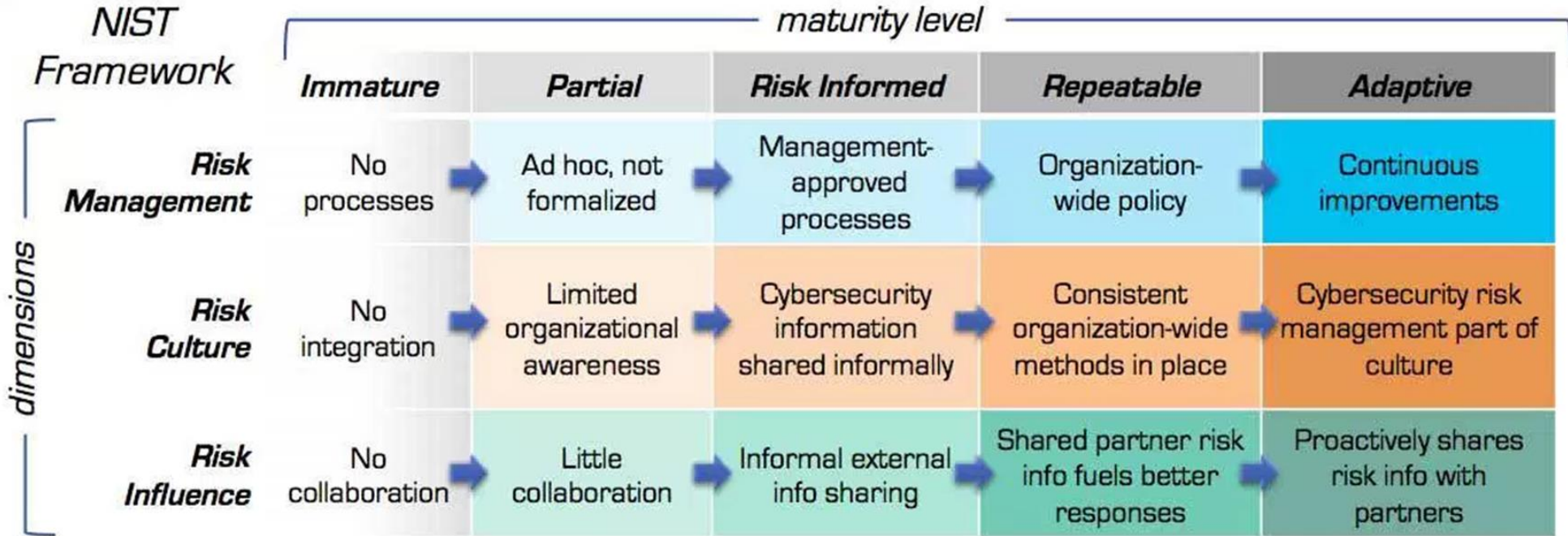
Where am I today relative to the Framework?



Target Profile

Desired state of alignment between Core elements and organizational requirements, risk, tolerance, & resources.

Where do I aspire to be relative to the Framework?



Assessing risk – financial method

1. **Estimate potential losses (SLE)**—This step involves determining the single loss expectancy (SLE). SLE is calculated as follows:

– **Single loss expectancy (SLE) = Asset value X Exposure factor**

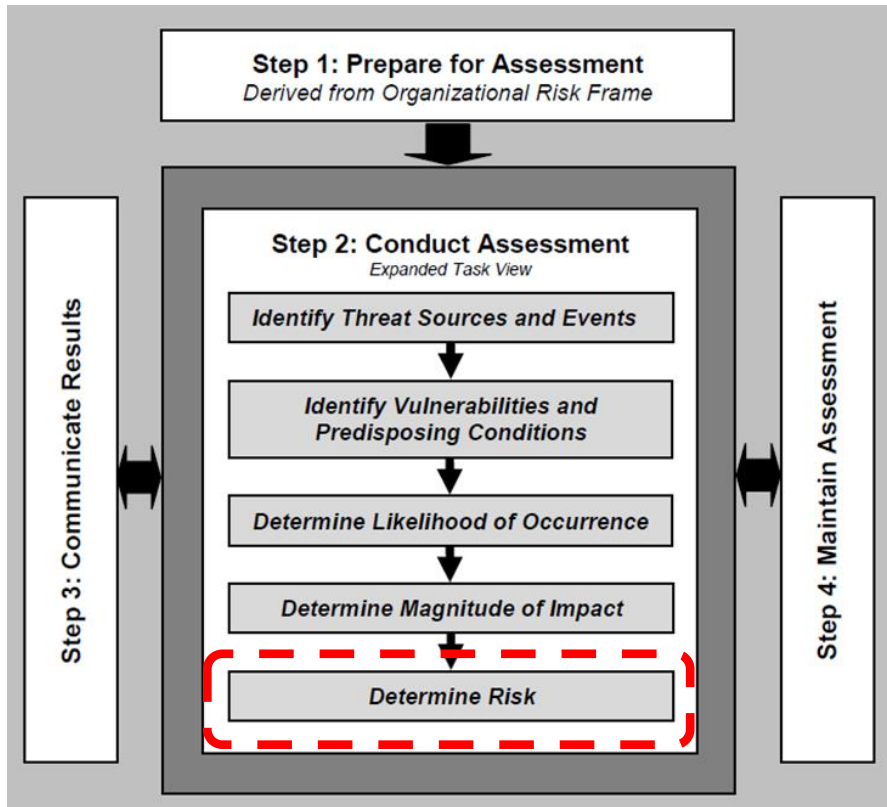
Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO)**—The purpose of a threat analysis is to determine the likelihood of an unwanted event. The goal is to estimate the **annual rate of occurrence (ARO)**. Simply stated, **how many times is this expected to happen in one year?**

