MIS 5206
Protection of Information Assets
Unit/Class #1b

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: “Cybersecurity Framework”
- ISACA Risk IT Framework, pp. 9-30

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”

Vacca 3rd Edition, pp. 3-4

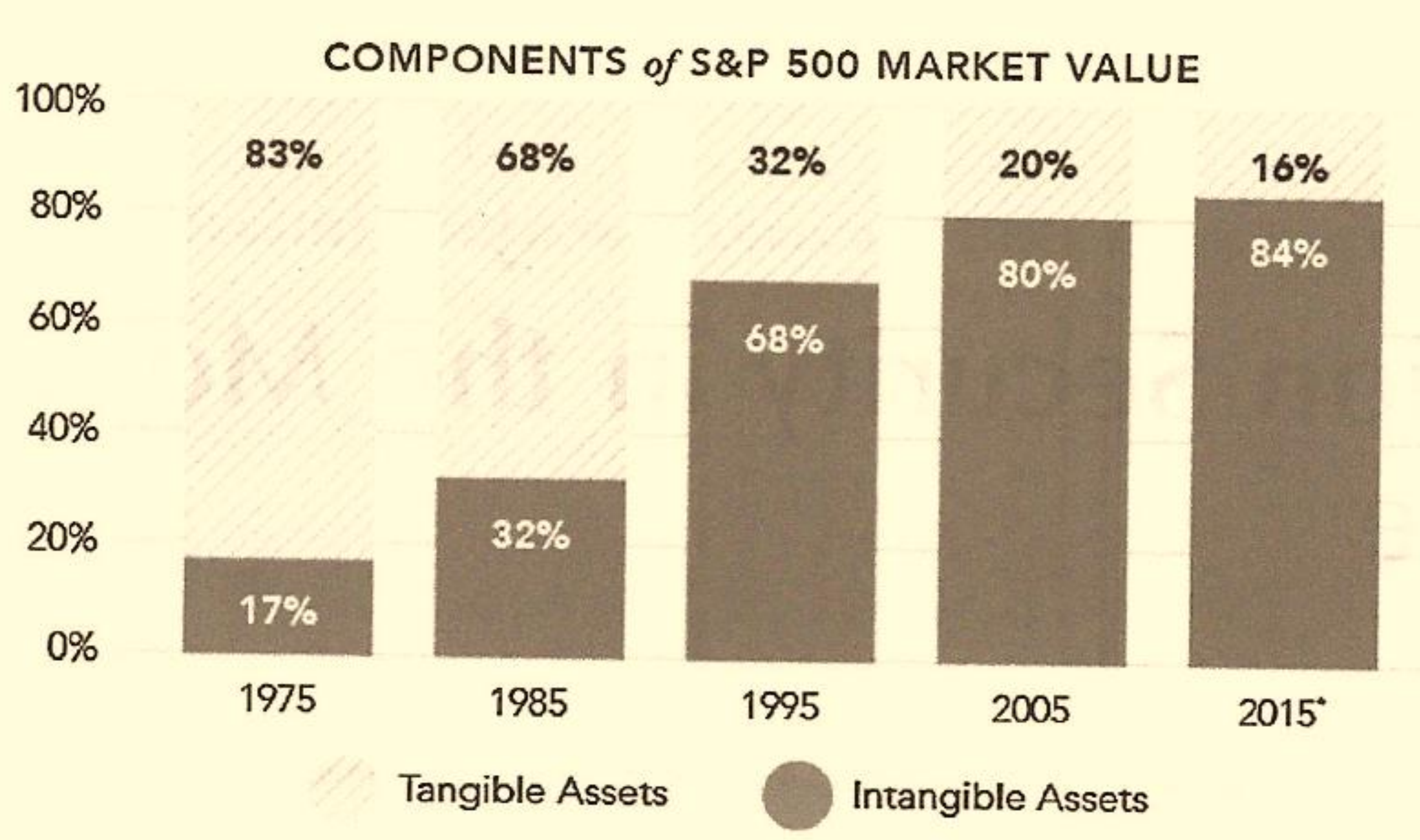


FIGURE 1.1 Change in public company assets from tangible to intangible.

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

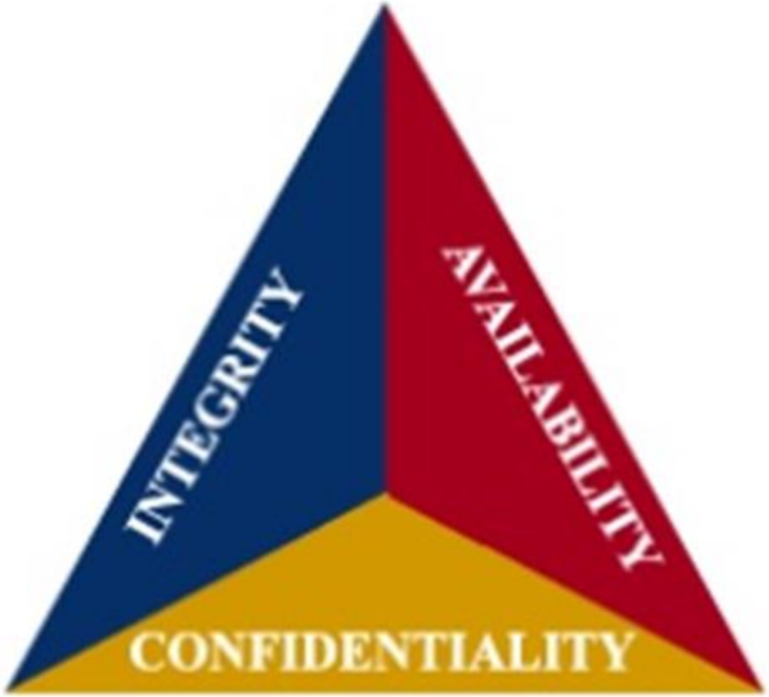
What about information security has not changed over the years?

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



Key concepts

Information security means protecting information and information systems from:

- *Unauthorized access, use, disclosure*
  Confidentiality breaches
- *Unauthorized modification or destruction*
  Integrity breaches
- *Disruption of timely and reliable access to and use of information*
  Availability breaches

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***
- ***Unauthorized modification or destruction***
- ***Disruption of timely reliable access & use of information***

…of an enterprises’ information and information systems

Physical

Technical

Administrative

What is a threat…

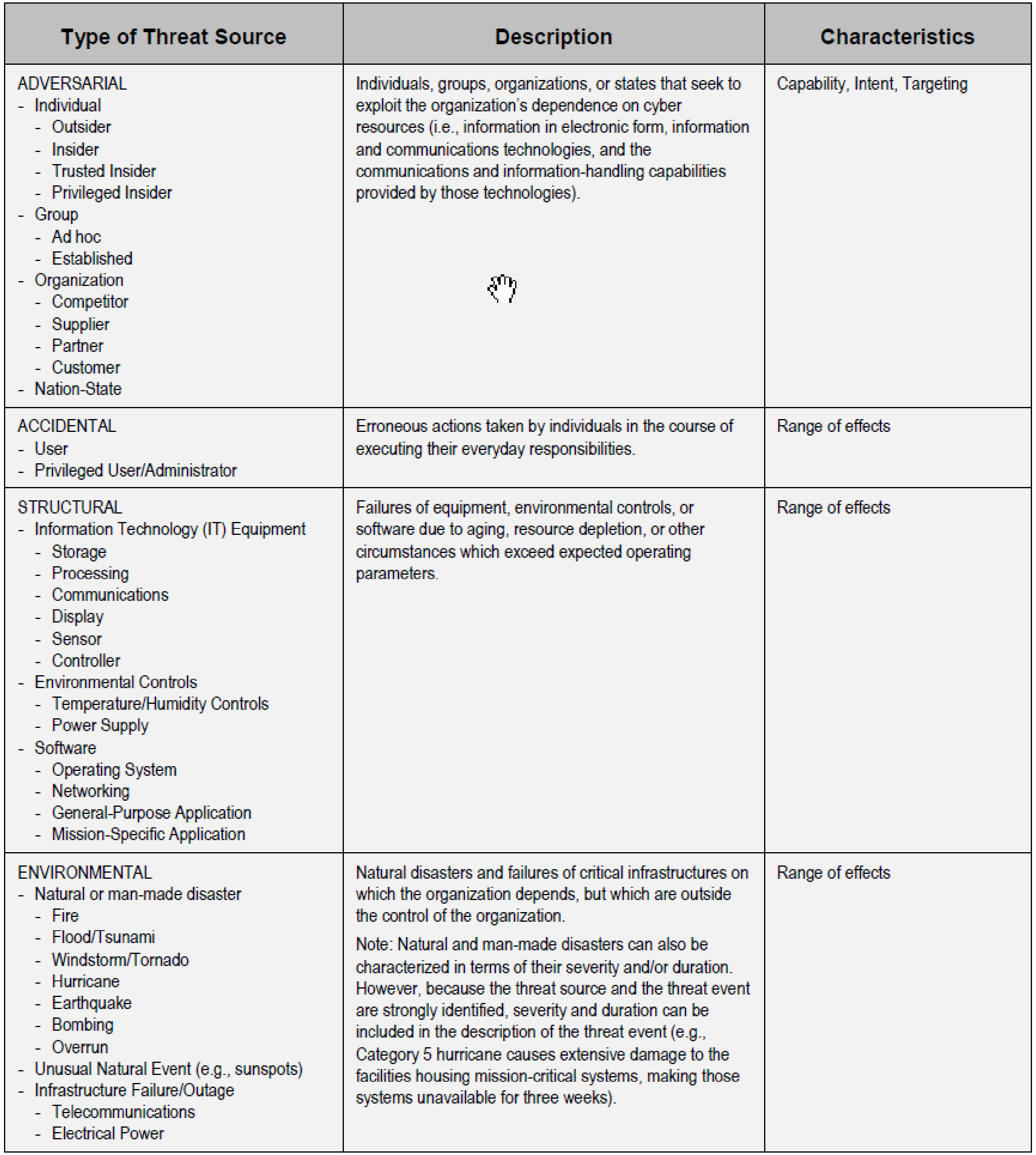
Threats to information and information systems include:

- Purposeful attacks *("Human malicious")*
- Human errors *("Human ignoramus")*
- Structural Failures
- Environmental disruptions

