MIS 5206
Protection of Information Assets
Unit #0b

Understanding an Organization's Risk Environment

Readings

- Vacca Chapter 1 “Information Security in the Modern Enterprise”
- Vacca Chapter 2 ” Building a Secure Organization”
- NIST Reading 1: “Framework for Improving Critical Infrastructure Cybersecurity”
- ISACA Risk IT Framework, pp. 1-42 1a

Agenda

- Business context for data and information security
- Key concepts
  - Confidentiality, Integrity, Availability
  - Threats
  - Vulnerabilities
  - Risks
  - Risk mitigations
- Critical infrastructure
- Risk management standards and frameworks
- Next class

The value of business' data is at a peak

"A generation ago the asset base of US public companies was more than 80% tangible property" (e.g. raw materials, real estate, railroad cars…)

"Today… intangibles… account for more than 80% of listed company value"

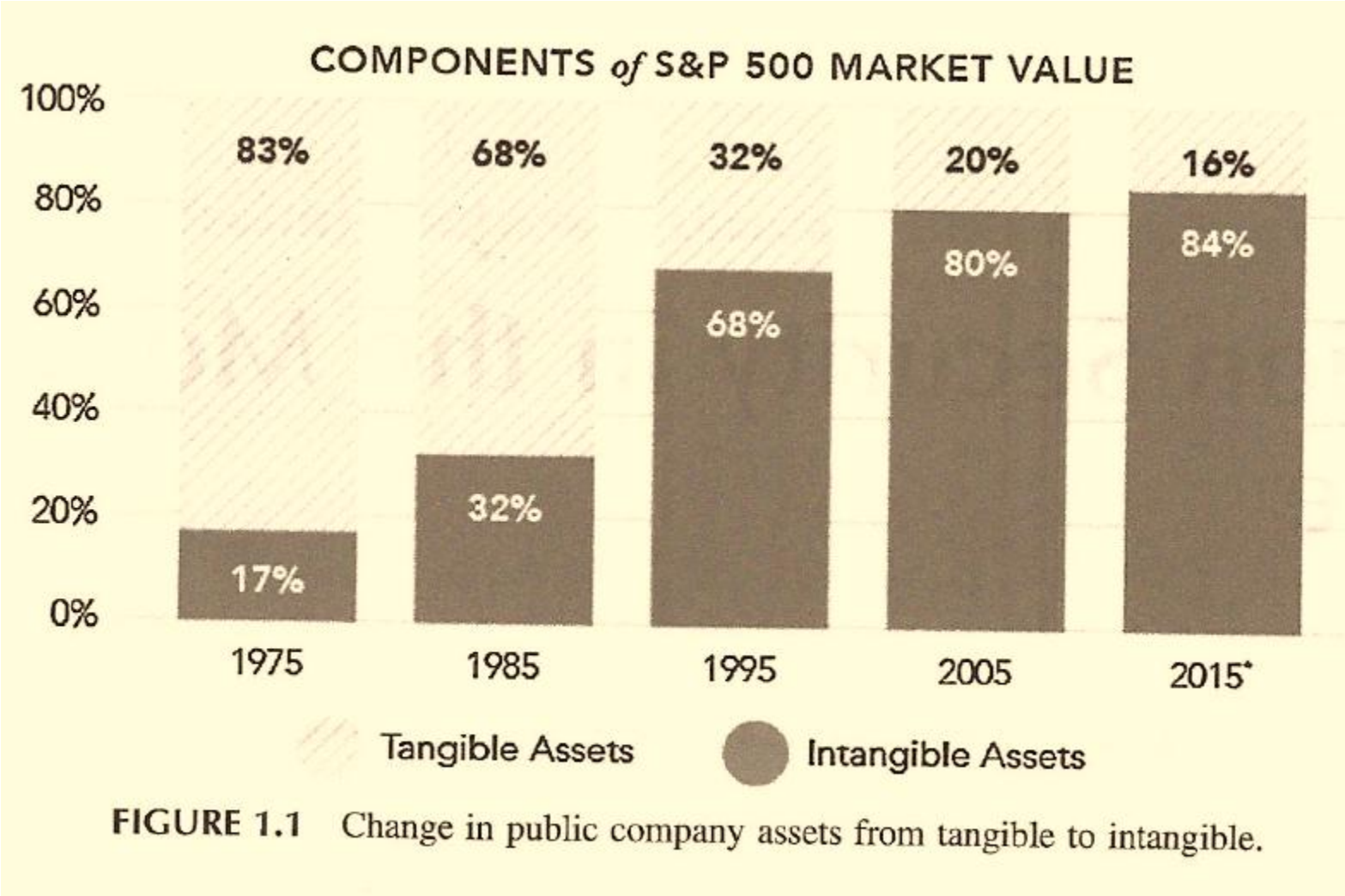


FIGURE 1.1 Change in public company assets from tangible to intangible.

Vacca 3rd Edition, pp. 3-4

Information Security Transformation

1970 data security examples

- Guarding the photocopier
- Watching who went in and out of the front door

Today's data security must consider

- Devices able to grab gigabytes of data and move them anywhere in the world in an instant
- Laptops, tablets and smartphones with direct connection to company data are endpoints in a global network, creating thousands to millions of "front doors" leaving industry at its most vulnerable

One thing has not changed over the years…

Human beings remain the primary vector for loss of corporate value

AND

Humans also control the processes and technologies central to information security function that preserves corporate value

PAUSE – Next Video

Key concepts

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 a cyber 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

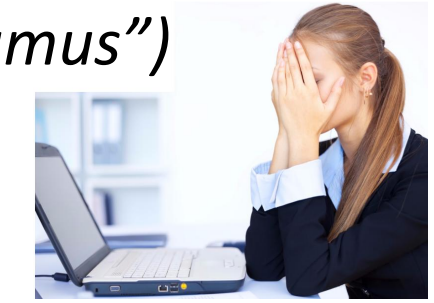
Administrative

What is a threat…

Threats to information and information systems include:

- Purposeful attacks *(“Human malicious”)*

- Human errors *(“Human ignoramus”)*



- Structural Failures

- Environmental disruptions

Taxonomy of threat sources

1. Adversarial
2. Accidental
3. Structural
4. Environmental

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

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	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).	Capability, Intent, Targeting

ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - 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

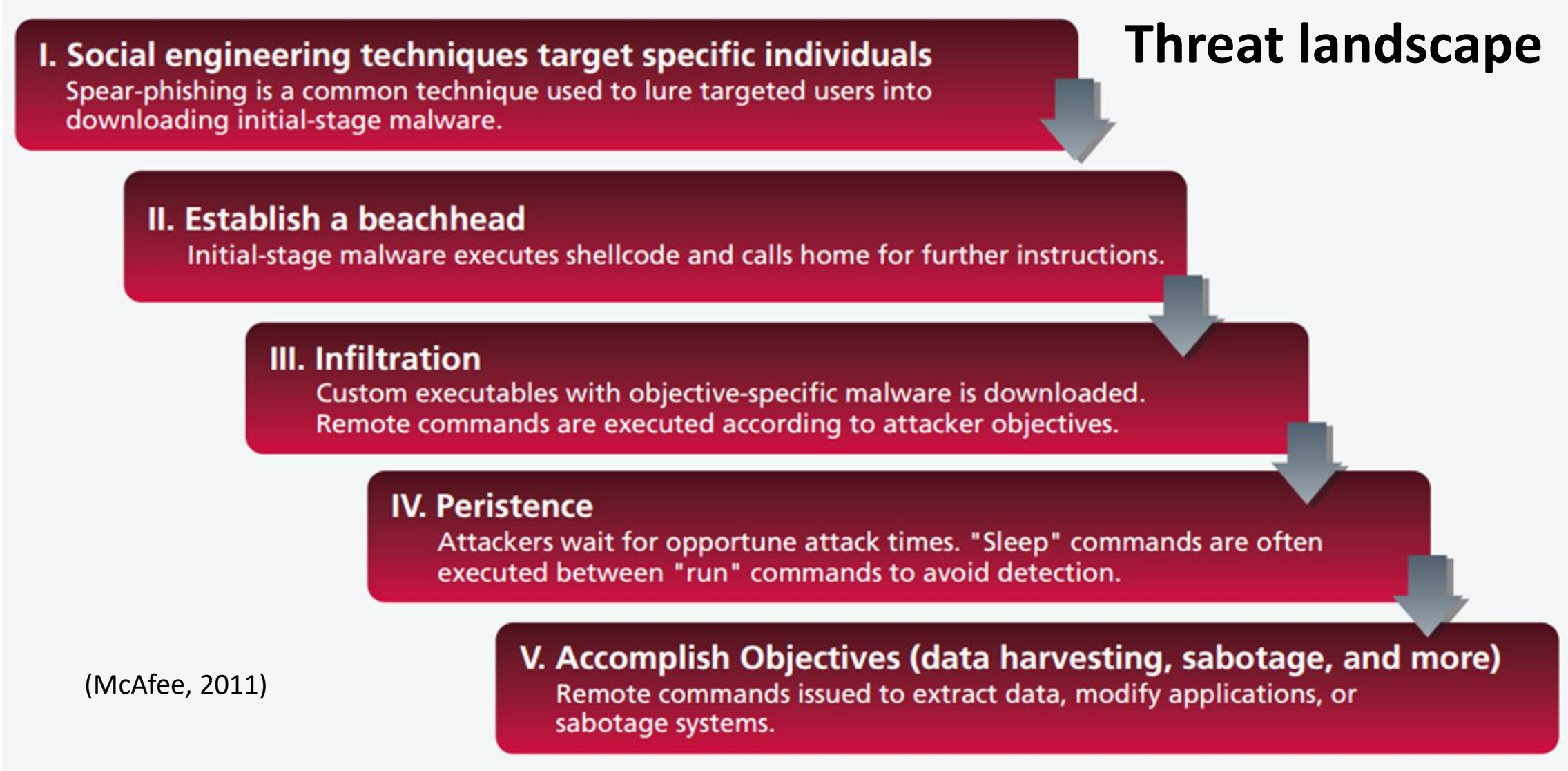
ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	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).
		Range of effects

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	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).	Capability, Intent, Targeting