3. **Determine annual loss expectancy (ALE)**—This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

– **Annualized loss expectancy (ALE) = Single loss expectancy (SLE) X Annualized rate of occurrence (ARO)**

Assessing IT risk – financial method




Annualized loss expectancy (ALE) =

Single loss expectancy (SLE) X Annualized rate of occurrence (ARO)

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 32

Assessing IT risk – relative “scale” method



The diagram shows a flow from Likelihood (green oval) to Threat (pink oval) and Vulnerability (yellow oval), which both lead to Risk (pink oval). Risk then leads to Impact (blue oval).

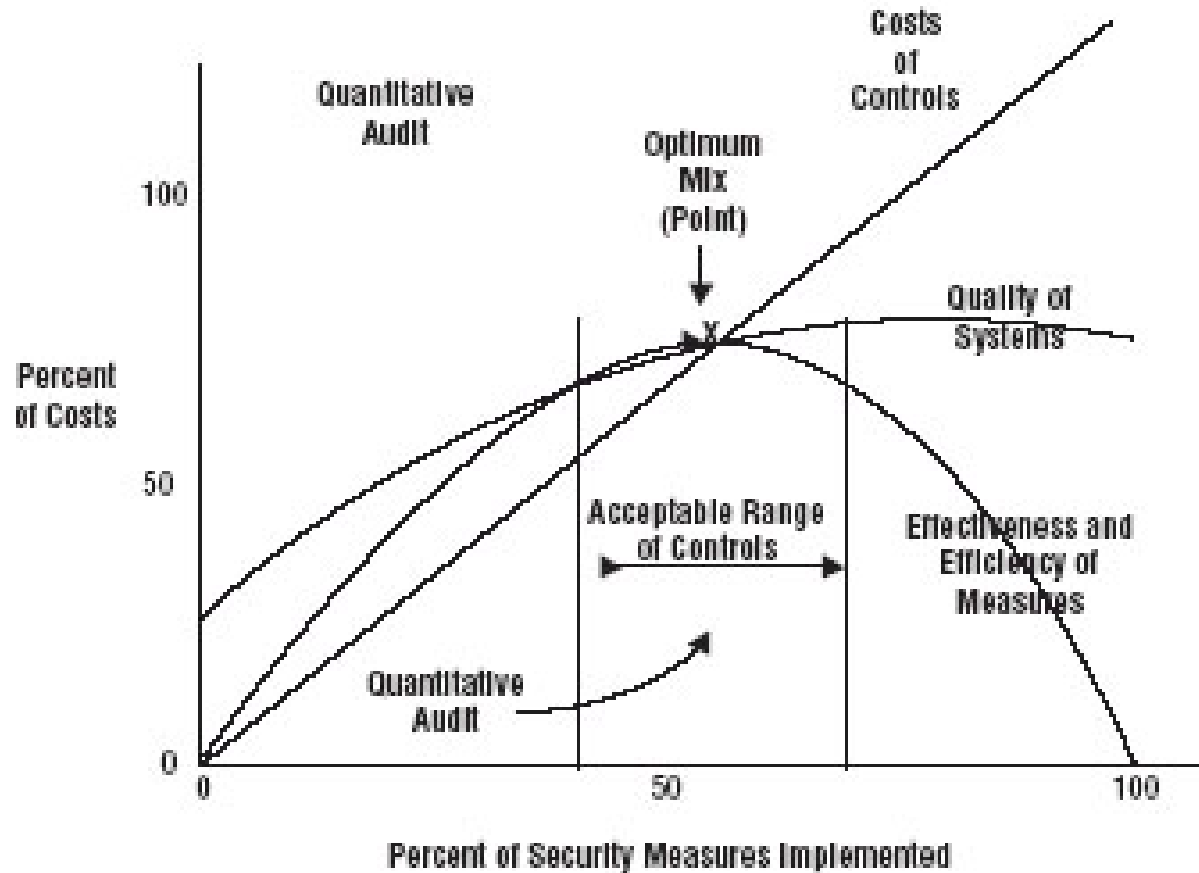
| | | Impact | | |
|-------------------|--|----------------------|----------------------|------------------------|
| Threat Likelihood | | Low (10) | Moderate (50) | High (100) |
| High (1.0) | | $10 \times 1.0 = 10$ | $50 \times 1.0 = 50$ | $100 \times 1.0 = 100$ |
| Moderate (0.5) | | $10 \times 0.5 = 5$ | $50 \times 0.5 = 25$ | $100 \times 0.5 = 50$ |
| Low (0.1) | | $10 \times 0.1 = 1$ | $50 \times 0.1 = 5$ | $100 \times 0.1 = 10$ |