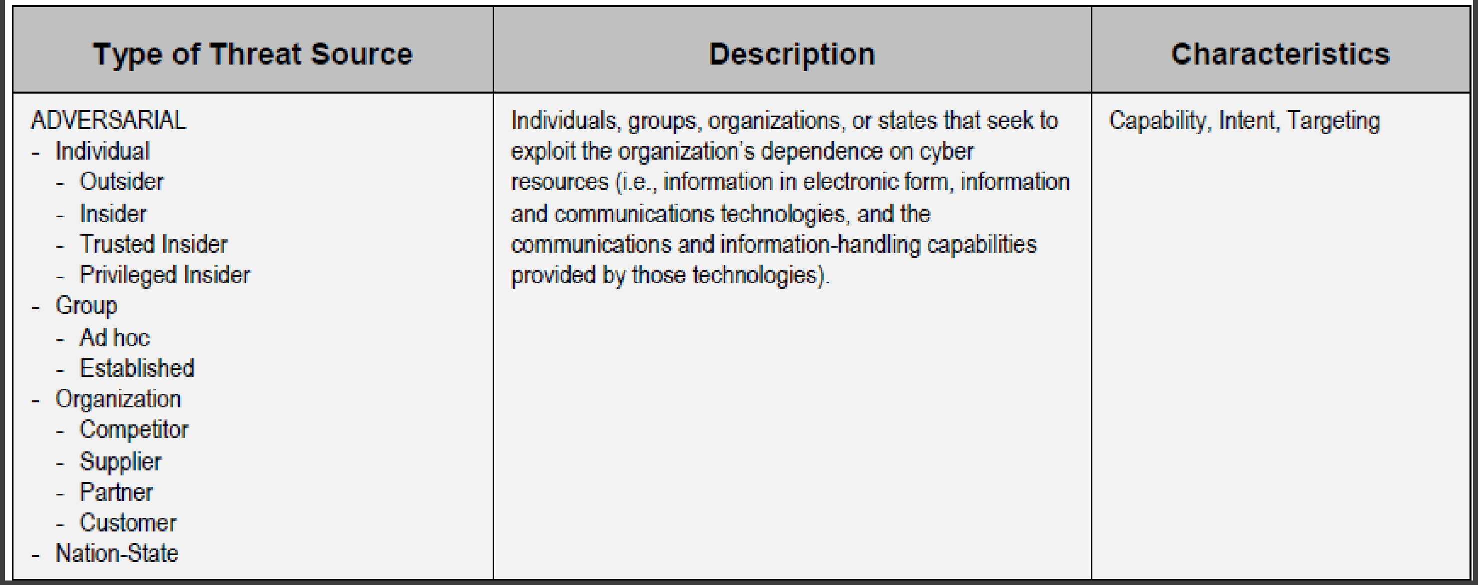
Taxonomy of threat sources

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

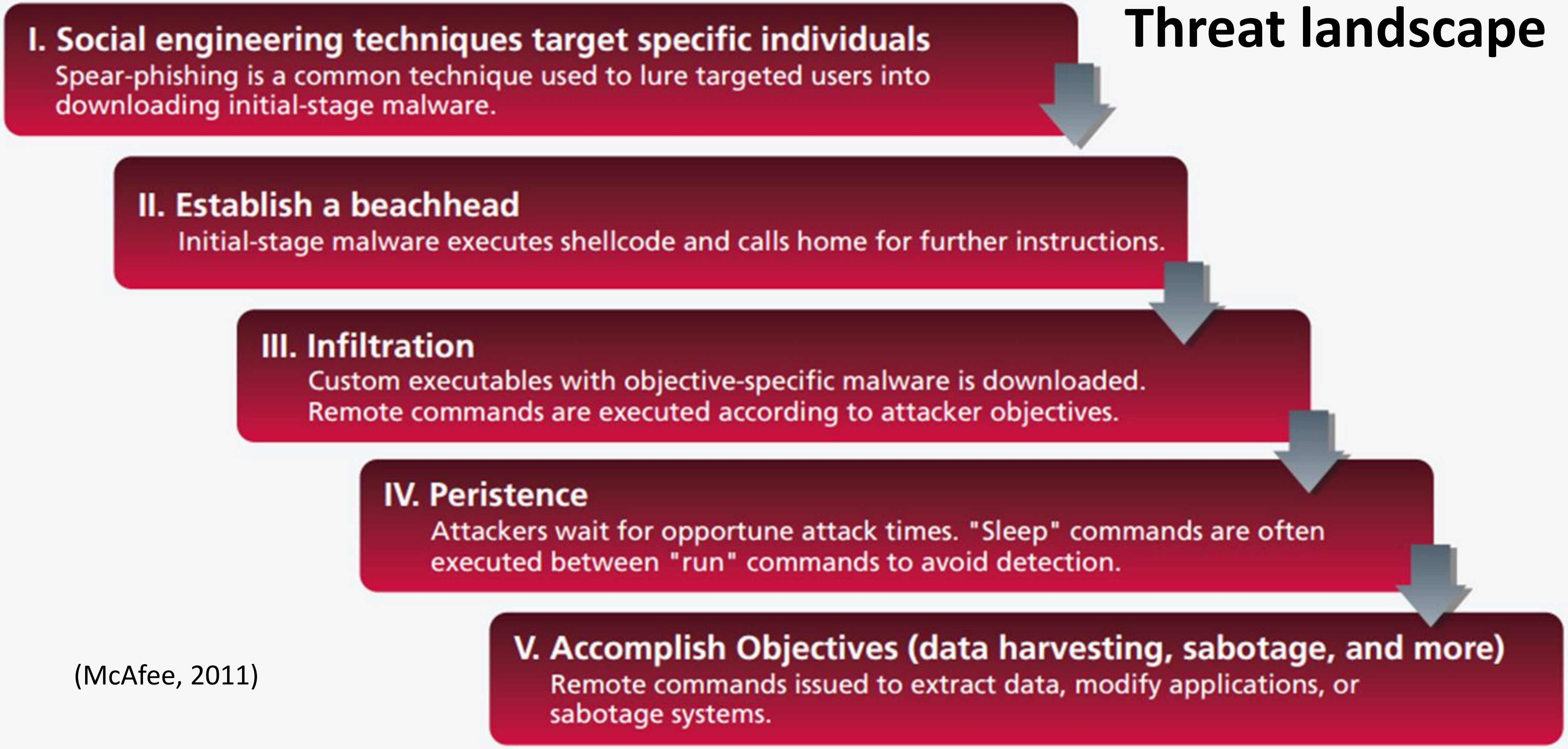


Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit 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

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

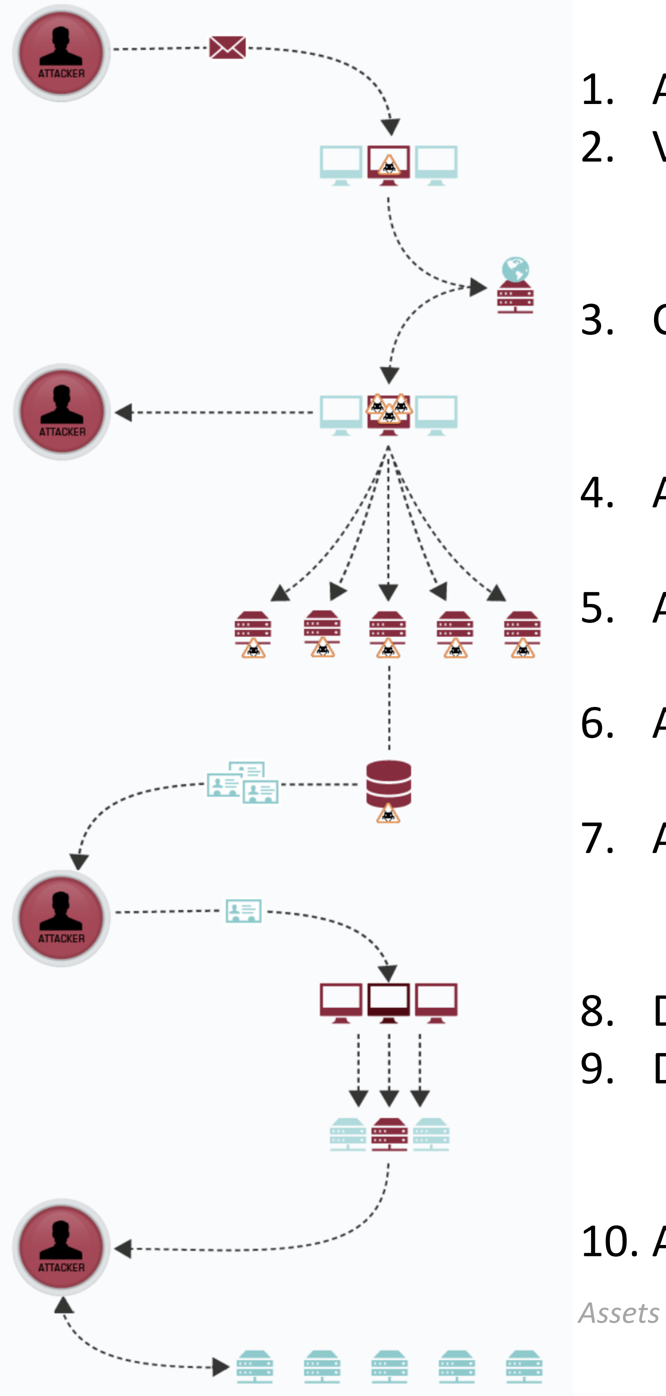
V. Accomplish Objectives (data harvesting, sabotage, and more)
Remote commands issued to extract data, modify applications, or sabotage systems.

(McAfee, 2011)

Anatomy of an Attack

(MANDIANT, 2015)

Threat landscape



1. Attacker sends spear fishing e-mail
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

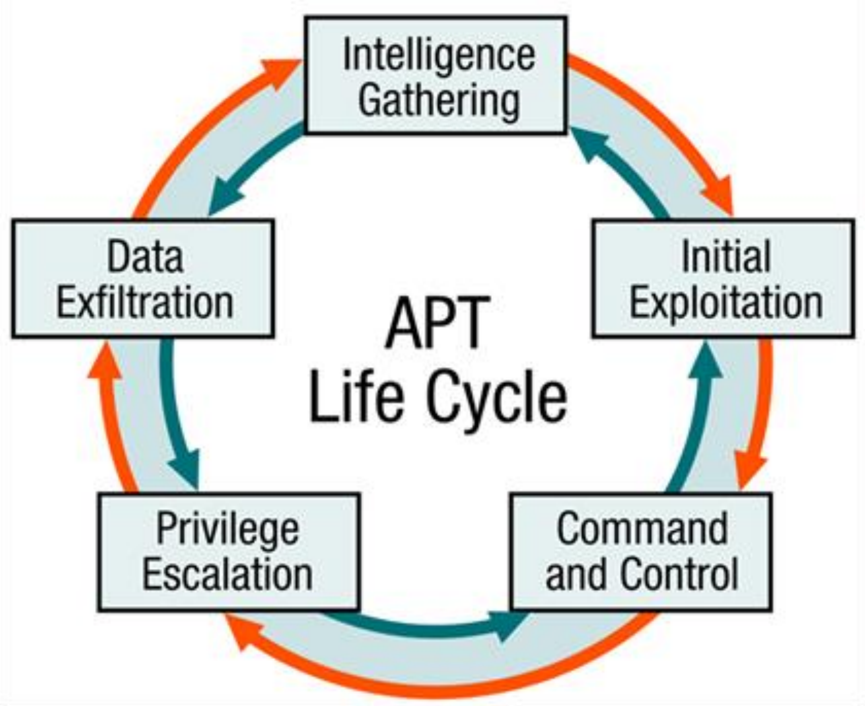
8. Data collected on staging server
9. Data exfiltrated

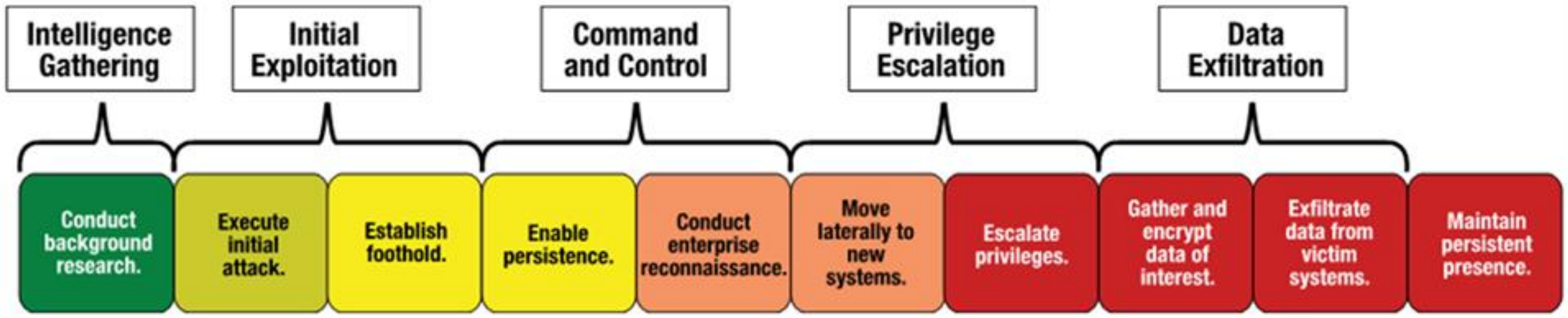
10. Attacker covers tracts
    - Deletes files
    - Can return any time

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

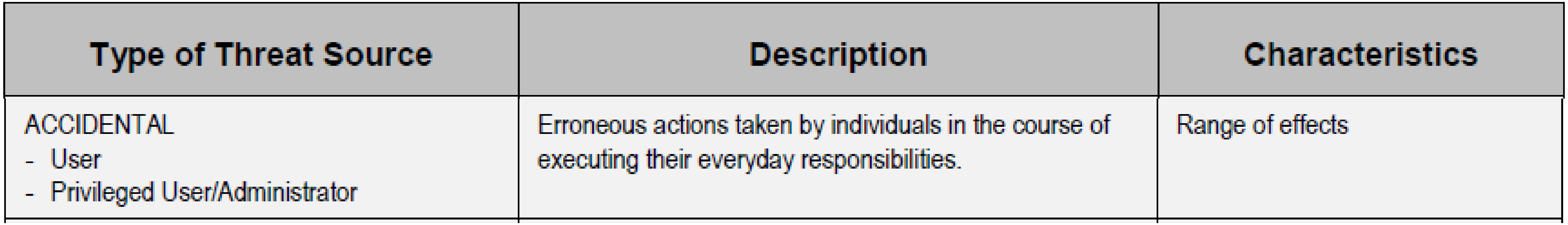
Threat landscape

Anatomy of Advanced Persistent Threats (APT)




Intelligence Gathering
Initial Exploitation
Command and Control
Privilege Escalation
Data Exfiltration
Conduct background research.
Execute initial attack.
Establish foothold.
Enable persistence.
Conduct enterprise reconnaissance.
Move laterally to new systems.
Escalate privileges.
Gather and encrypt data of interest.
Exfiltrate data from victim systems.
Maintain persistent presence.