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

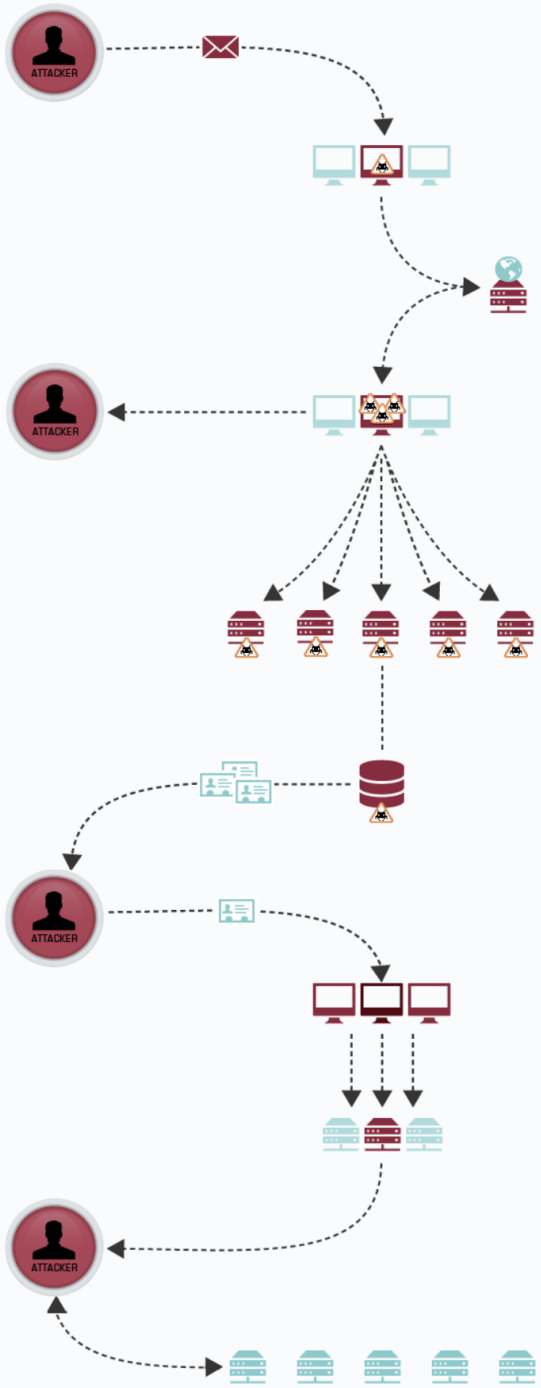
Anatomy of an Attack



(McAfee, 2011)

Anatomy of an Attack

(MANDIANT, 2015)



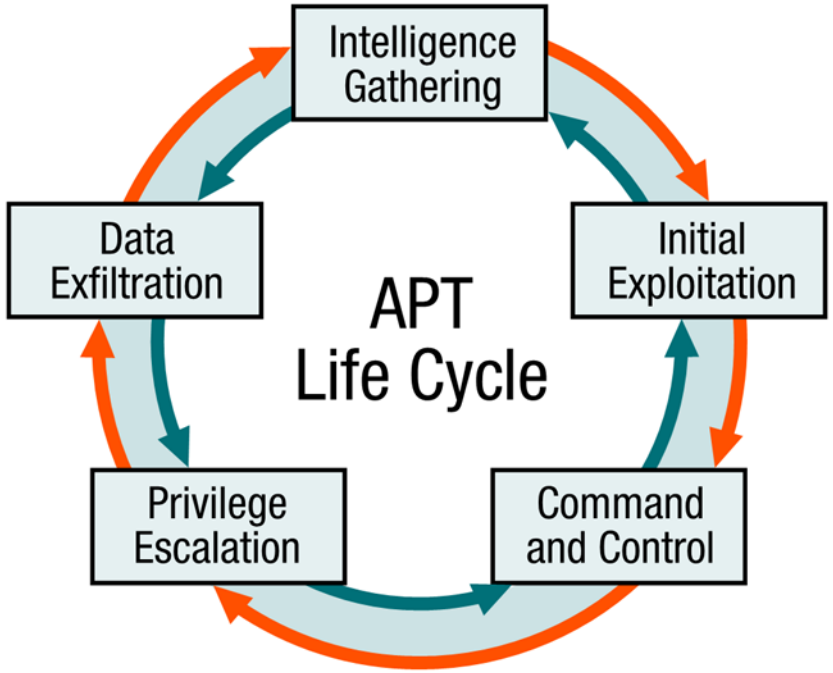
1. Attacker sends spear fishing e-mail
2. Victim opens attachment
   - Custom malware is installed
3. Custom malware communicates to control web site
   - Pulls down additional malware
4. Attacker establishes multiple backdoors
5. Attacker accesses system
   - Dumps account names and passwords from domain 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 tracts
    - Deletes files
    - Can return any time

Assets

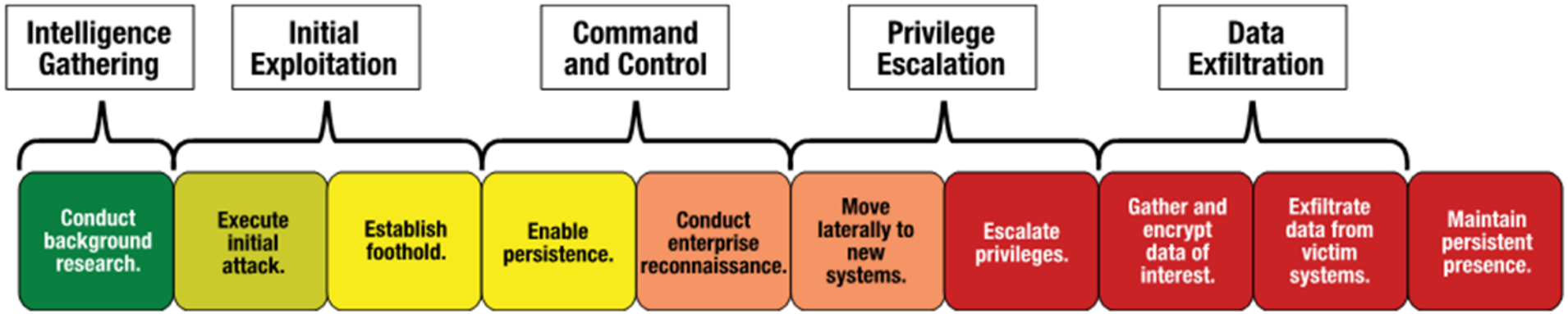
Threat landscape

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

Threat landscape



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]

PAUSE – Next Video

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 and causes

- Computer operator errors
- Data entry (input) errors
- Update of wrong file
- Physical damage to disk
- Misplaced disk files
- Unlocked trash containers
- Trusting malicious people

Taxonomy of cybersecurity threat sources

Type of Threat Source	Description	Characteristics

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - 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

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

Structural Threat Examples

- Air conditioning failure
- Building collapse
- Water and sewer pipe breaks
- Failure of computer hardware
- Failure of fire alarms or smoke detectors
- Gas line explosions
- Power outages (brownouts, blackouts, transients, spikes, sags and power surges)
- …

Taxonomy of cybersecurity threat sources

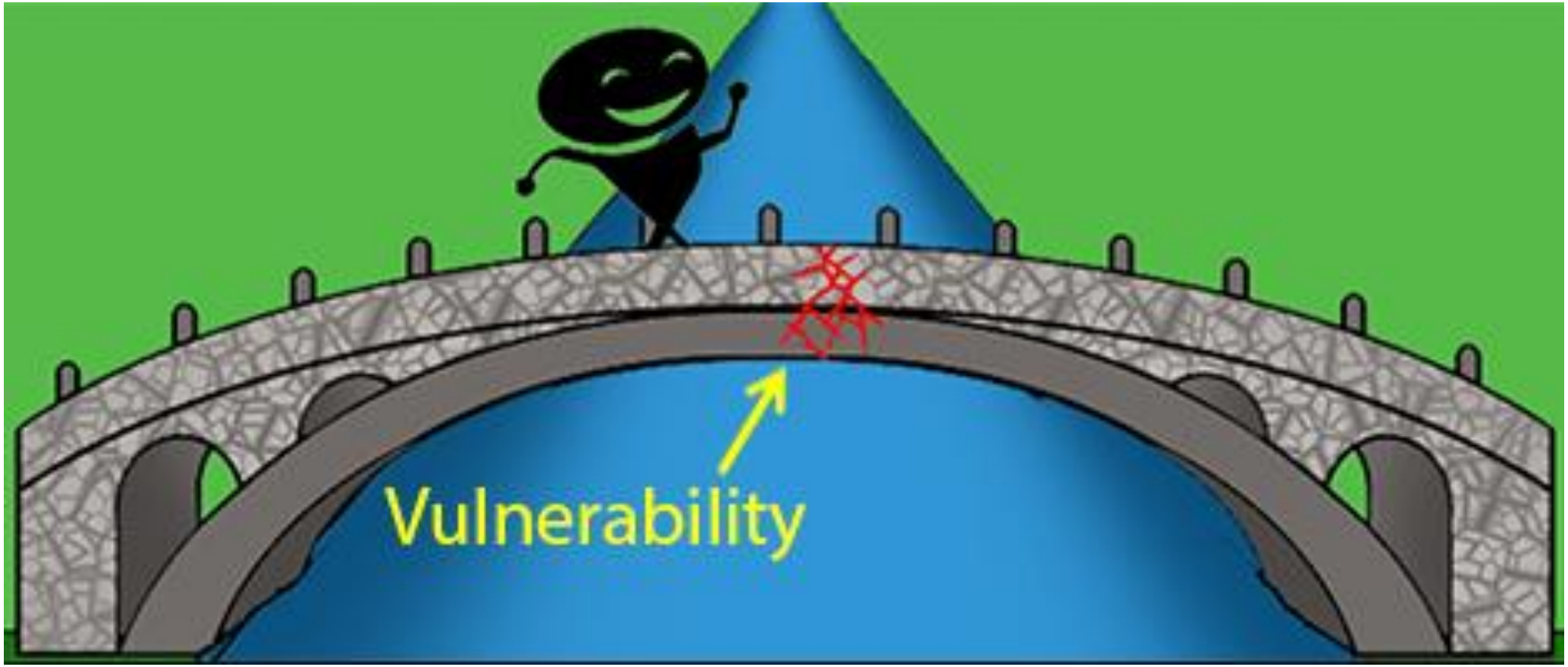
Type of Threat Source	Description	Characteristics

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	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).
		Range of effects

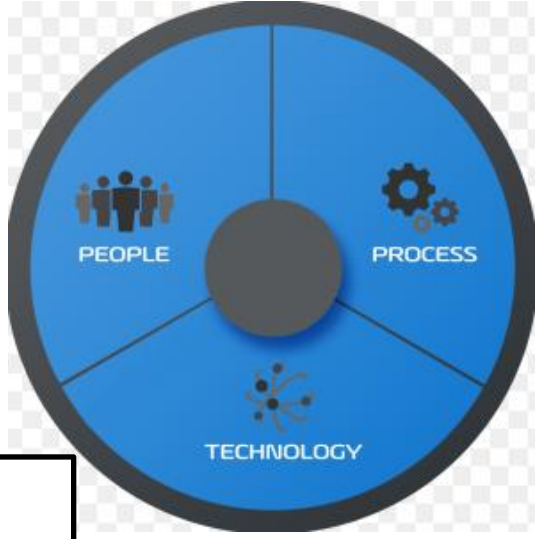
NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66