Risk Scale: High (>50 to 100) Moderate (>10 to 50) Low (1 to 10)

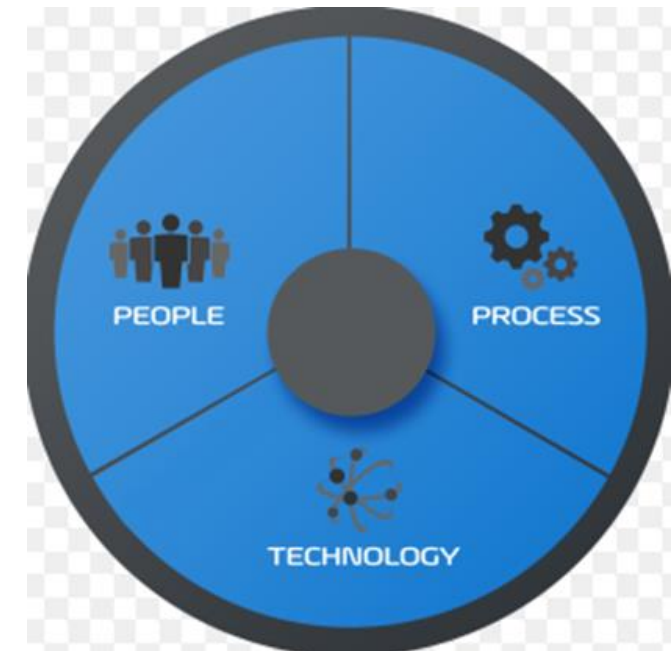
01527a

NIST SP 800-100 “Information Security Handbook: A Guide for Managers”, page 99

What is a Risk Mitigation?



An approach for lessening or avoiding the impact of a risk (i.e. potential impact) in an acceptable and cost-effective manner



Risk mitigation approaches

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure)
- Fences
- Role-based access control
- Segregation of duties
- Redundant data center
- Corporate code of conduct
- Internal audit
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Firewalls
- Change management
- Penetration testing
- Placement of authentication / authorization / database / accounting servers in secure location
- Receptionists
- Residue controls - disintegrator / shredders
- Secure file wipes
- Secure passwords
- Single sign-on
- Environmental controls (air conditioners, humidifiers)

Risk mitigation approaches – Physical controls ?

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure)
- Fences
- Role-based access control
- Segregation of duties
- Redundant data center
- Corporate code of conduct
- Internal audit
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Firewalls
- Change management
- Penetration testing
- Placement of authentication / authorization / database / accounting servers in secure location
- Receptionists
- Residue controls - disintegrator / shredders
- Secure file wipes
- Secure passwords
- Single sign-on
- Environmental controls (air conditioners, humidifiers)

Risk mitigation approaches – Physical controls?

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- **Canine patrols**
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure)
- **Fences**
- Role-based access control
- Segregation of duties
- **Redundant data center**
- Corporate code of conduct
- Internal audit
- **Grounds lighting**
- Intrusion detection software
- **Locked doors and terminals**
- **Motion-detection devices**
- Network firewalls
- Change management
- Penetration testing
- **Placement of authentication / authorization / database / accounting servers in secure location**
- **Receptionists**
- **Residue controls - disintegrator / shredders**
- Secure file wipes
- Secure passwords
- Single sign-on
- **Environmental controls (air conditioners, humidifiers)**

Risk mitigation approaches – Technical controls ?

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure)
- Fences
- Role-based access control
- Segregation of duties
- Redundant data center
- Corporate code of conduct
- Internal audit
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Firewalls
- Change management
- Penetration testing
- Placement of authentication / authorization / database / accounting servers in secure location
- Receptionists
- Residue controls - disintegrator / shredder
- Secure file wipes
- Secure passwords
- Single sign-on
- Environmental controls (air conditioners, humidifiers)

Risk mitigation approaches – Technical controls?