Taxonomy of cybersecurity threat sources



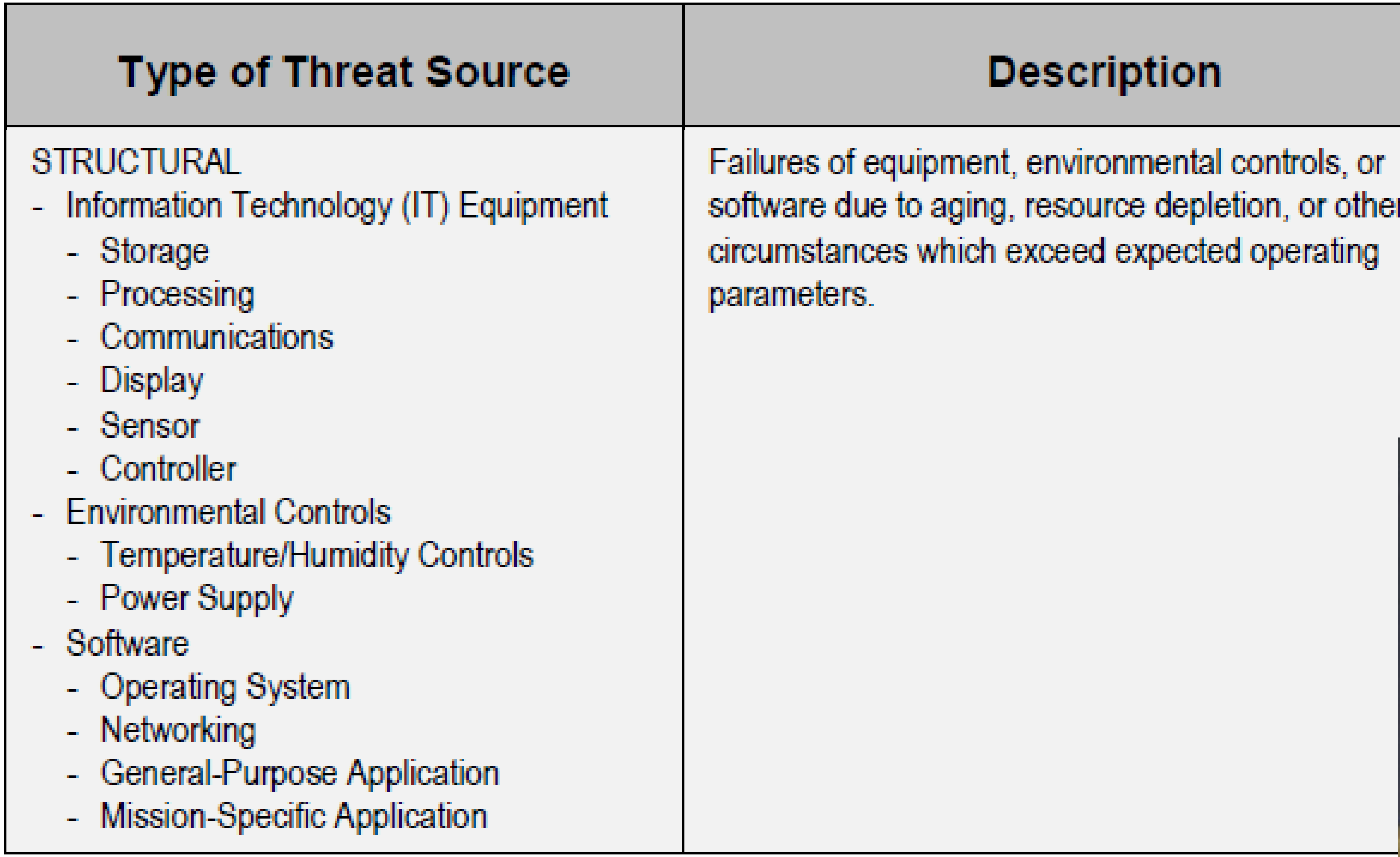
Type of Threat Source	Description	Characteristics
ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

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



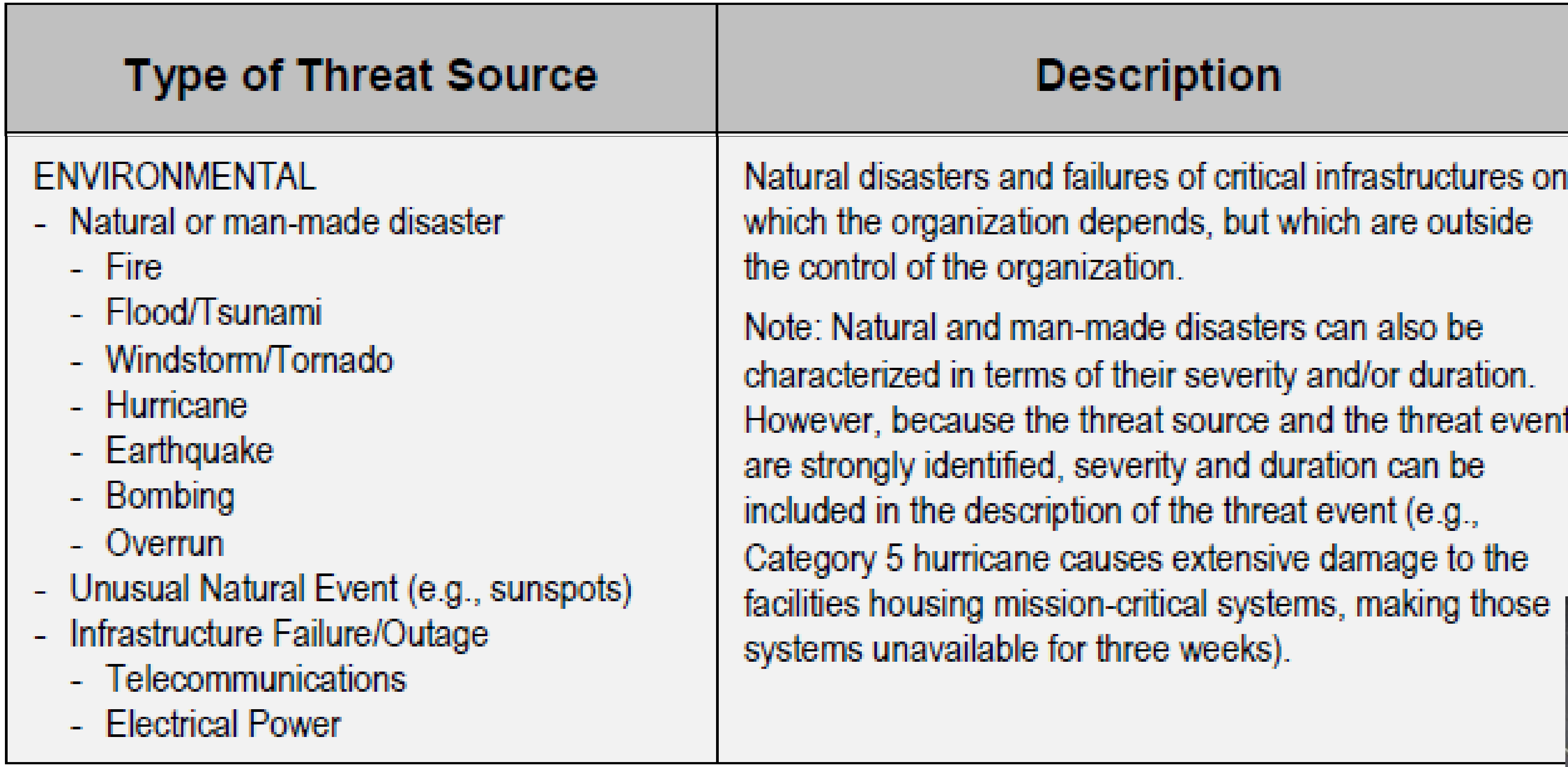
Type of Threat Source	Description	Characteristics
STRUCTURAL - Information Technology (IT) Equipment - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls - Temperature/Humidity Controls - Power Supply - Software - Operating System - Networking - General-Purpose 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)
- …

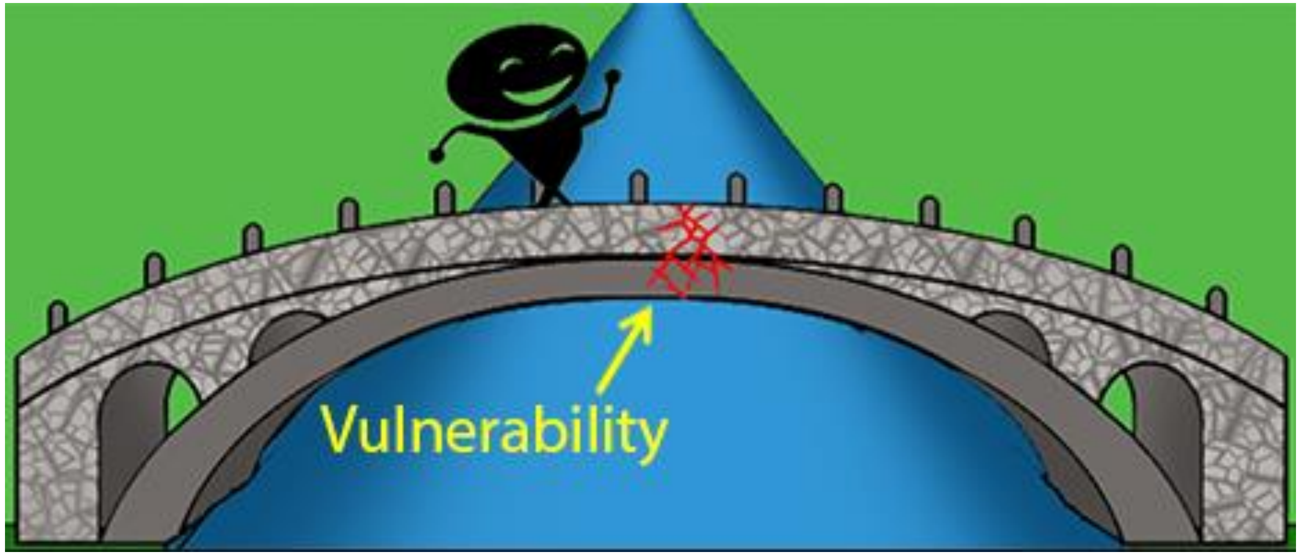
Taxonomy of cybersecurity threat sources



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

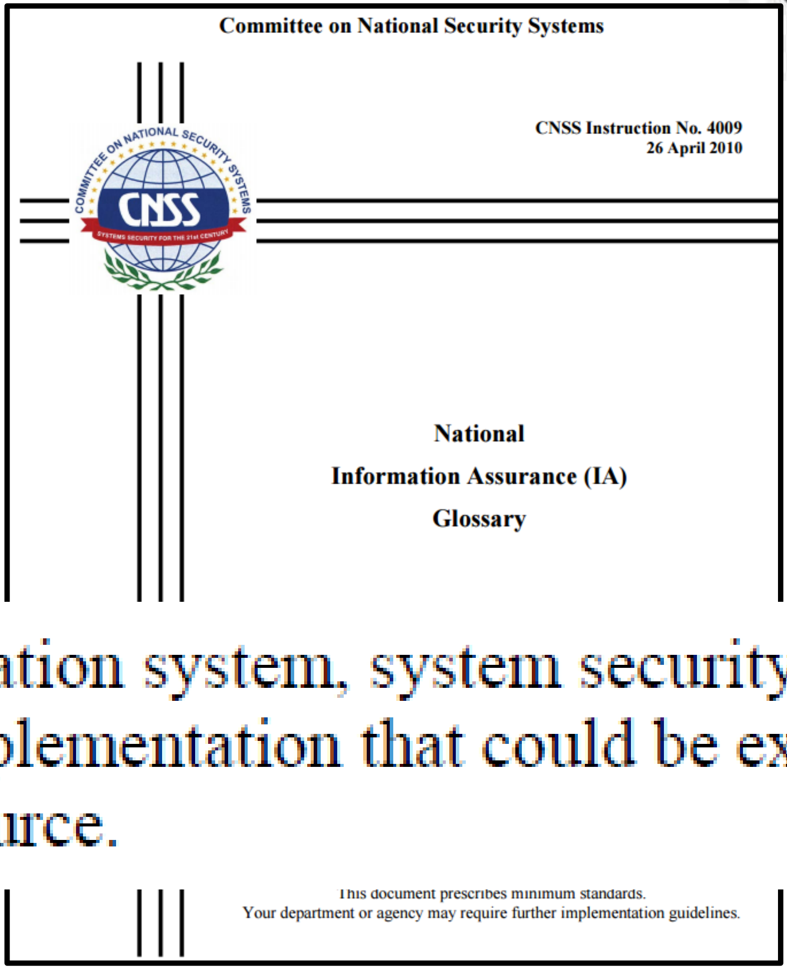
NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66