PAUSE – Next Video

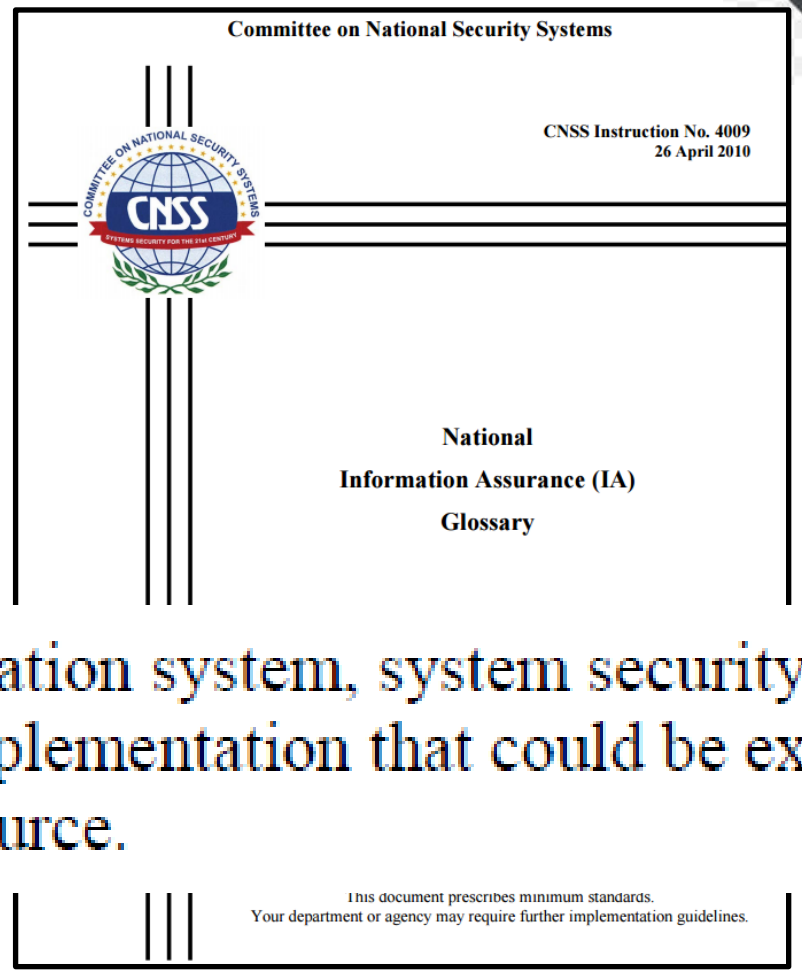
What is a Vulnerability?



What is a Vulnerability?



Any unaddressed susceptibility to a Adversarial, Accidental, Structural or Environmental threat is an information security vulnerability


Committee on National Security Systems

CNSS Instruction No. 4009
26 April 2010

National
Information Assurance (IA)
Glossary

This document prescribes minimum standards.
Your department or agency may require further implementation guidelines.

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

Vulnerabilities

Inadequacies in any of these areas:

Risk Assessment
Planning
System and Services Acquisition
Certification, Accreditation, and Security Assessments
Personnel Security
Physical and Environmental Protection
Contingency Planning
Configuration Management
Maintenance
System and Information Integrity
Media Protection
Incident Response
Awareness and Training
Identification and Authentication
Access Control
Audit and Accountability
System and Communications Protection

PAUSE – Next Video

What is a Risk?

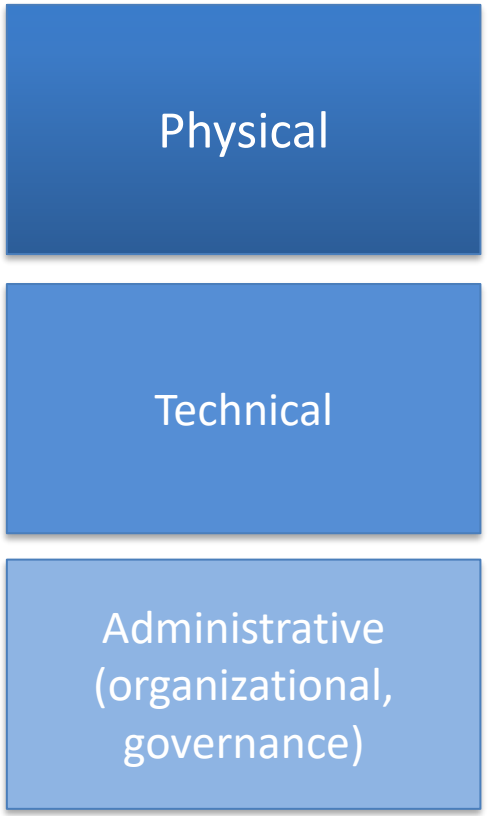
A measure of the potential impact of a threat resulting from an exploitation of a vulnerability

Potential loss resulting from unauthorized:

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

…of an enterprises' information

Can be expresses in quantitative and qualitative terms



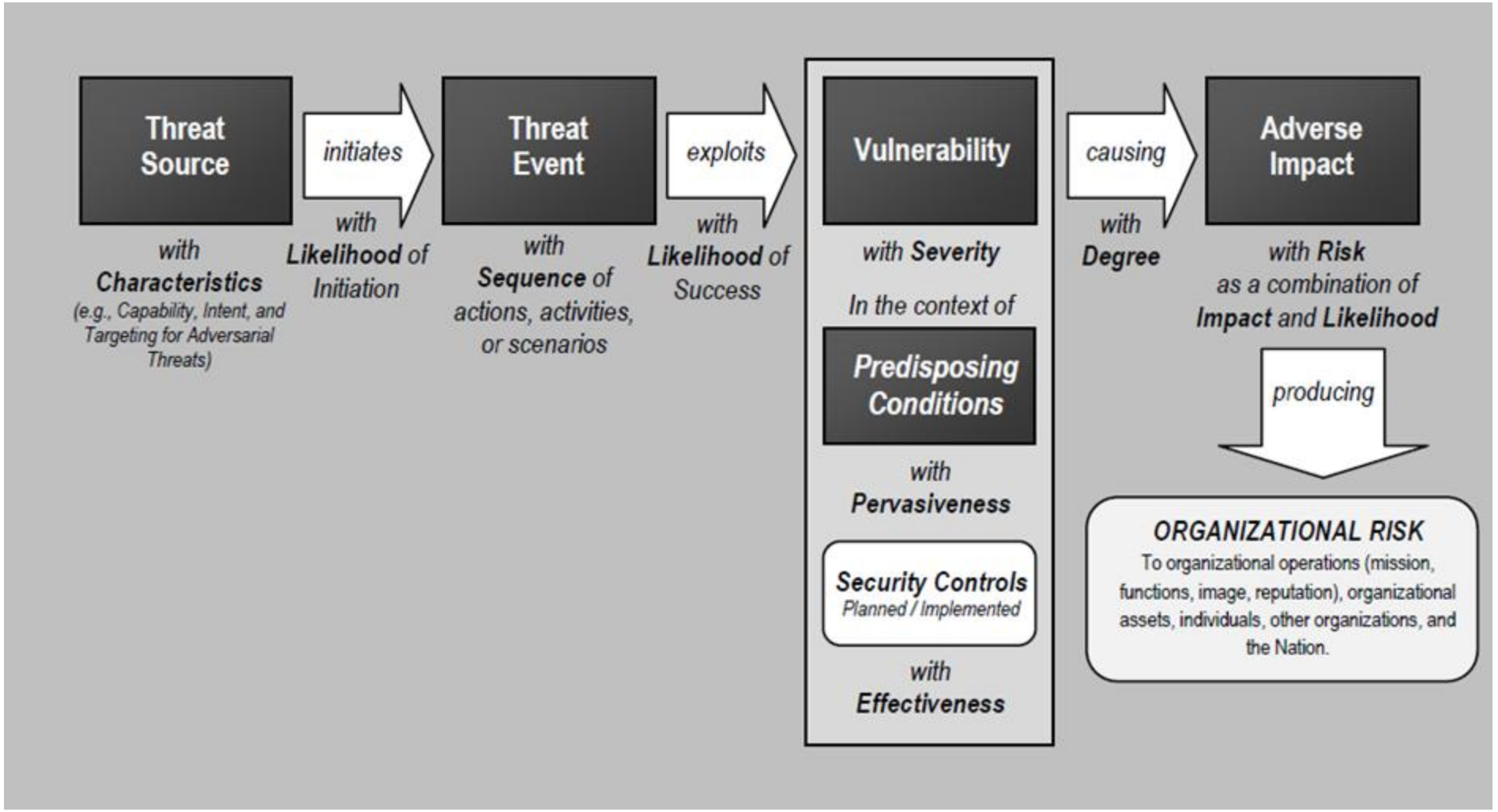
Information security risks

- Economic impact and financial loss
  - Replacement costs (software, hardware, other)
  - Backup restoration and recovery costs
  - Reprocessing, reconstruction costs
  - Theft/crime (non-computer, computer)