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- Code of sanctions against vendors/suppliers/contractors
- Color-coded ID badges
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure)
- Fences
- Role-based access control
- Segregation of duties
- Redundant data center
- Corporate code of conduct
- Internal audit
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Network firewalls
- Change management
- Penetration testing
- Placement of authentication / authorization / database / accounting servers in secure location
- Receptionists
- Residue controls - disintegrator / shredder
- Secure file wipes
- Secure passwords (may be organizational too)
- Single sign-on
- Environmental controls (air conditioners, humidifiers)

Risk mitigation approaches – Administrative controls?

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- **Code of sanctions against vendors/suppliers/contractors**
- **Color-coded ID badges**
- Content scanners
- Electronic scanning devices
- Encoded data (cryptography; public key infrastructure, private key infrastructure)
- Fences
- **Role-based access control**
- **Segregation of duties**
- Redundant data center
- **Corporate code of conduct**
- **Internal audit**
- Grounds lighting
- Intrusion detection software
- Locked doors, terminals
- Motion-detection devices
- Firewalls
- **Change management**
- Penetration testing
- Placement of authentication / authorization / database / accounting servers in secure location
- Receptionists
- Residue controls - disintegrator / shredders
- Secure file wipes
- **Secure passwords (may be technical too)**
- Single sign-on
- Environmental controls (air conditioners, humidifiers)

Next time: Information Security Classification...

| Information Category | Description | Examples |
|---------------------------|--|--|
| Unclassified Public | Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital. | <ul style="list-style-type: none"> Product brochures widely distributed Information widely available in the public domain, including publicly available Company web site areas Sample downloads of Company software that is for sale Financial reports required by regulatory authorities Newsletters for external transmission |
| Proprietary | Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital. | <ul style="list-style-type: none"> Passwords and information on corporate security procedures Know-how used to process client information Standard Operating Procedures used in all parts of Company's business All Company-developed software code, whether used internally or sold to clients |
| Client Confidential Data | Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital. | <ul style="list-style-type: none"> Client media Electronic transmissions from clients Product information generated for the client by Company production activities as specified by the client |
| Company Confidential Data | Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital. | <ul style="list-style-type: none"> Salaries and other personnel data Accounting data and internal financial reports Confidential customer business data and confidential contracts Non disclosure agreements with clients\vendors Company business plans |

| | POTENTIAL IMPACT | | |
|---|---|---|--|
| Security Objective | LOW | MODERATE | HIGH |
| Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542] | The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542] | The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542] | The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

Test Taking Tip

- Read the answers first -

This contradicts many people's test taking recommendations...

...but, it works. Here's why:

- Quickly alerts you to the type of question to expect
- Focuses your attention in reading the question for meaningful information
- Gives you advanced warning that there may be more than one significant concepts (option to answer in the form "Both A & B")
- Gives you an opportunity to get a sense of the sort of answer the test maker is looking for
- There may be more than one valid answer, but the test maker may be looking for "best mitigation for the situation" or "least risk in the situation"

Test Taking Tip

Example:



- A. Transaction authorization
- B. Loss or duplication of EDI transmissions
- C. Transmission delay
- D. Deletion or manipulation of transactions prior to or after establishment of application controls



Test Taking Tip

Example:

Which of the following represents the GREATEST potential risk in an EDI environment?

- A. Transaction authorization
- B. Loss or duplication of EDI transmissions
- C. Transmission delay
- D. Deletion or manipulation of transactions prior to or after establishment of application controls



Test Taking Tip

Example:

Which of the following represents the GREATEST potential risk in an EDI environment?

- A. Transaction authorization
- B. Loss or duplication of EDI transmissions
- C. Transmission delay
- D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A

Moving forward...

| When | Actor | Task | Type |
|-----------------------|-----------------|------------------------------------|---------------|
| Friday | Instructor (me) | Post reading questions (Friday am) | |
| Sunday 11:59pm | Student | Post answers to reading questions | Assignment |
| Tuesday 11:59am | Student | Post 4 comments to others' answers | Participation |
| Tuesday 11:59am | Student | Post "In The News" article | Participation |
| Wednesday 9am-12:30pm | Both of Us | Class meeting | Participation |
| Thursday | Instructor | Post summary notes | |

Reading questions for Week 3

- What are the 3 types of risk mitigating controls? Which is the most important? Why is it the most important?
- How you would apply the FIPS security categorizations to decide if each of the information security risk mitigations ("safeguards") described in the FGDC guidelines is needed?
- Which two information security objectives could be put at risk if the alternative mitigations (i.e. "safeguards") recommended by the FGDC guidelines are applied? Explain how each could be put at risk.

Protecting Information Assets

- Week 2 -

Understanding an Organization's Risk Environment