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

COMMITTEE ON NATIONAL SECURITY SYSTEMS
CNSS
SYSTEMS SECURITY FOR THE 21st CENTURY

CNSS Instruction No. 4009
26 April 2010

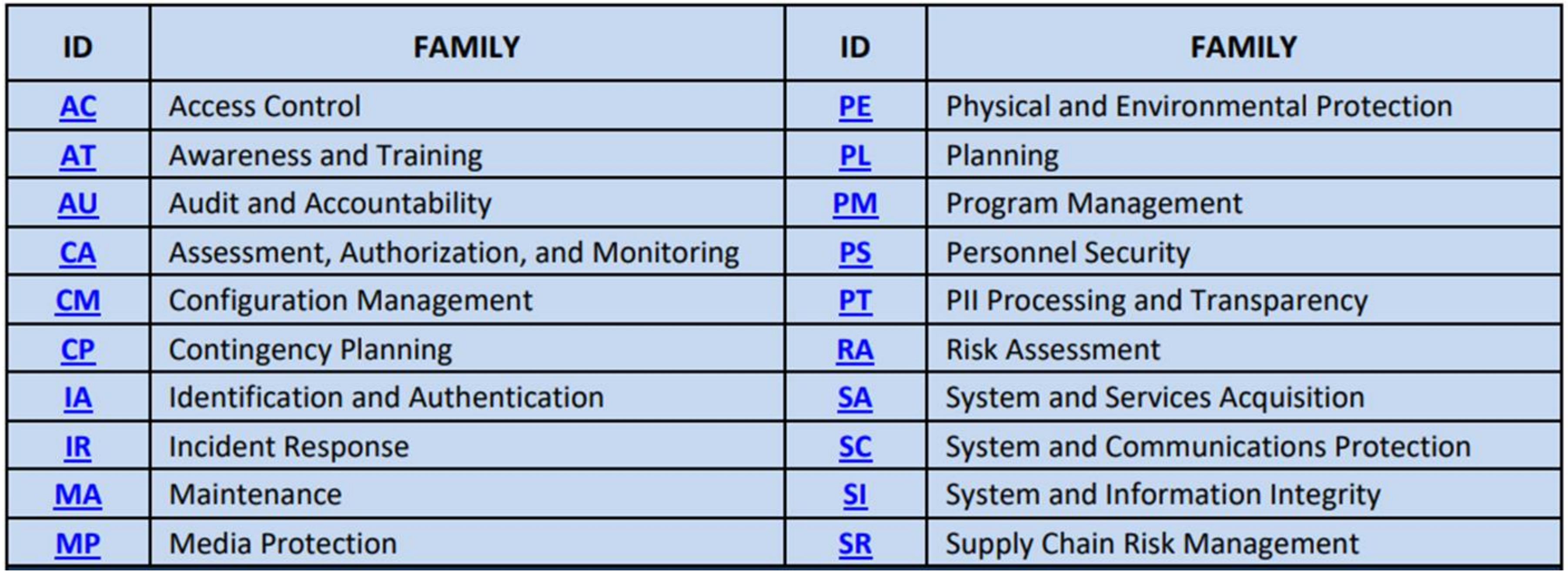
National
Information Assurance (IA)
Glossary

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

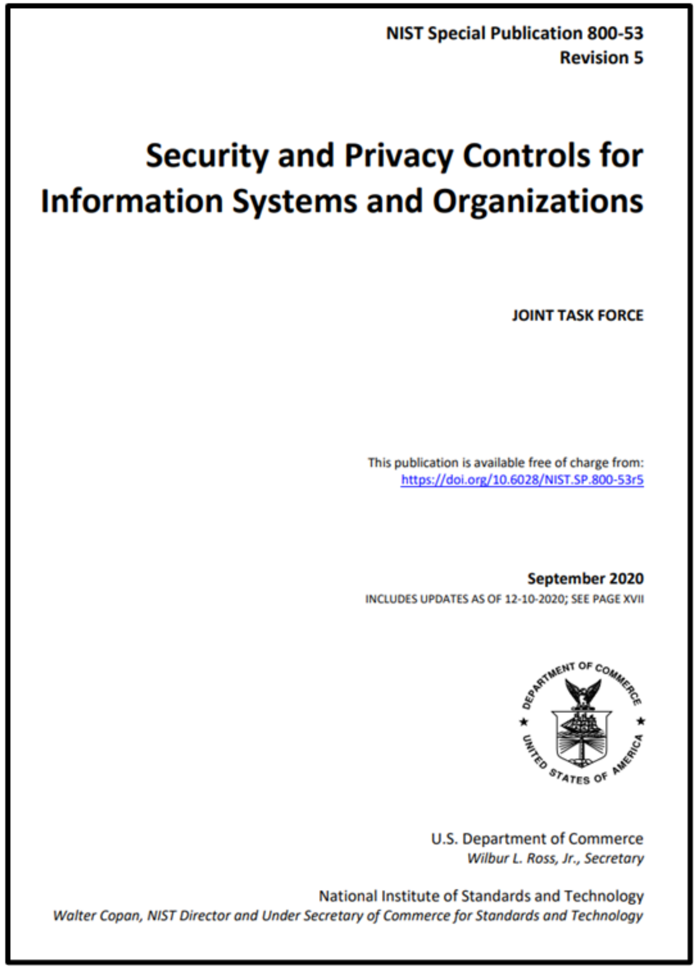
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerabilities

Inadequacies in any of these areas:



ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

What is a Risk?

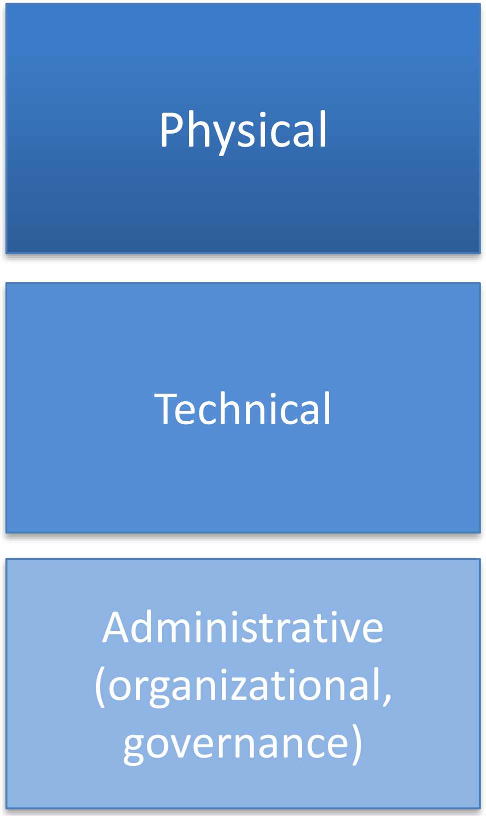
A measure of the potential impact of a threat resulting from an exploitation of a vulnerability

Potential loss resulting from unauthorized:

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

…of an enterprises' information

Can be expresses in quantitative and qualitative terms



Physical

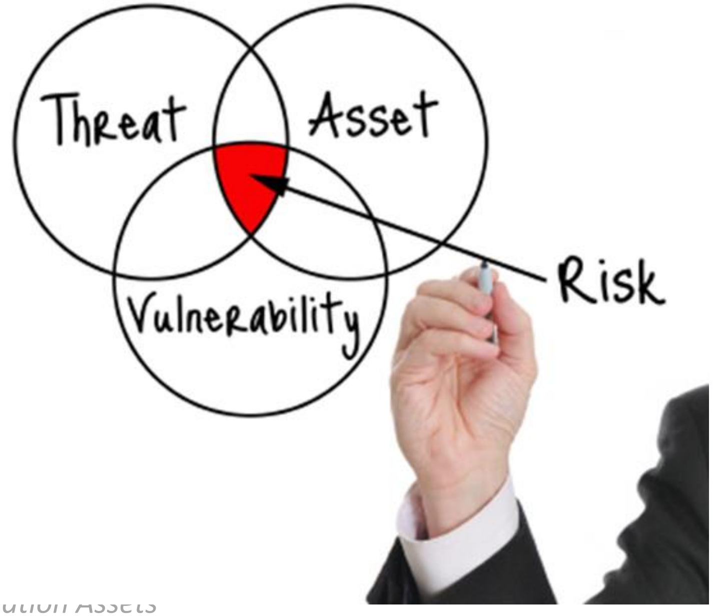
Technical

Administrative (organizational, governance)

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)

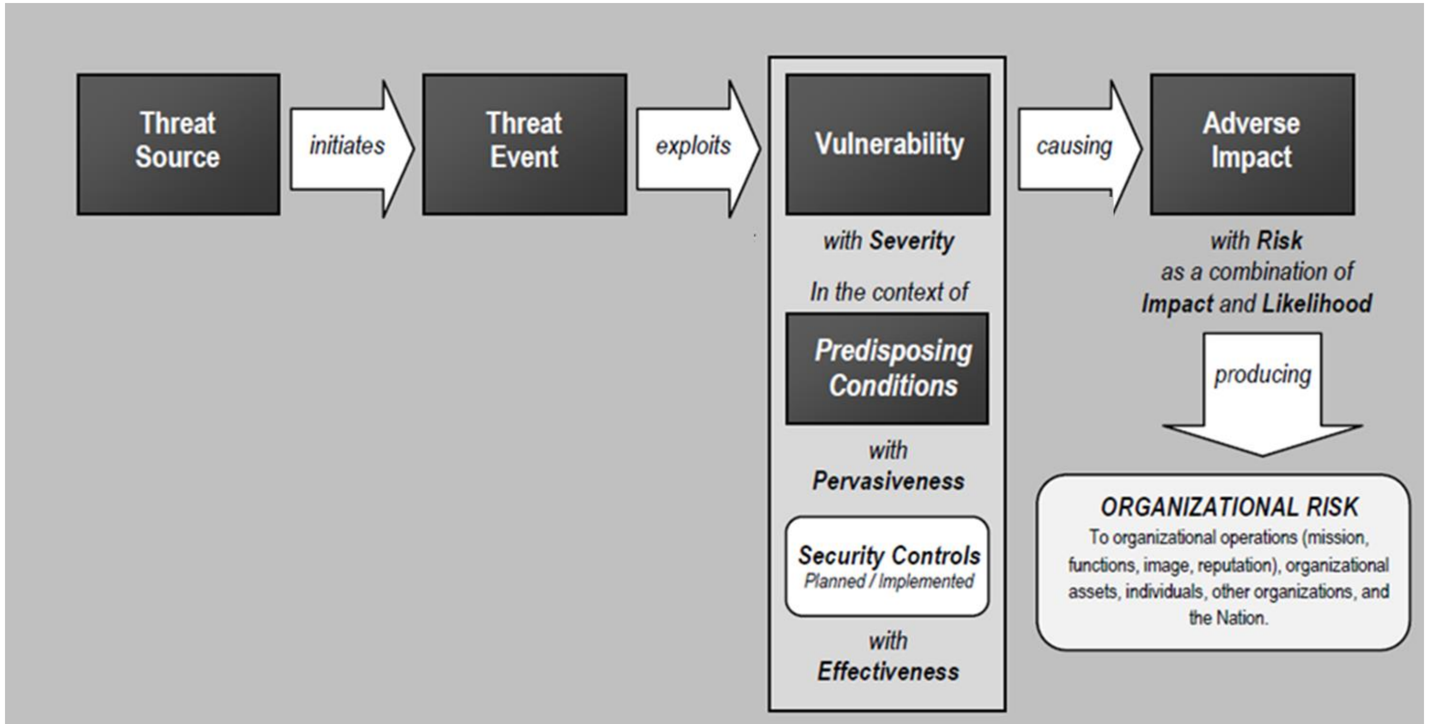


- Loss of life
- Losses due to fraud, theft, larceny, bribery
- Impact of
  - lost competitive edge
  - lost data
  - lost time
  - lost productivity
  - lost business

- Bankruptcy
- Business interruption
- Frustration
- Ill will
- Injury
- Impacts of inaccurate data

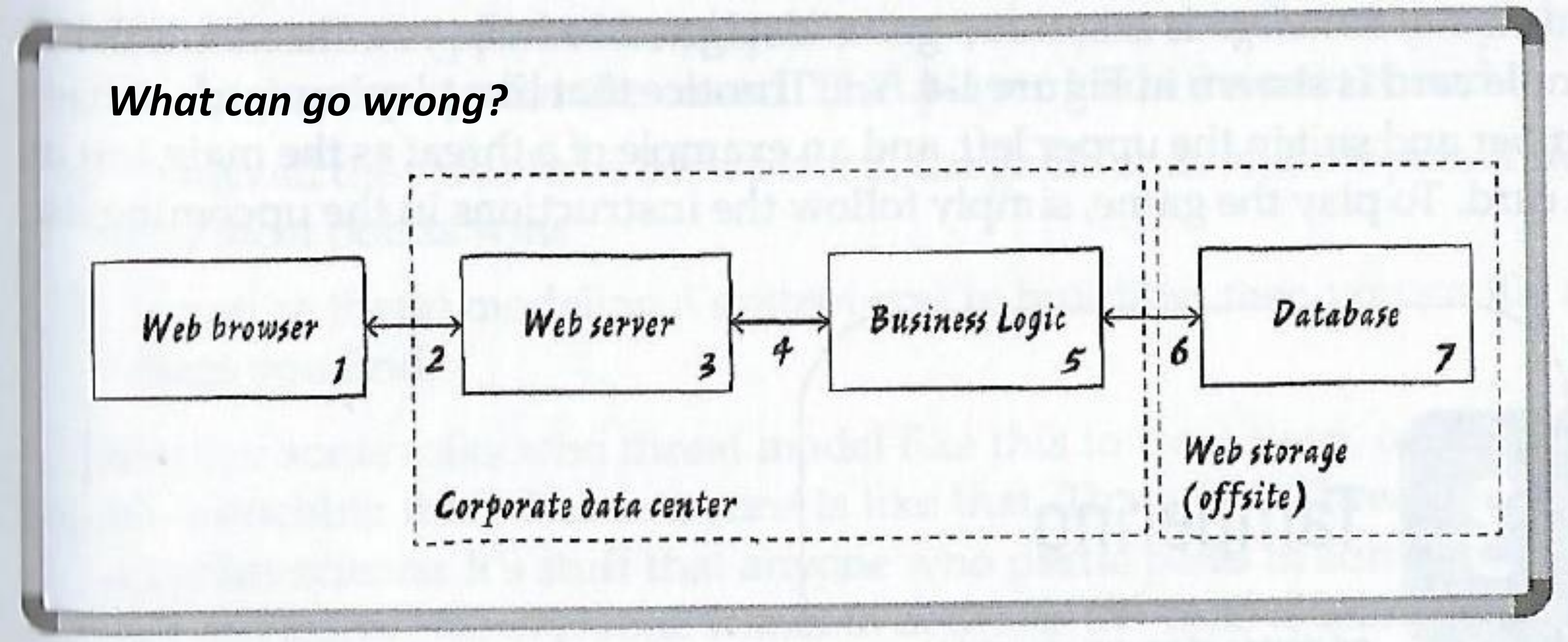
Risk analysis with an IT risk model

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



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

Process for Assessing IT risk



What can go wrong?