- Loss of life
- 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

Example of an IT risk model

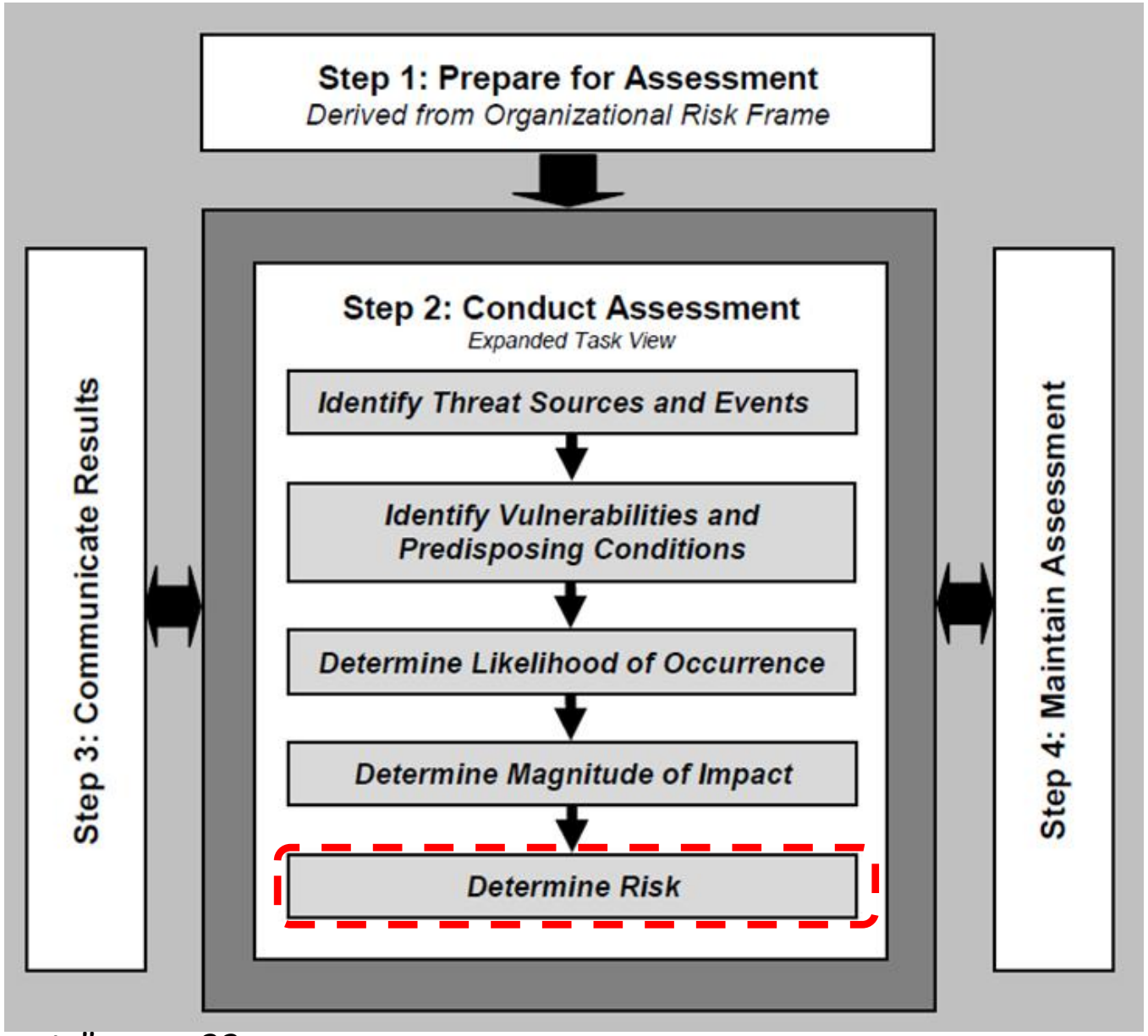


NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 21

Risk analysis with an IT risk model

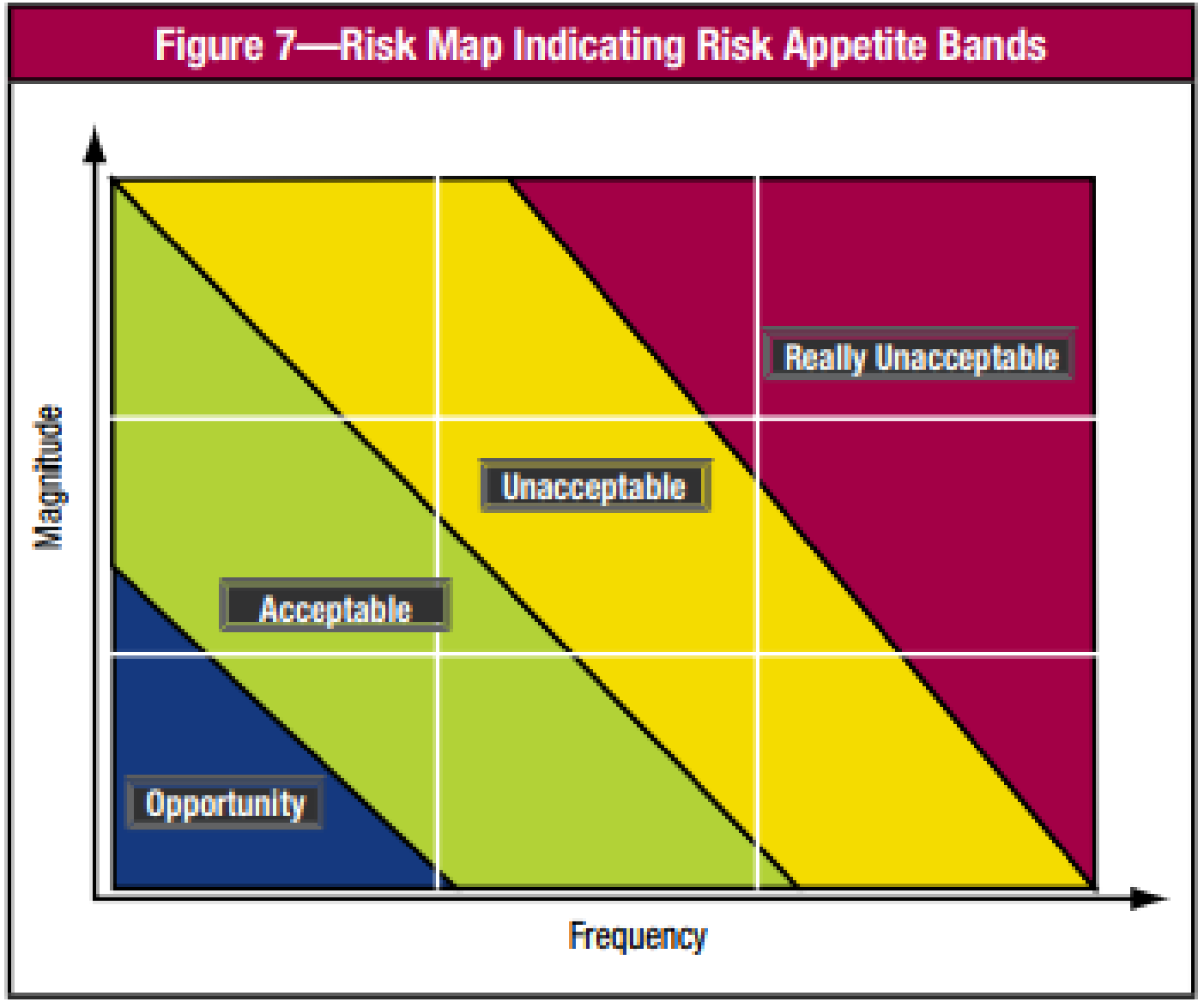
Type	Threat Agent	Can exploit this vulnerability	Resulting in this impact
Physical	Fire	Lack of fire extinguishers	Facility and computer damage, and possible loss of life
Physical	Intruder	Lack of security guard	Broken windows and stolen computers and devices
Technical	Contractor	Lax access control mechanisms	Stolen trade secrets
Technical	Malware	Lack of antivirus software	Virus infection…
Technical	Hacker	Unprotected services running on a server	Unauthorized access to confidential information
Administrative	Employee	Lack of training	Unauthorized distribution of sensitive information
Administrative	Employee	Lack of auditing	Uncontrolled invalid modifications to decision support data

Process for Assessing IT risk



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

How to determine if risk is acceptable?



Quantitative risk assessment – 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 migh 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 t 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)**

Note: This calculation assumes total loss of an asset. If an asset retains part of its useful value, the SLE should be adjusted by an appropriate amount.

PAUSE – Next Video

Risk Management Techniques

Once threats and risks are identified, each risk can be managed by:

1. Avoidance
2. Acceptance
3. Transfer
4. Mitigation (“Controls”)

Risk mitigations – Which are 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 mitigations – 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 mitigations – 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)

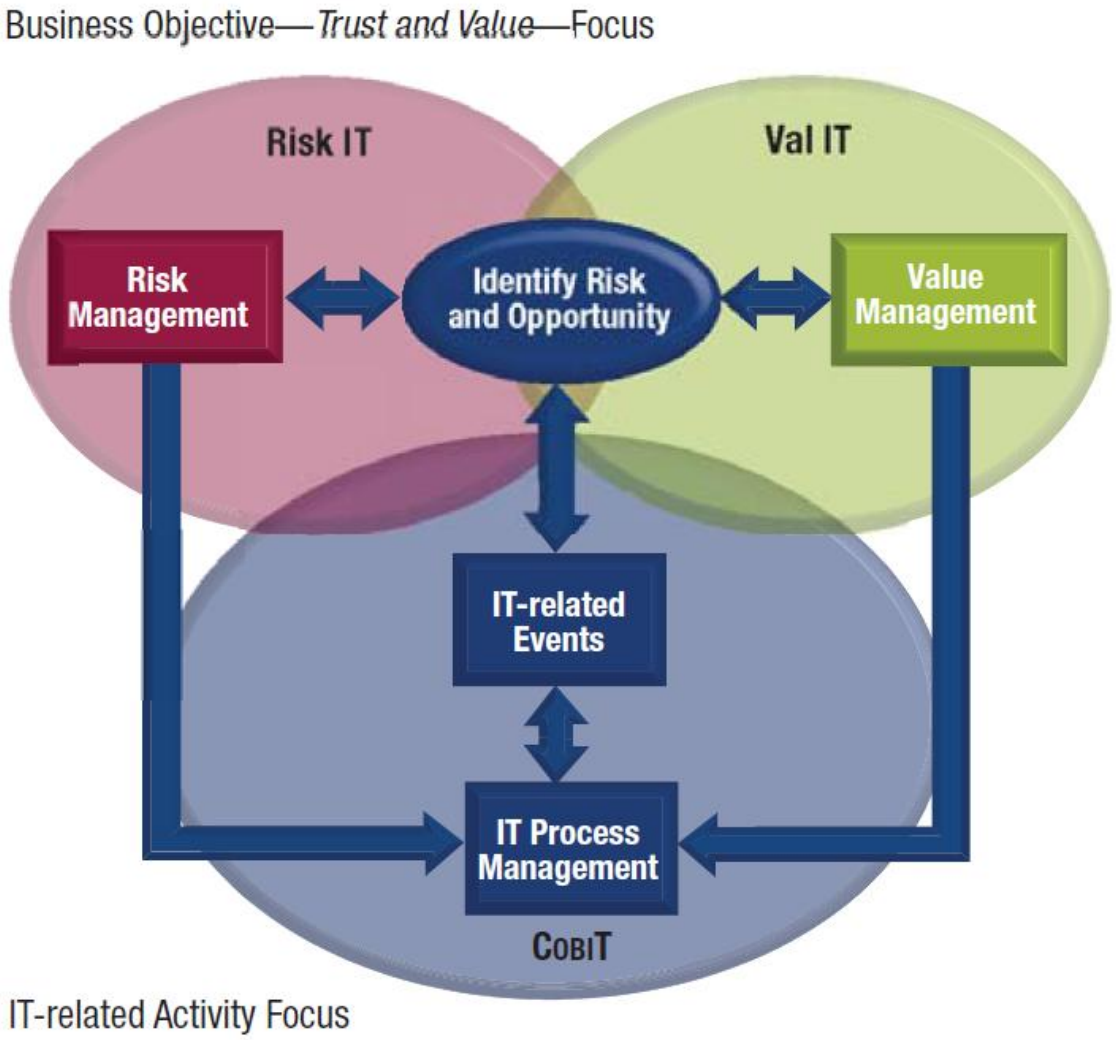
Risk mitigations –Administrative controls

- 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)

PAUSE – Next Video

ISACA's RiskIT Framework



- ISACA's Risk IT Framework is useful to guide an organization's approach to trading IT Risk for IT value
- Also guides implementing IT governance in enterprises adopting COBIT as their IT governance framework for risk management and control
- COBIT

  Control **OB**jectives for **I**nformation and related **T**echnologies

  - IT governance framework and supporting toolset enabling managers to bridge the gap between business risks, risk control requirements, and technical issues

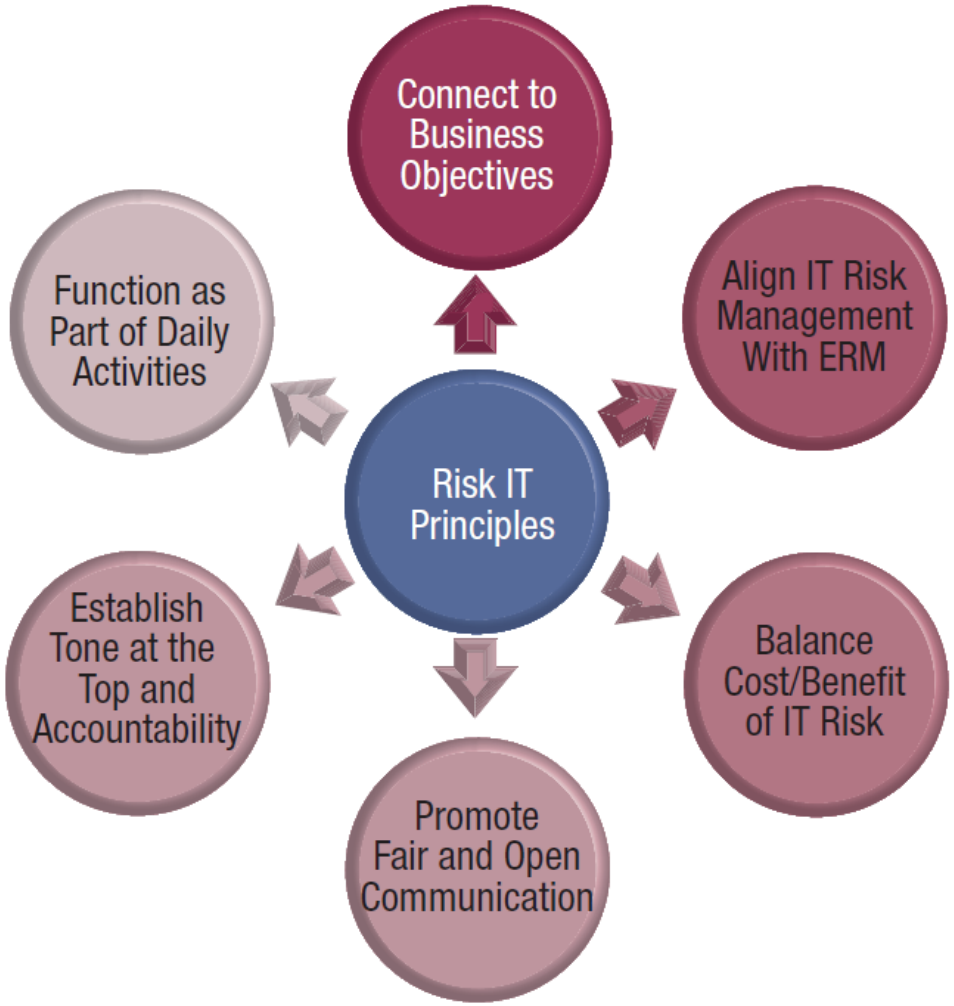
The RiskIT Framework

Groups key activities into three domains

Provides guidance on:

- Key activities within each process,
- Responsibilities for the process, information flows between processes
- Performance management of the process

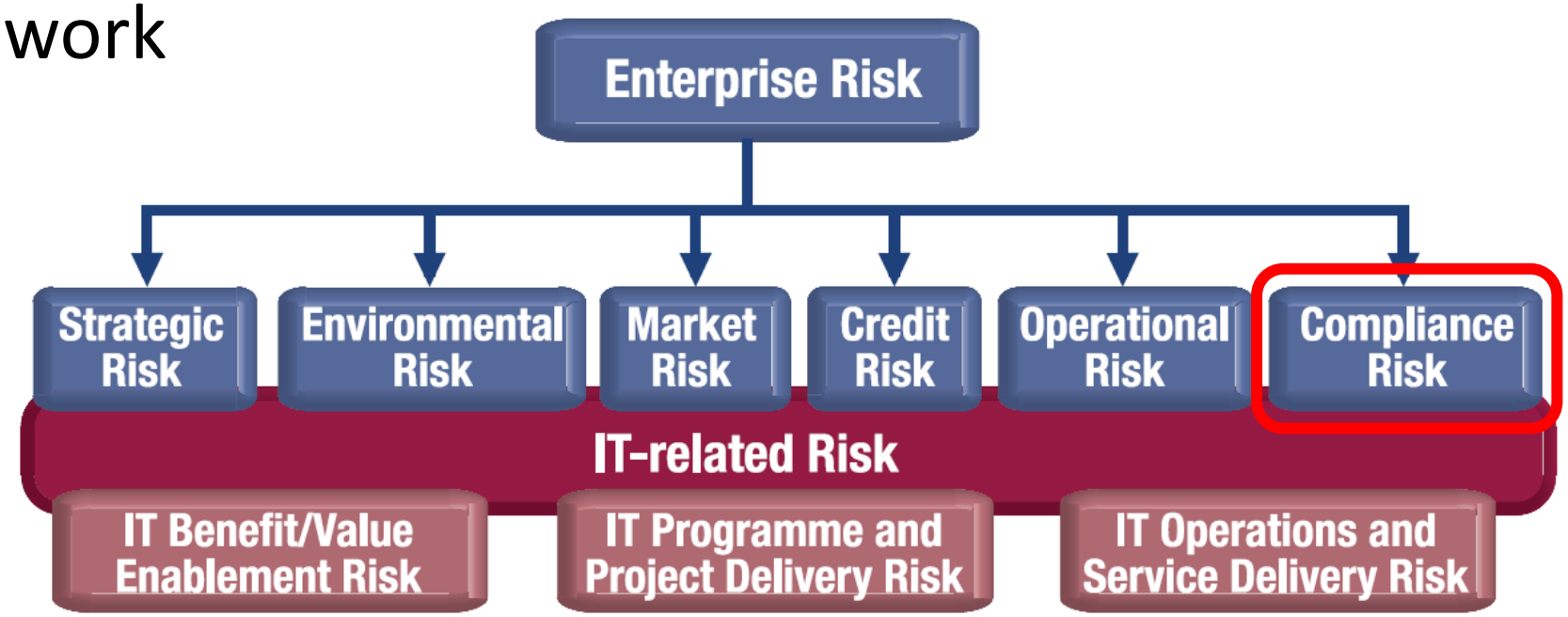
The RiskIT Framework



The Risk IT framework is about trading off IT value with IT risk—in other words… business risk related to the use of IT

- The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk

The RiskIT Framework



IT risk is business risk

- Associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise
- Consists of IT-related events and conditions that could potentially impact the business
  - *Can occur with both uncertain frequency and magnitude*
  - *Create challenges in meeting strategic goals and objectives*

PAUSE – Next Video

Critical Infrastructure

Certain infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of a country

- *Telecommunications*
- *Electrical power systems*
- *Gas and oil storage and transport*
- *Banking and finance*
- *Transportation*
- *Water supply systems*
- *Emergency services*
- *Continuity of government*

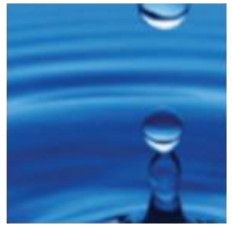
Critical Infrastructure Information –data that can be used in either physical or computer-based attack that directly or indirectly

- Affects viability of a facility or critical infrastructure
- Threatens public health or safety
- Harms commerce
- Violates governmental laws

Protected System –any physical or computer-based system, information or data, process or procedure that directly or indirectly affects the viability of a facility or critical infrastructure

Critical Infrastructure Sectors

Transportation 

Water and Wastewater Systems 

Dams 

Emergency Services 

Commercial Facilities 

Nuclear Reactors, Materials, and Waste 

Defense Industrial Base 

Communications 

Energy 

Chemical 

Government Facilities 

Critical Manufacturing 

Healthcare and Public Health 

Information Technology 

Food and Agriculture 

Financial Services 

Transportation sector - example

- ☒ Regulatory
- ☒ Financial (save or earn $)
- ☒ Political
- ☐ Environmental / Social benefit
- ☒ Reputation
- ☒ Technological need
- ☐ Other _____

Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!

John A. Volpe National Transportation Systems Center

U.S. Department of Transportation
Research and Innovative Technology Administration

Frequent Hacks Into Highway Dynamic Message Signs

John A. Volpe National Transportation Systems Center

U.S. Department of Transportation
Research and Innovative Technology Administration

Transportation sector - example

- ☒ Regulatory
- ☒ Financial (save or earn $)
- ☒ Political
- ☐ Environmental / Social benefit
- ☒ Reputation
- ☒ Technological need
- ☐ Other _____

Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!

John A. Volpe National Transportation Systems Center

U.S. Department of Transportation
Research and Innovative Technology Administration

Even "Isolated" Legacy Systems Are Vulnerable

14 Year Old Boy Derails Polish Trams, January 2008

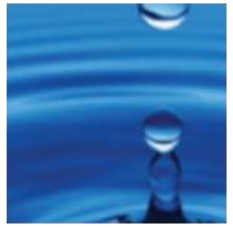
- 4 light rail trains derailed, 12 people hurt
- Used modified television remote controller
- Locks disabling switch when vehicle present not installed

John A. Volpe National Transportation Systems Center

U.S. Department of Transportation
Research and Innovative Technology Administration

Critical Infrastructure Sectors

Transportation 

Water and Wastewater Systems 

Dams 

Emergency Services 

Commercial Facilities 

Nuclear Reactors, Materials, and Waste 

Defense Industrial Base 

Communications 

Energy 

Chemical 

Government Facilities 

Critical Manufacturing 

Healthcare and Public Health 

Information Technology 

Food and Agriculture 

Financial Services 

Water/Wastewater sector – Attack example

Vitek Boden worked for Hunter Watertech, an Australian firm that installed SCADA radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia (a rural area of great natural beauty and a tourist destination)

- **Applied for a job with the Maroochy Shire Council**
- **Walked away from a "strained relationship" with Hunter Watertech**
- **The Council decided not to hire him**
- **Boden decided to get even with both the Council and his former employer**

- ***Maroochy Shire Council had no existing information security policies, procedures, nor cyber security defenses***
- **On at least 46 occasions Boden issued radio commands to the sewage equipment**
  - **Caused 800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel**
  - **Marine life died, the creek water turned black, the stench was unbearable for residents**

PAUSE – Next Video

ISO/IEC 27001 Standard

Considered a leading example of risk management for information security

- Created in 2005 and updated in 2013 by agreement between
  - International Organization for Standardization (ISO)
  - International Electro-technical Commission (IEC)
- Specific requirements for security management systems and controls
- Firms can apply to be audited and certified as ISO/IEC 27001 compliant

Federal Information Security Management Act (FISMA) of 2002

Federal Information Security Modernization Act (FISMA) of 2014

Recognize importance of information security to the economy and national security

- **Require each government agency to provide information security**
  - **For information and information systems supporting their operations and assets**
    - *Including those provided or managed by another agency, contractors, or other source*

Other short titles	Confidential Information Protection and Statistical Efficiency Act of 2002
Long title	An Act to strengthen Federal Government information security, including through the requirement for the development of mandatory information security risk management standards.
Acronyms (colloquial)	FISMA
Nicknames	E-Government Act of 2002

https://www.dhs.gov/fisma

FISMA - Federal Information Security Management Act defines

"Information security" as protection of…

- Confidentiality, integrity, and availability ("CIA") of data and information
- Data, information and information systems from unauthorized…
  - Access, use, disclosure = **Confidentiality**
  - Modification = **Integrity**
  - Disruption or destruction = **Availability**

What is NIST?

National Institute of Standards and Technology
U.S. Department of Commerce

- Non-regulatory agency of the United States Department of Commerce
- Measurement standards laboratory

Mission: *Promote innovation and industrial competitiveness*

- NIST's activities organized as laboratory programs:
  - Nanoscale Science and Technology, Engineering, Neutron Research, Material Measurement, Physical Measurement…
  - **Information Technology**

NIST is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets (excluding national security systems)

NIST National Institute of Standards and Technology
Information Technology Laboratory

SEARCH CSRC: GO

CONTACT SITE MAP

Computer Security Division
Computer Security Resource Center

CSRC Home | About | Projects / Research | Publications | News & Events

- FISMA
- Detailed Overview
- Risk Management Framework (RMF)
  - RMF Steps - FAQs, Roles & Responsibilities, Guides
- Applying the RMF to Federal Information Systems Course
- Security Categorization
- Security Controls
- Security Assessment
- Authorization and Monitoring
- Security Configuration Settings
- Industrial Control System Security
- Compliance
- Resources
- News
- Events
- Schedule
- FAQs - FISMA Project

CSRC HOME > GROUPS > SMA > FISMA

RISK MANAGEMENT FRAMEWORK (RMF) OVERVIEW

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the ***management of organizational risk***---that is, the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system---the security controls necessary to protect individuals and the operations and assets of the organization.