Quantitative definition of risk *financial method*

Risk = Impact × Probability

- *Risk is an "expected value", which is a quantitative measure of impact a threat event would have on the organization times the probability that it might happen*

Annualize Loss Expectancy (ALE) = Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

ALE = SLE X ARO

Single Loss Expectancy (SLE) = Asset value X Exposure factor

- Calculations of SLE consider such things as:
  - replacement cost of the asset
  - opportunity cost of delays because asset is no longer available
  - cost for purchasing credit monitoring for customers
  - fines and other economic impacts of the loss of confidentiality, integrity and availability of the information or information system
- Exposure factor is the % damage that a realized threat would have on the asset

Annual Rate of Occurrence (ARO) is a probability indicating how many times this is expected in one year?

Risk Management Techniques

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

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

How can we make a computer 100% secure?

3 Golden Rules to ensure computer security:

1. Do not own a computer
2. Do not power it on
3. Do not use it

Cryptographer who helped develop the Unix computer operating system, which controls many of the world’s computers and touches almost every aspect of modern life

Robert Morris

Chief Scientist, National Security Agency’s (NSA) National Computer Security Center, 1986-1994

Risk mitigations – Which are physical, technical and administrative controls ?

- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate revocation list
- 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 – Technical - *Administrative*

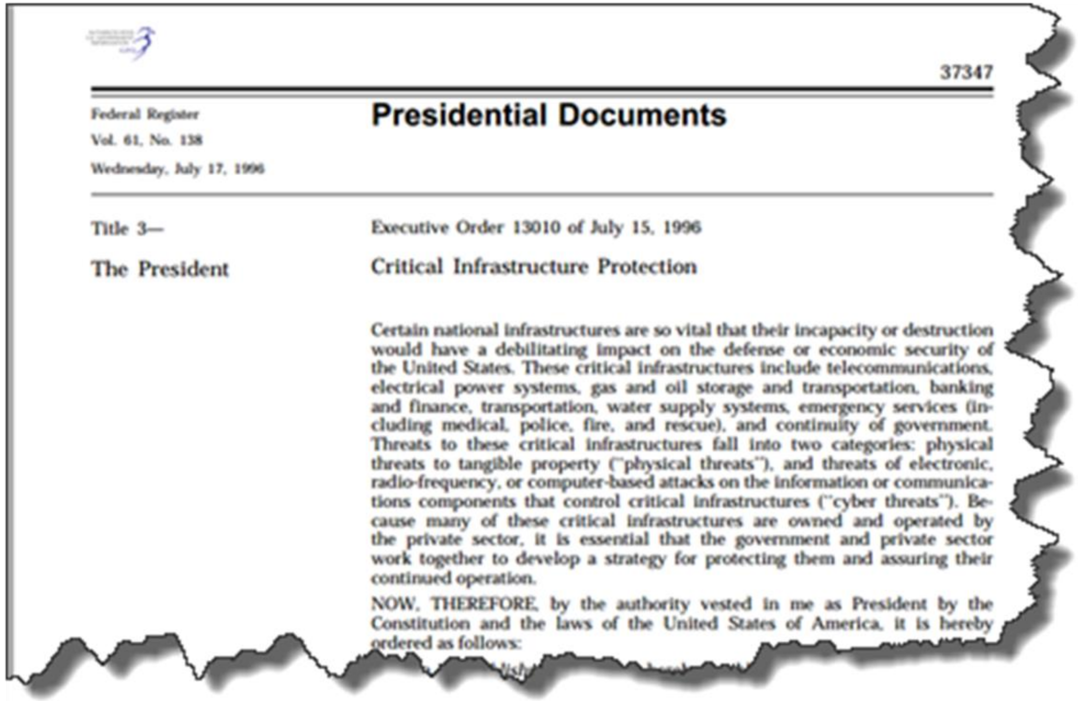
- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- Canine patrols
- Card-activated locks
- Certificate authority
- *Code of sanctions against vendors/suppliers/contractors*
- *Color-coded ID badges*
- Content scanners
- 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 / shredders
- Secure file wipes
- Secure passwords
- Single sign-on
- Environmental controls (air conditioners, humidifiers)

Critical Infrastructure

1996 Presidential Executive Order identified critical infrastructure needing protection…

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

1. ***Water supply systems***
2. ***Transportation***
3. ***Gas and oil storage and transport***
4. ***Telecommunications***
5. ***Electrical power systems***
6. ***Banking and finance***
7. ***Emergency services***
8. ***Continuity of government***



37347

Federal Register
Vol. 61, No. 138
Wednesday, July 17, 1996

Presidential Documents

Title 3—

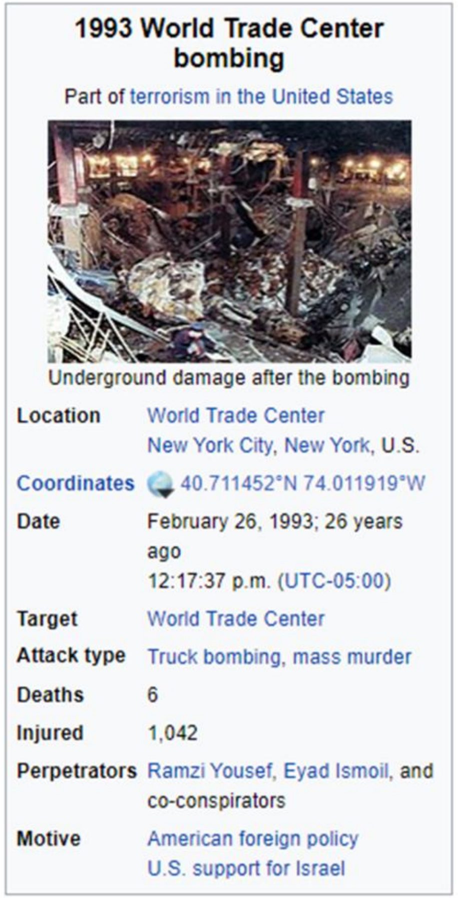
The President

Executive Order 13010 of July 15, 1996

Critical Infrastructure Protection

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:



1993 World Trade Center bombing

Part of terrorism in the United States

Underground damage after the bombing

Location	World Trade Center New York City, New York, U.S.
Coordinates	40.711452°N 74.011919°W
Date	February 26, 1993; 26 years ago 12:17:37 p.m. (UTC-05:00)
Target	World Trade Center
Attack type	Truck bombing, mass murder
Deaths	6
Injured	1,042
Perpetrators	Ramzi Yousef, Eyad Ismoil, and co-conspirators
Motive	American foreign policy U.S. support for Israel

(PPD-21)

Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21) issued in 2013 identified…

16 U.S. Critical Infrastructure Sectors needing protection

Transportation

Commercial Facilities

Energy

Healthcare and Public Health

Water and Wastewater Systems

Nuclear Reactors, Materials, and Waste

Chemical

Information Technology

Dams

Defense Industrial Base

Government Facilities

Food and Agriculture

Emergency Services

Communications

Critical Manufacturing

Financial Services

https://www.cisa.gov/critical-infrastructure-sectors

https://www.cisa.gov/critical-infrastructure-sectors

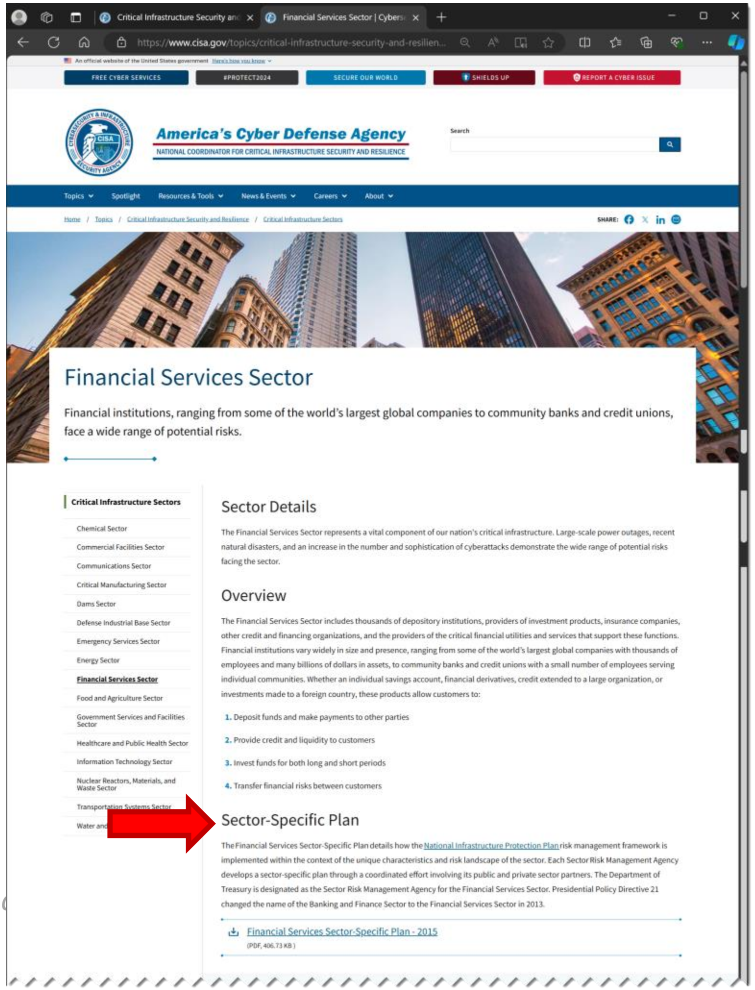
Critical Infrastructure Information –data that can be used in either physical or computer-based attack that directly or indirectly

- 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 Sector-Specific Plan

Each sector has a sector-specific plan that details how the National Infrastructure Protection Plan is implemented through government and private sector partnerships to work together to manage risks and achieve security and resilience outcomes


Critical Infrastructure Security an
Financial Services Sector | Cybers
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilien...
An official website of the United States government Here's how you know
FREE CYBER SERVICES
#PROTECT2024
SECURE OUR WORLD
SHIELDS UP
REPORT A CYBER ISSUE
America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
Home / Topics / Critical Infrastructure Security and Resilience / Critical Infrastructure Sectors
SHARE:

Financial Services Sector

Financial institutions, ranging from some of the world's largest global companies to community banks and credit unions, face a wide range of potential risks.

Critical Infrastructure Sectors

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- **Financial Services Sector**
- Food and Agriculture Sector
- Government Services and Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and

Sector Details

The Financial Services Sector represents a vital component of our nation's critical infrastructure. Large-scale power outages, recent natural disasters, and an increase in the number and sophistication of cyberattacks demonstrate the wide range of potential risks facing the sector.