Risk-Based Approach

The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. The following activities related to managing organizational risk (also known as the ***Risk Management Framework***) are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the system development life cycle and the Federal Enterprise Architecture:

Step 1: Categorize

Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis (1).

Step 2: Select

Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions (2).

Step 3: Implement

Implement the security controls and document how the controls are deployed within the information system and environment of operation.

PAUSE – Next Video

NIST Special Publication 800-39

Managing Information Security Risk

Organization, Mission, and Information System View

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

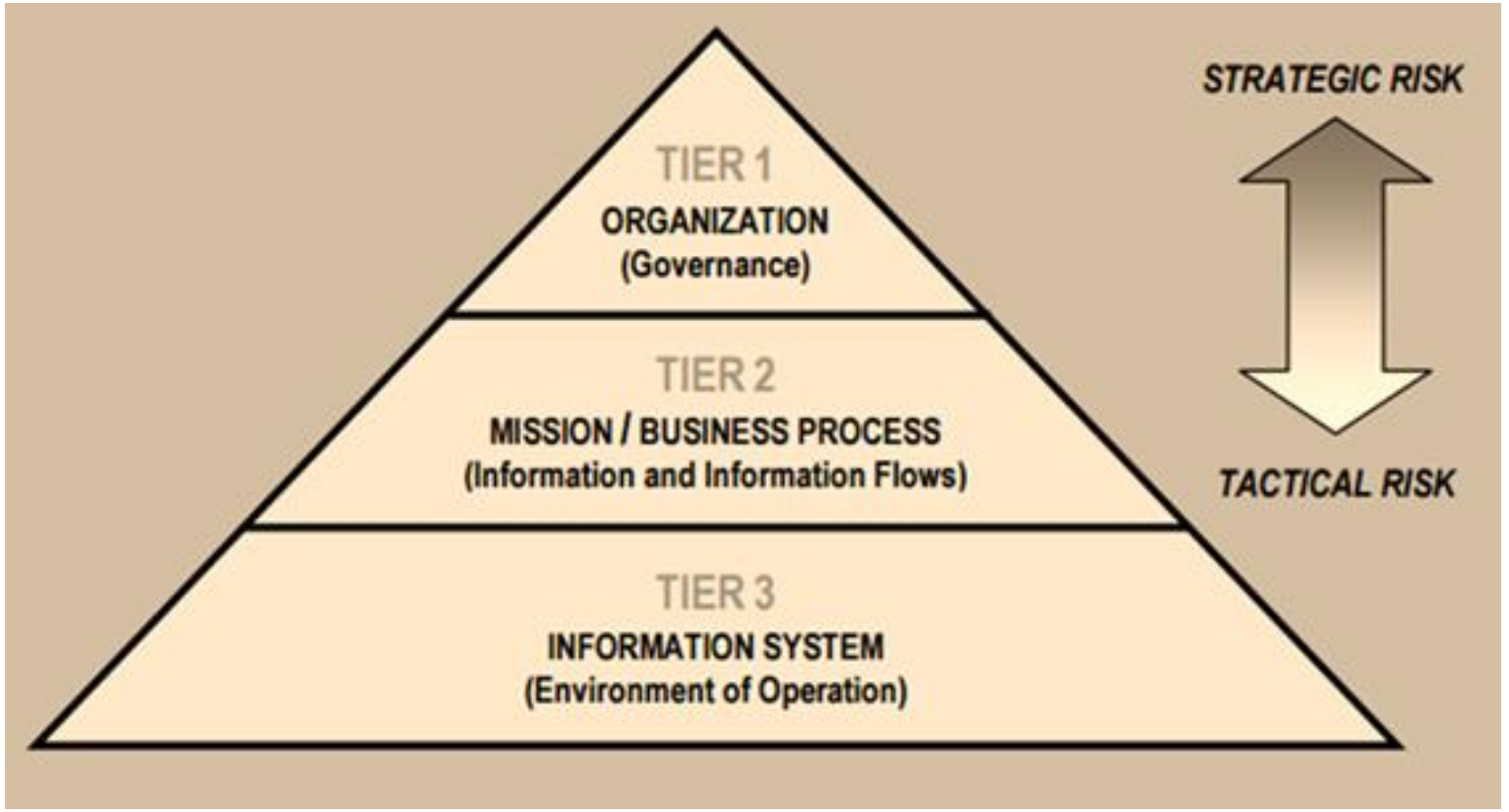
INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

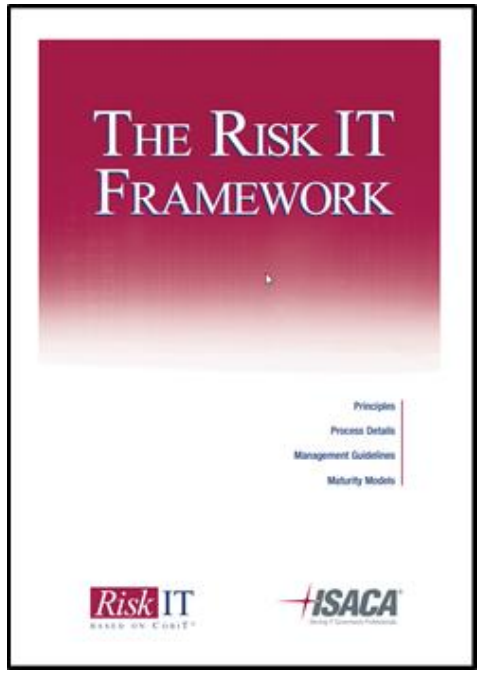
March 2011

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

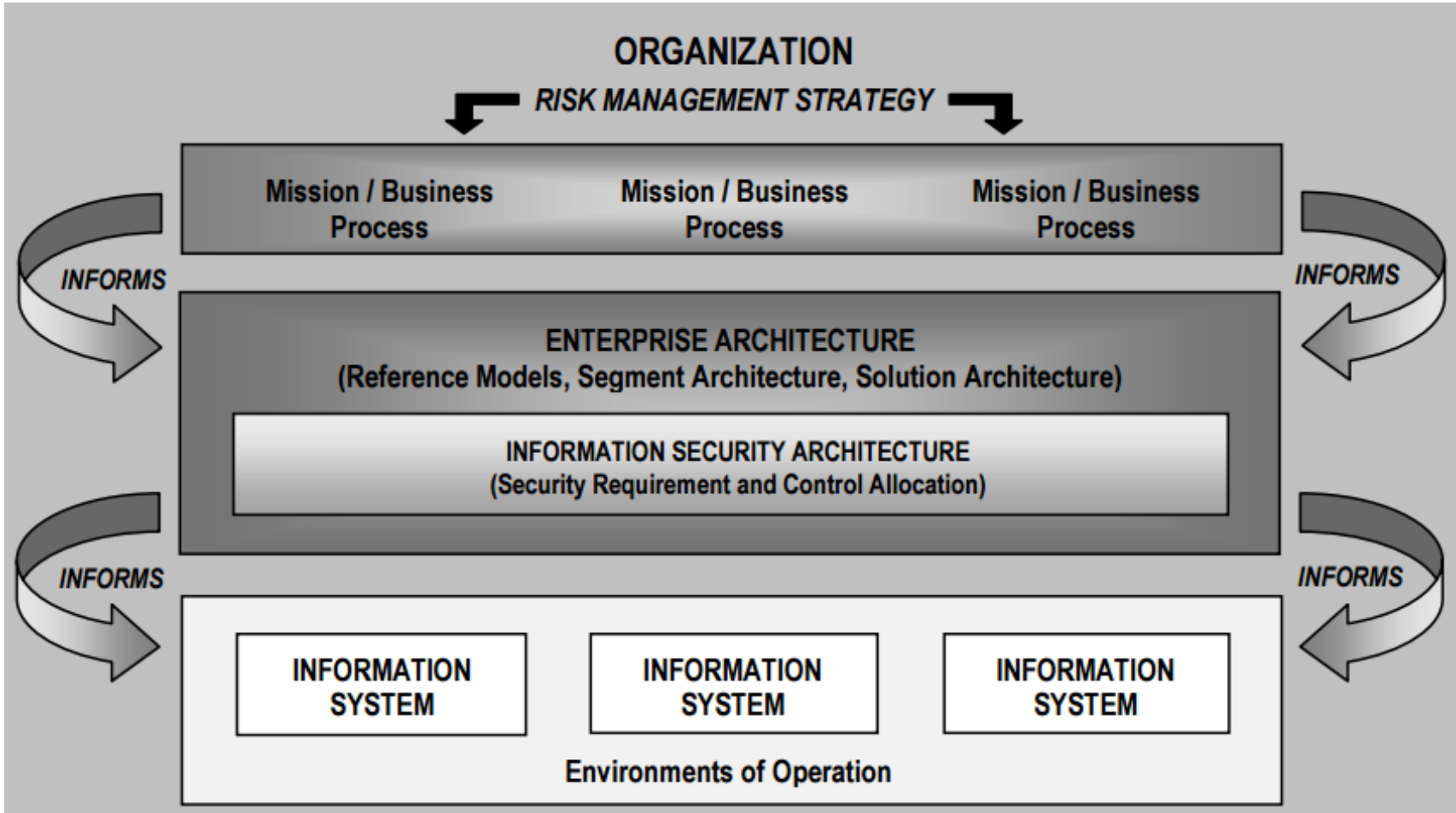


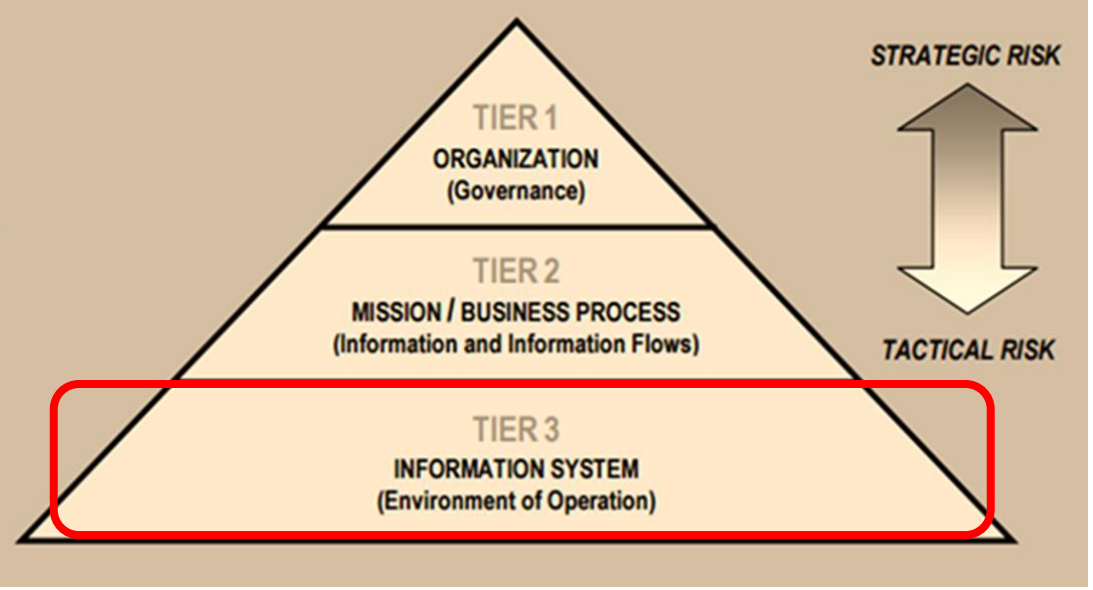

TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)