Overview

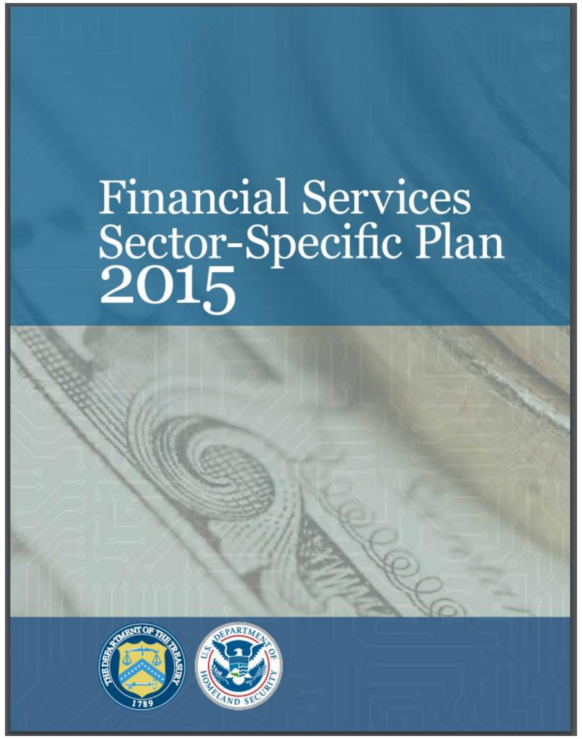
The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities. Whether an individual savings account, financial derivatives, credit extended to a large organization, or investments made to a foreign country, these products allow customers to:

1. Deposit funds and make payments to other parties
2. Provide credit and liquidity to customers
3. Invest funds for both long and short periods
4. Transfer financial risks between customers

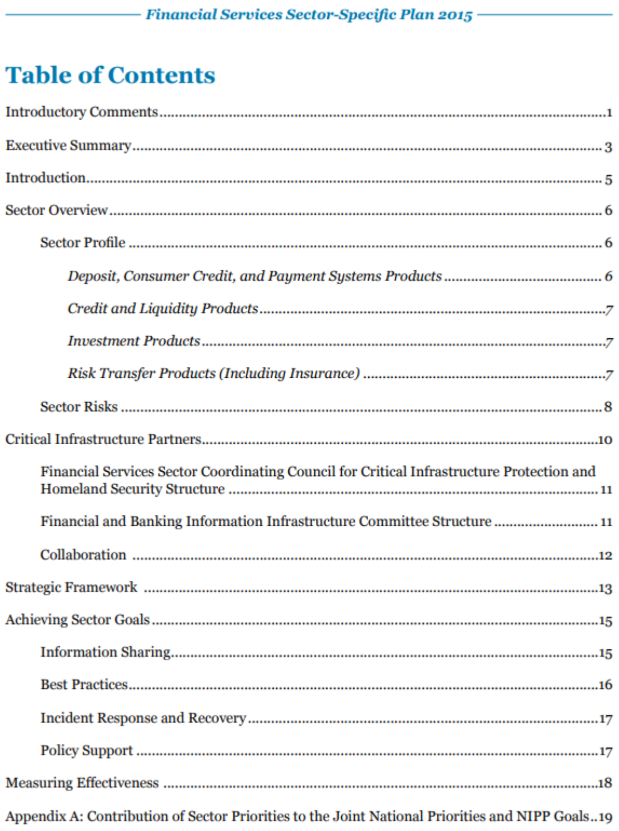
Sector-Specific Plan

The Financial Services Sector-Specific Plan details how the National Infrastructure Protection Plan risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector. Each Sector Risk Management Agency develops a sector-specific plan through a coordinated effort involving its public and private sector partners. The Department of Treasury is designated as the Sector Risk Management Agency for the Financial Services Sector. Presidential Policy Directive 21 changed the name of the Banking and Finance Sector to the Financial Services Sector in 2013.

Financial Services Sector-Specific Plan - 2015
(PDF, 406.73 KB)



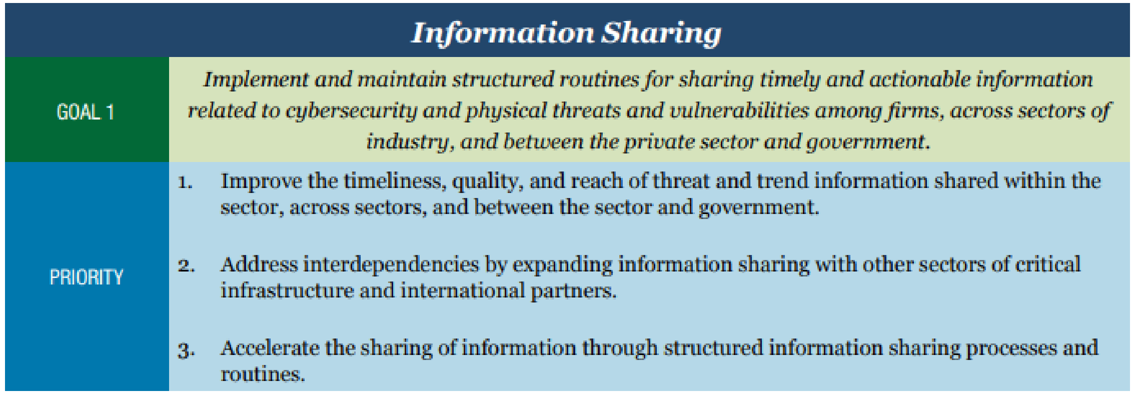
Financial Services Sector-Specific Plan 2015



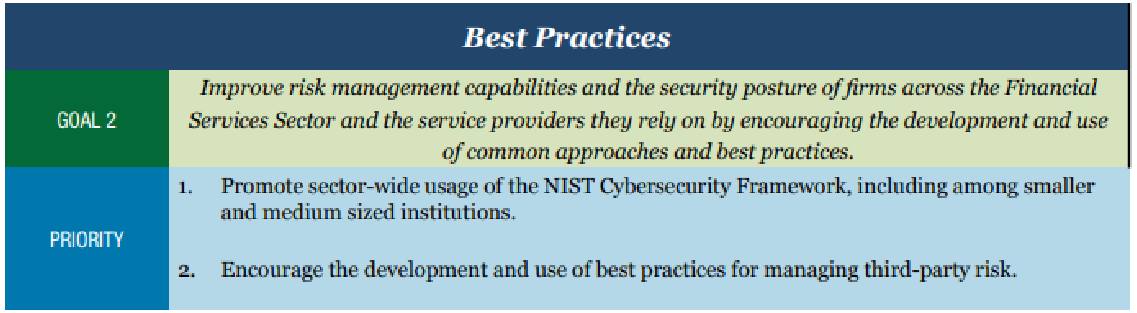
Financial Services Sector-Specific Plan 2015

Table of Contents

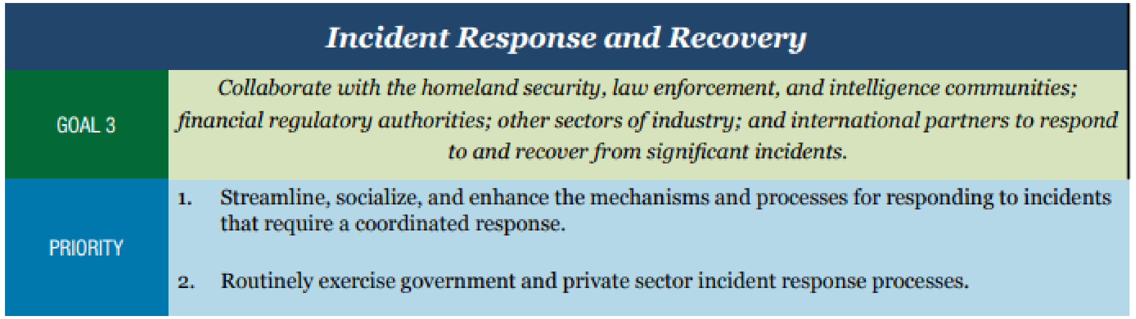
Financial Services Sector-Specific Plan 2015



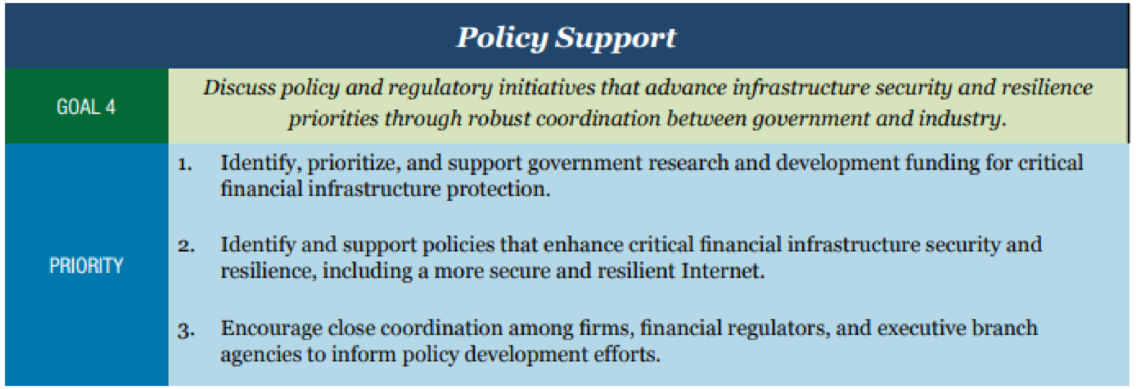
	Information Sharing
GOAL 1	*Implement and maintain structured routines for sharing timely and actionable information related to cybersecurity and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.*
PRIORITY	1. Improve the timeliness, quality, and reach of threat and trend information shared within the sector, across sectors, and between the sector and government. 2. Address interdependencies by expanding information sharing with other sectors of critical infrastructure and international partners. 3. Accelerate the sharing of information through structured information sharing processes and routines.



	Best Practices
GOAL 2	*Improve risk management capabilities and the security posture of firms across the Financial Services Sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.*
PRIORITY	1. Promote sector-wide usage of the NIST Cybersecurity Framework, including among smaller and medium sized institutions. 2. Encourage the development and use of best practices for managing third-party risk.



	Incident Response and Recovery
GOAL 3	*Collaborate with the homeland security, law enforcement, and intelligence communities; financial regulatory authorities; other sectors of industry; and international partners to respond to and recover from significant incidents.*
PRIORITY	1. Streamline, socialize, and enhance the mechanisms and processes for responding to incidents that require a coordinated response. 2. Routinely exercise government and private sector incident response processes.



	Policy Support
GOAL 4	*Discuss policy and regulatory initiatives that advance infrastructure security and resilience priorities through robust coordination between government and industry.*
PRIORITY	1. Identify, prioritize, and support government research and development funding for critical financial infrastructure protection. 2. Identify and support policies that enhance critical financial infrastructure security and resilience, including a more secure and resilient Internet. 3. Encourage close coordination among firms, financial regulators, and executive branch agencies to inform policy development efforts.