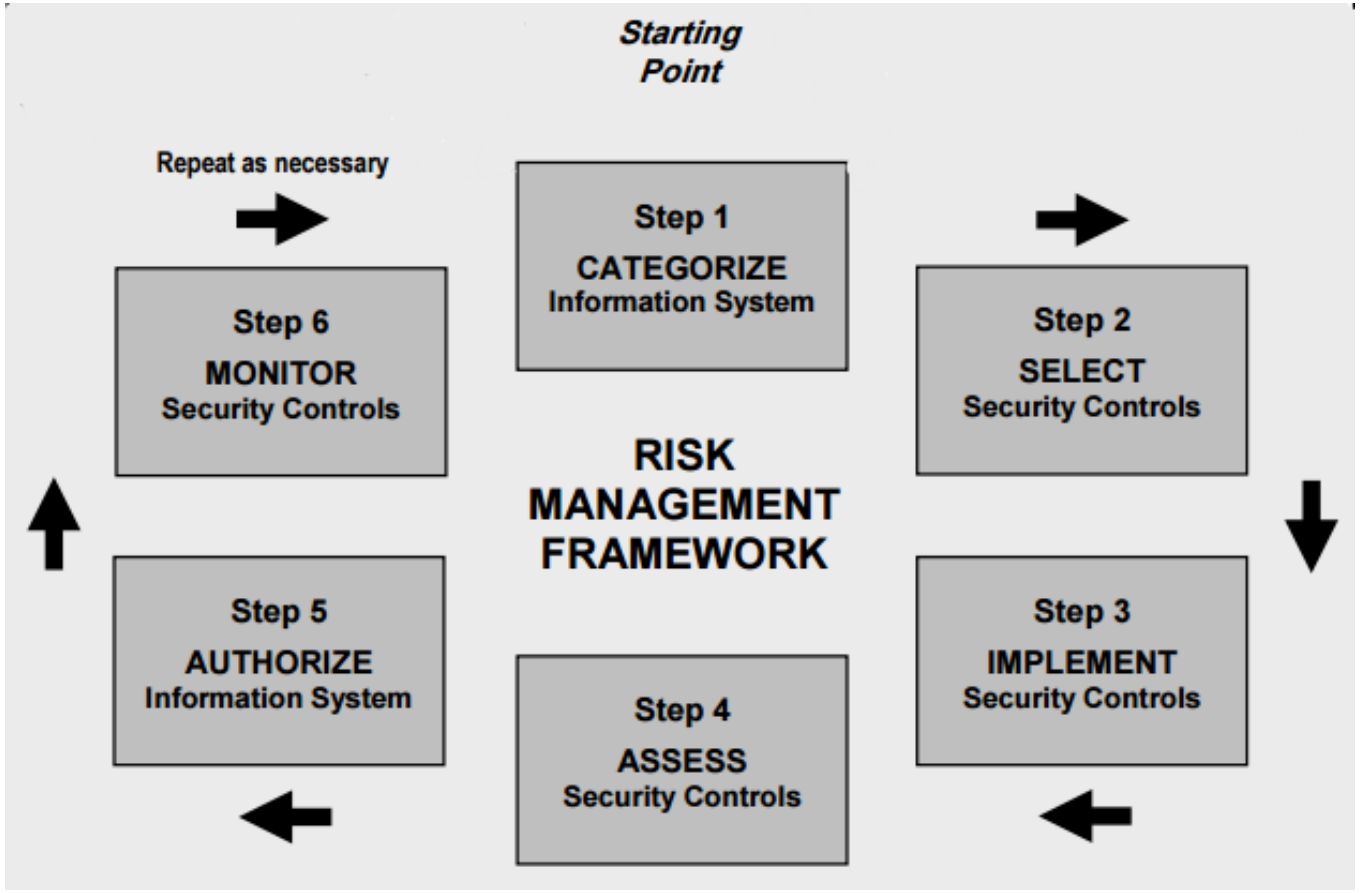

THE RISK IT FRAMEWORK
Principles
Process Details
Management Guidelines
Maturity Models
Risk IT
ISACA


Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
Integrate With ERM
Establish and Maintain a Common Risk View
Make Risk-aware Business Decisions
Business Objectives
Communication
Manage Risk
Articulate Risk
React to Events
Risk Response
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Analyse Risk
Collect Data
Maintain Risk Profile
Risk Evaluation
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.


TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)


ORGANIZATION
RISK MANAGEMENT STRATEGY
Mission / Business Process
Mission / Business Process
Mission / Business Process
INFORMS
INFORMS
ENTERPRISE ARCHITECTURE
(Reference Models, Segment Architecture, Solution Architecture)
INFORMATION SECURITY ARCHITECTURE
(Security Requirement and Control Allocation)
INFORMS
INFORMS
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
Environments of Operation


STRATEGIC RISK
TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
TACTICAL RISK
TIER 3
INFORMATION SYSTEM
(Environment of Operation)


Starting Point
Repeat as necessary
Step 1
CATEGORIZE
Information System
Step 2
SELECT
Security Controls
Step 3
IMPLEMENT
Security Controls
Step 4
ASSESS
Security Controls
Step 5
AUTHORIZE
Information System
Step 6
MONITOR
Security Controls
RISK MANAGEMENT FRAMEWORK

NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Framework for Improving Critical Infrastructure Cybersecurity

Draft Version 1.1

National Institute of Standards and Technology

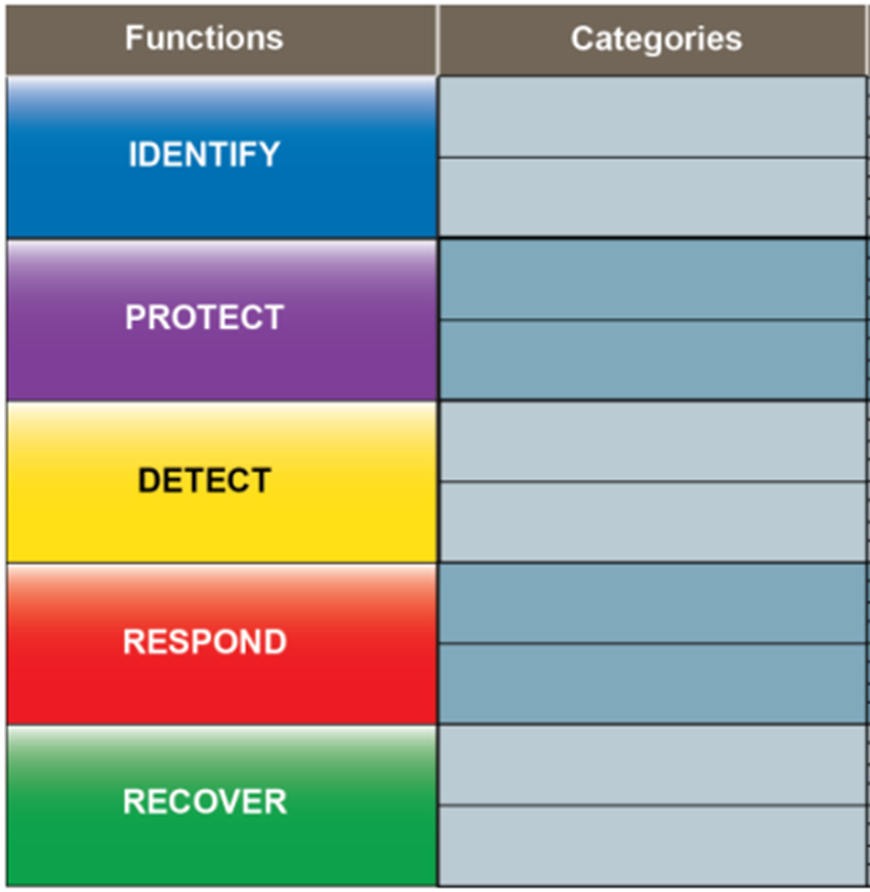
January 10, 2017

Refers to and builds on many principles of the ISO/IEC 27001 standard (and others)

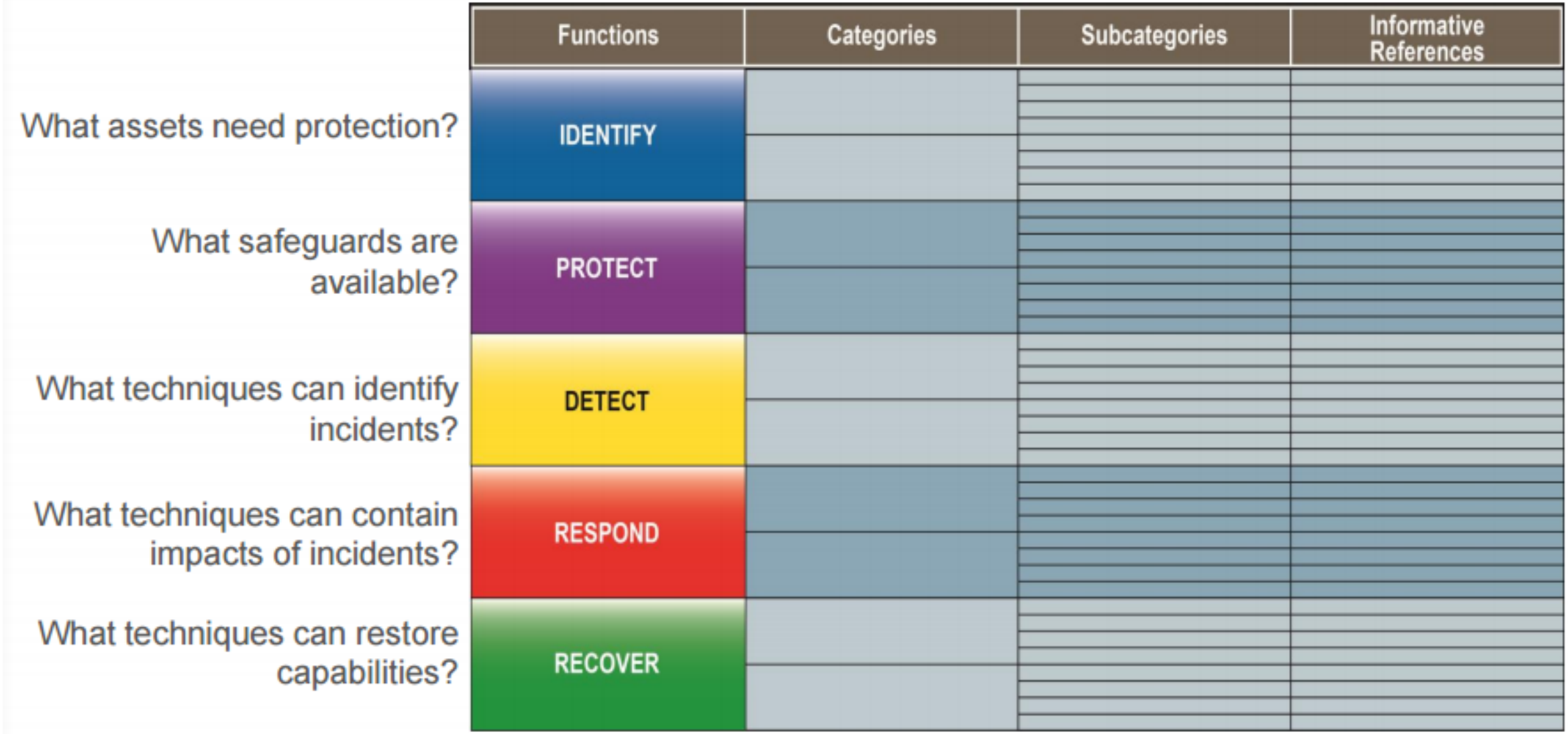
Goes way beyond IT and physical security environment

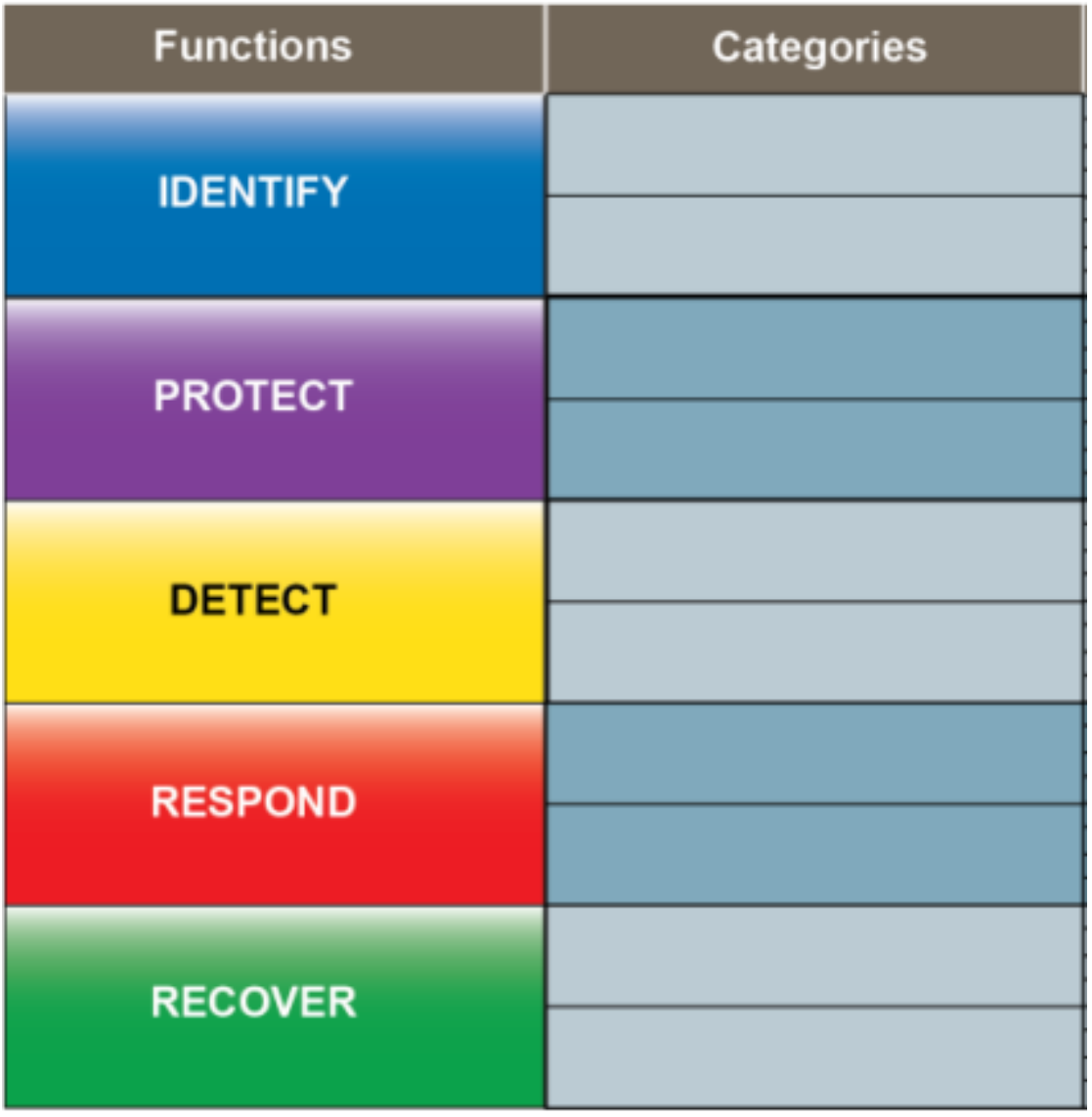
…by also including:

- Governance and management
- Staff policies and procedures
- Training
- Supply chain management



NIST Cybersecurity Framework's Core Functions



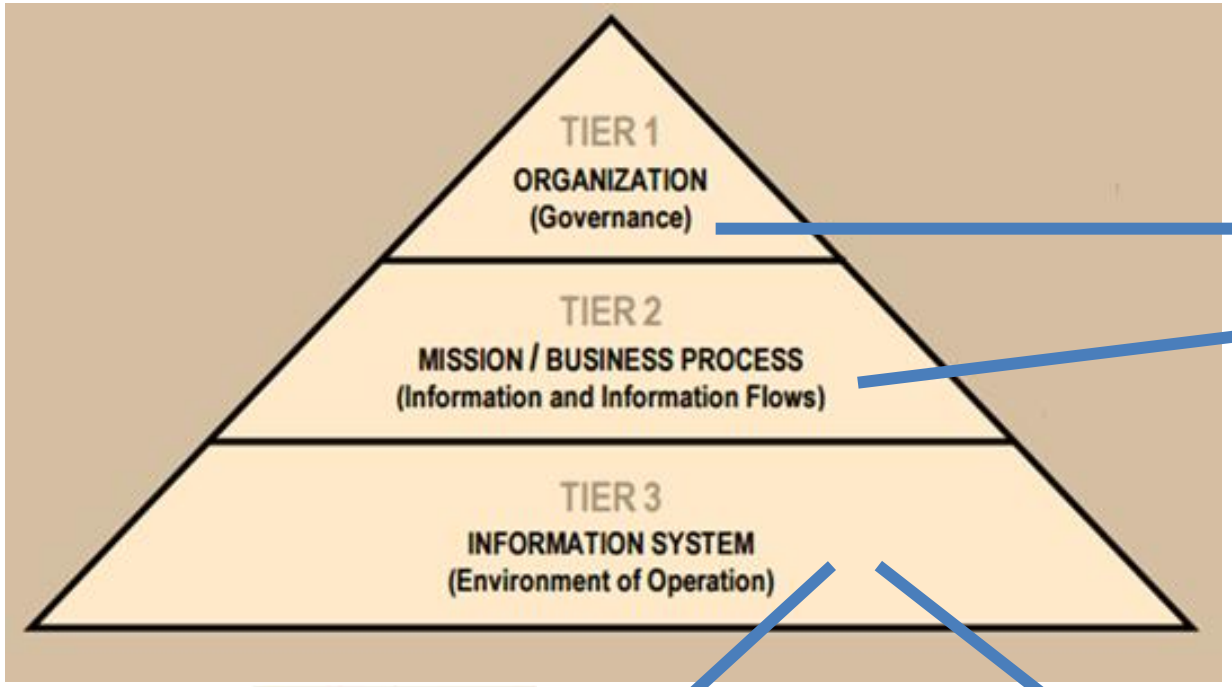


Function	Category Unique Identifier	Category
Identify	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
Protect	PR.AC	Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and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

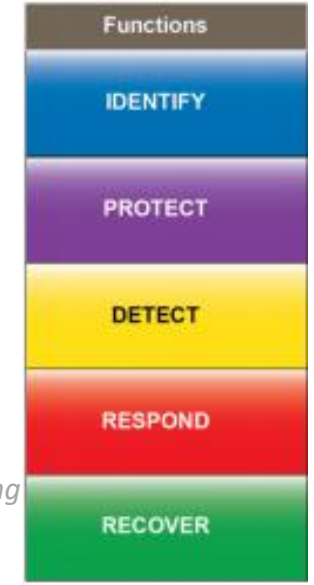
Cybersecurity Framework's Capability Maturity Tiers

	Risk Management Process	Integrated Risk Management Program	External Participation
Partial	• Not formalized • Reactive	• Limited awareness • Irregular risk management • Private information	No external collaboration
Risk Informed	• Approved practices • Not widely use as policy	• More awareness • Risk-informed, processes & procedures • Adequate resources • Internal sharing	Not formalized to interact & share information
Repeatable	• Approved as Policy • Update regularly	• Organization approach • Risk-informed, processes & procedures defined & implemented as intended, and reviewed • Knowledge & skills	• Collaborate • Receive information
Adaptive	Continuous improvement	• Risk-informed, processes & procedures for potential events • Continuous awareness • Actively	Actively shares information

In summary…

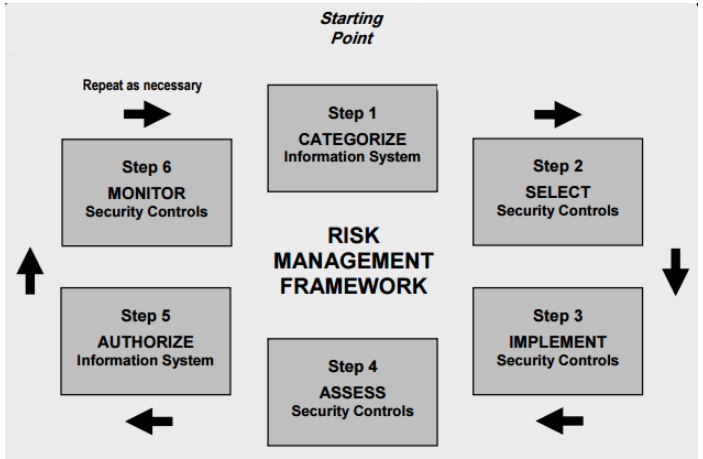


The RiskIT Framework



NIST Critical Infrastructure Cyber Security Framework

NIST Risk Management Framework



Next time: Information Security Classification…

How do you analyze risk when the need for InfoSec is measured in terms of life-safety and not financial risk measures ?

	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.

Agenda

- ✓ Business context for data and information security
- ✓ Key concepts
  - ✓ Confidentiality, Integrity, Availability
  - ✓ Threats
  - ✓ Vulnerabilities
  - ✓ Risks
  - ✓ Risk mitigations
- ✓ Critical infrastructure
- ✓ Risk management standards and frameworks
- ✓ Next class

MIS 5206
Protection of Information Assets
Unit #0b

Understanding an Organization's Risk Environment