Critical Infrastructure Sectors

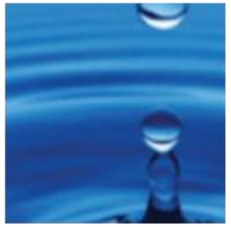
Transportation

Commercial Facilities

Energy

Healthcare and Public Health

Water and Wastewater Systems



Nuclear Reactors, Materials, and Waste

Chemical

Information Technology

Dams

Defense Industrial Base

Government Facilities

Food and Agriculture

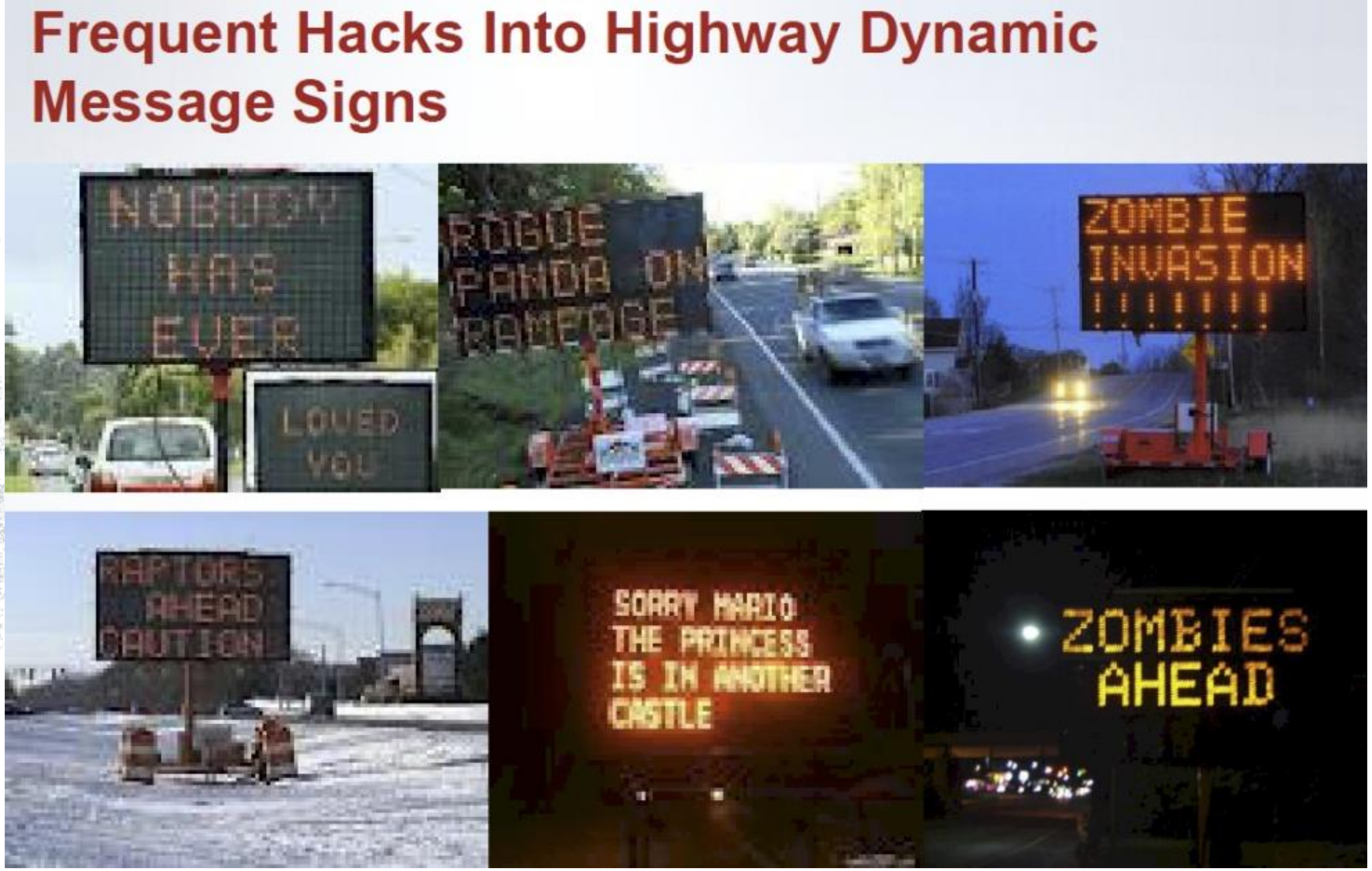
Emergency Services

Communications

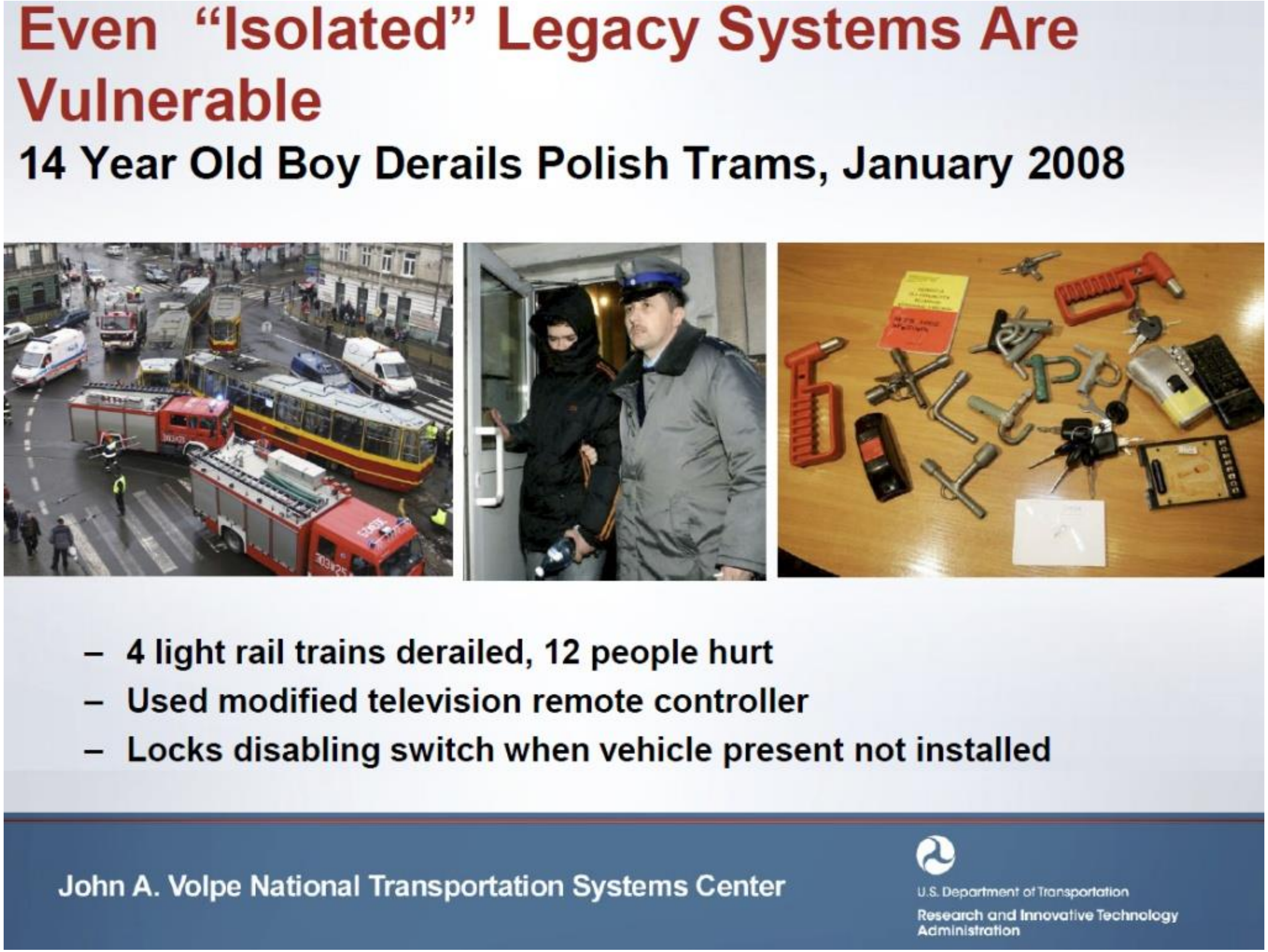
Critical Manufacturing

Financial Services

Transportation sector - examples



Frequent Hacks Into Highway Dynamic Message Signs



Even "Isolated" Legacy Systems Are Vulnerable

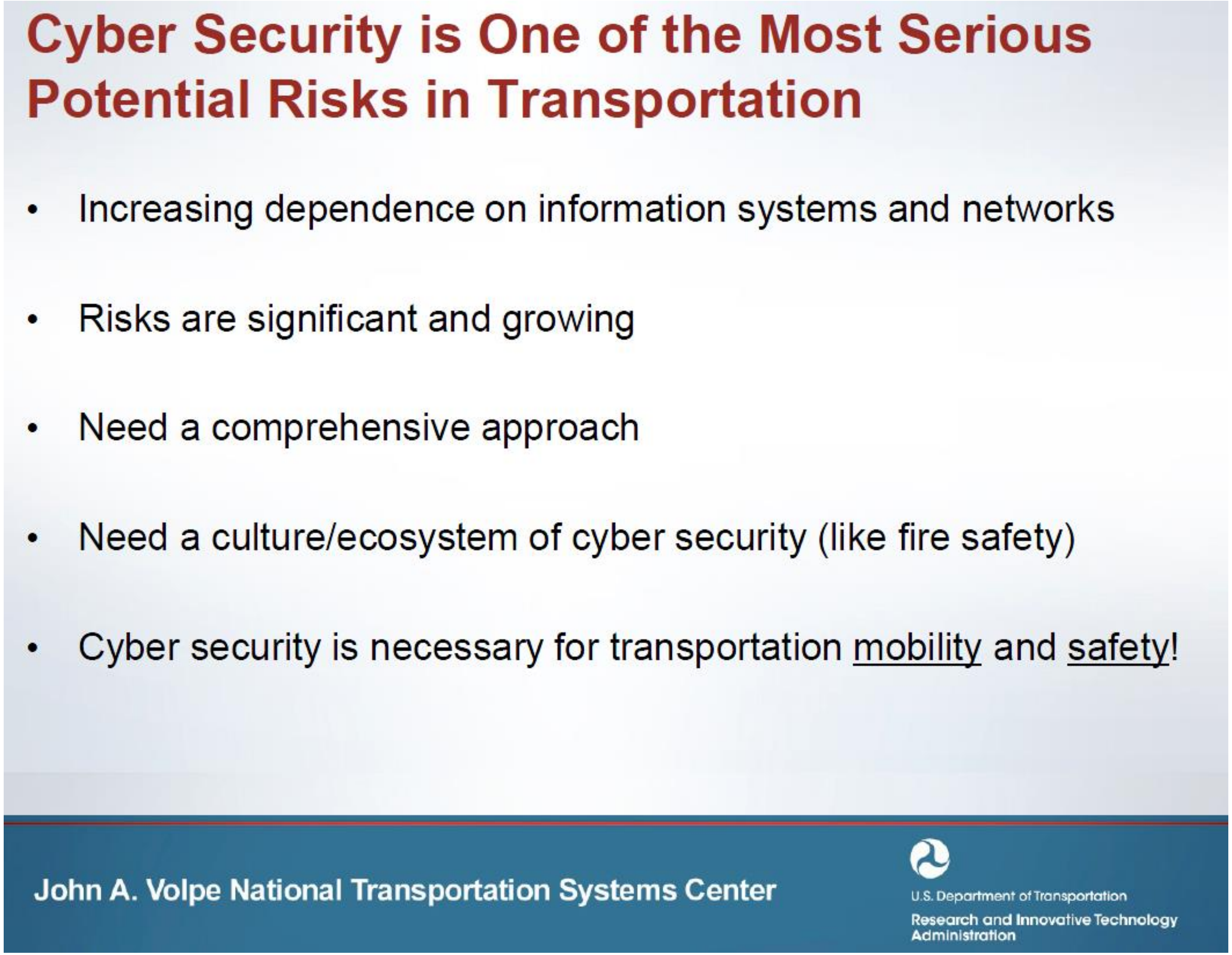
14 Year Old Boy Derails Polish Trams, January 2008

- 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



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

Critical Infrastructure Sectors

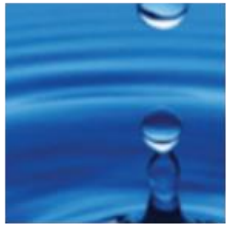
Transportation

Commercial Facilities

Energy

Healthcare and Public Health

Water and Wastewater Systems



Nuclear Reactors, Materials, and Waste

Chemical

Information Technology

Dams

Defense Industrial Base

Government Facilities

Food and Agriculture

Emergency Services

Communications

Critical Manufacturing

Financial Services

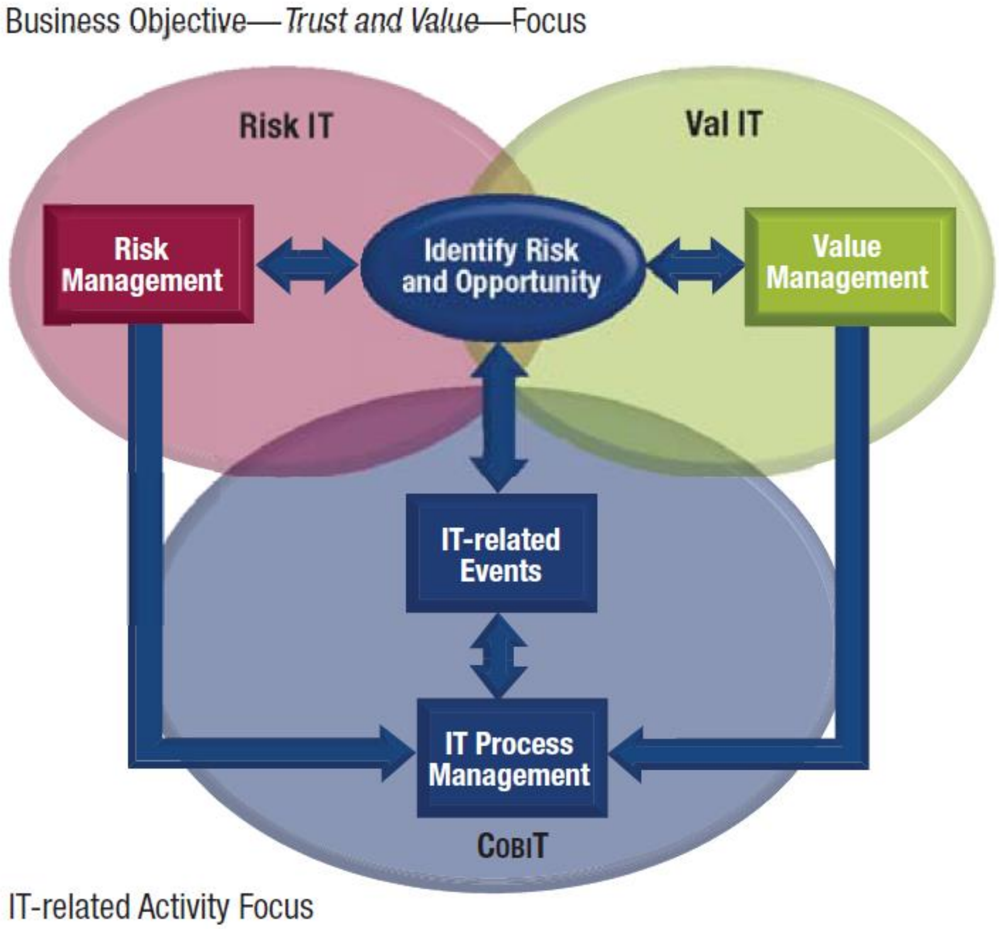
Water/Wastewater sector – Attack example 2001

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 the grounds of a Hyatt Regency hotel**
  - **Marine life died, the creek water turned black, the stench was unbearable for residents**

ISACA’s RiskIT Framework


Business Objective—*Trust and Value*—Focus
Risk IT
Val IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
CobiT
IT-related Activity Focus

- 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

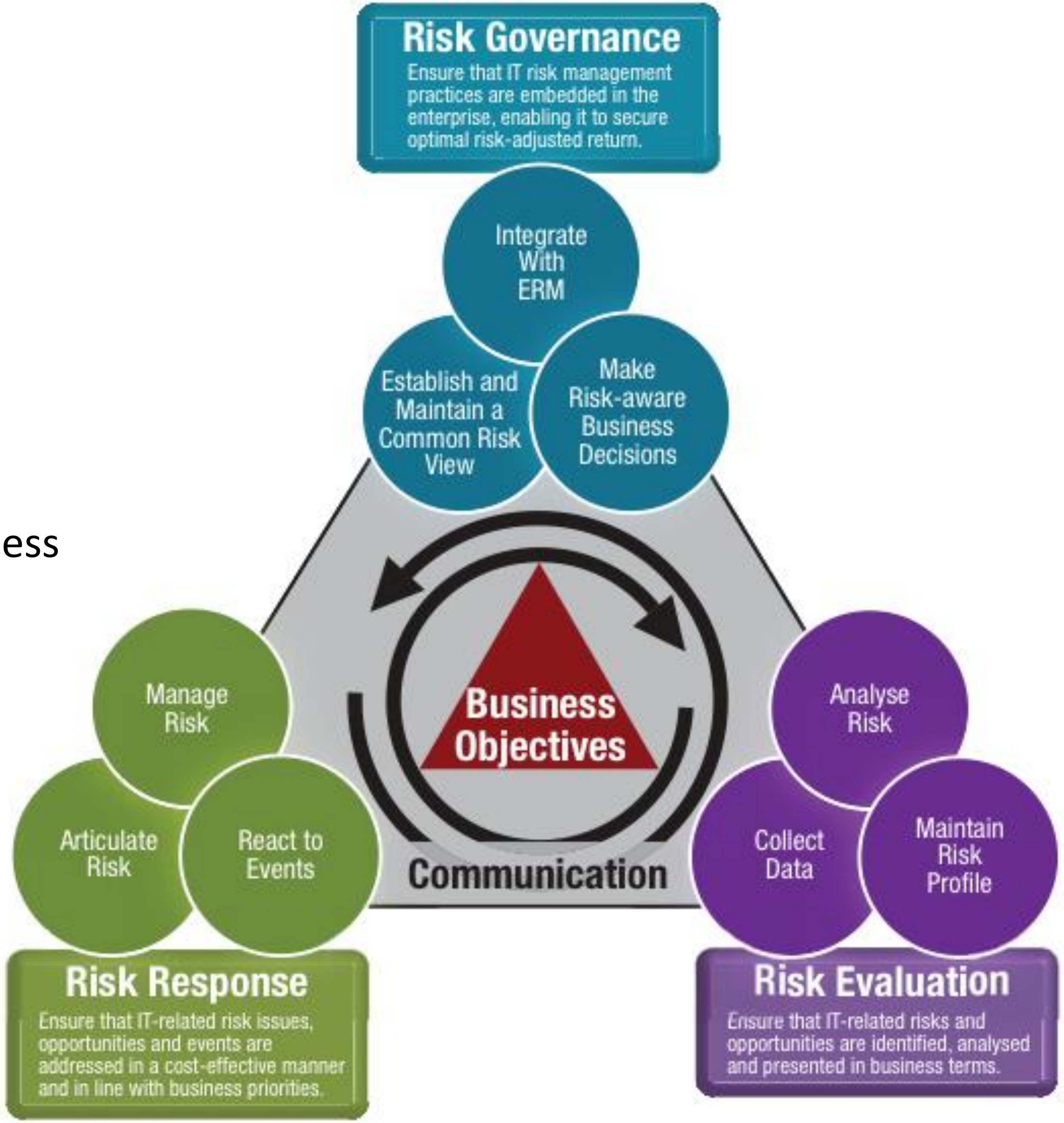
  – IT governance framework and supporting toolset enabling managers to bridge the gap between business risks, risk control requirements, and technical issues

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


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.

ISO/IEC 27001 Standard

Considered a leading example of risk management for information security and Privacy Protection

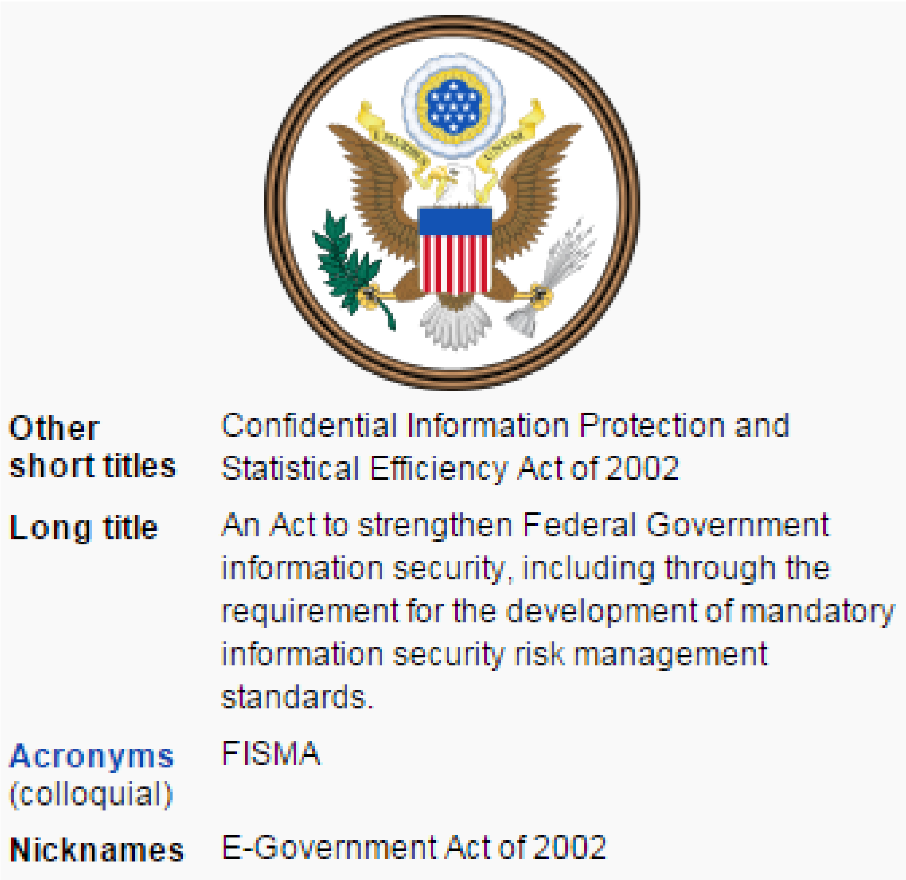
- Created in 2005 and updated in 2013, 2018, and 2022 by agreement between
  - International Organization for Standardization (ISO)
  - International Electro-technical Commission (IEC)
- Specific requirements for security management systems and controls
- Firms can apply to be audited and certified as ISO/IEC 27001 compliant

Federal Information Security Management Act (FISMA) of 2002

Federal Information Security Modernization Act (FISMA) of 2014

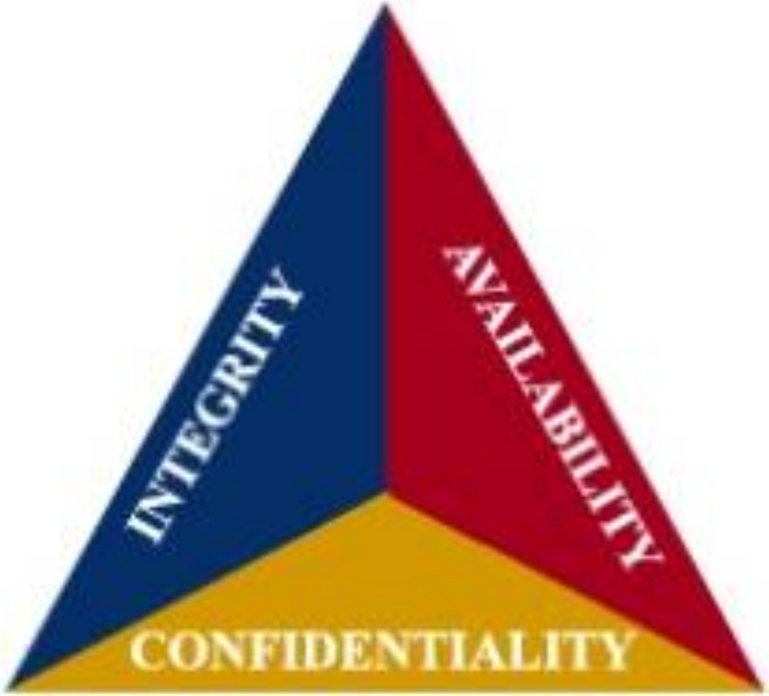
Recognize importance of information security to the economy and national security

- **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?

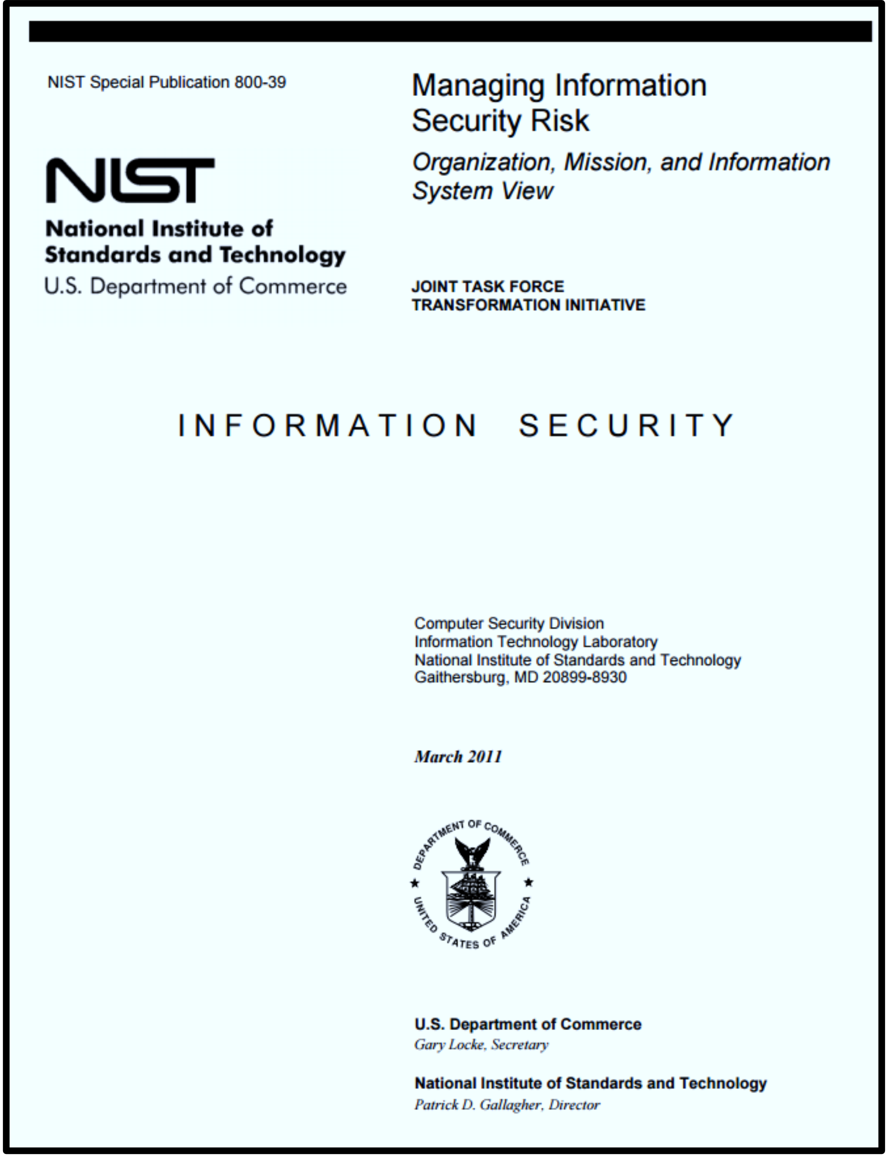
National Institute of Standards and Technology
U.S. Department of Commerce

- 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**

FISMA made 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 Special Publication 800-39

Managing Information Security Risk

Organization, Mission, and Information System View

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

JOINT TASK FORCE TRANSFORMATION INITIATIVE

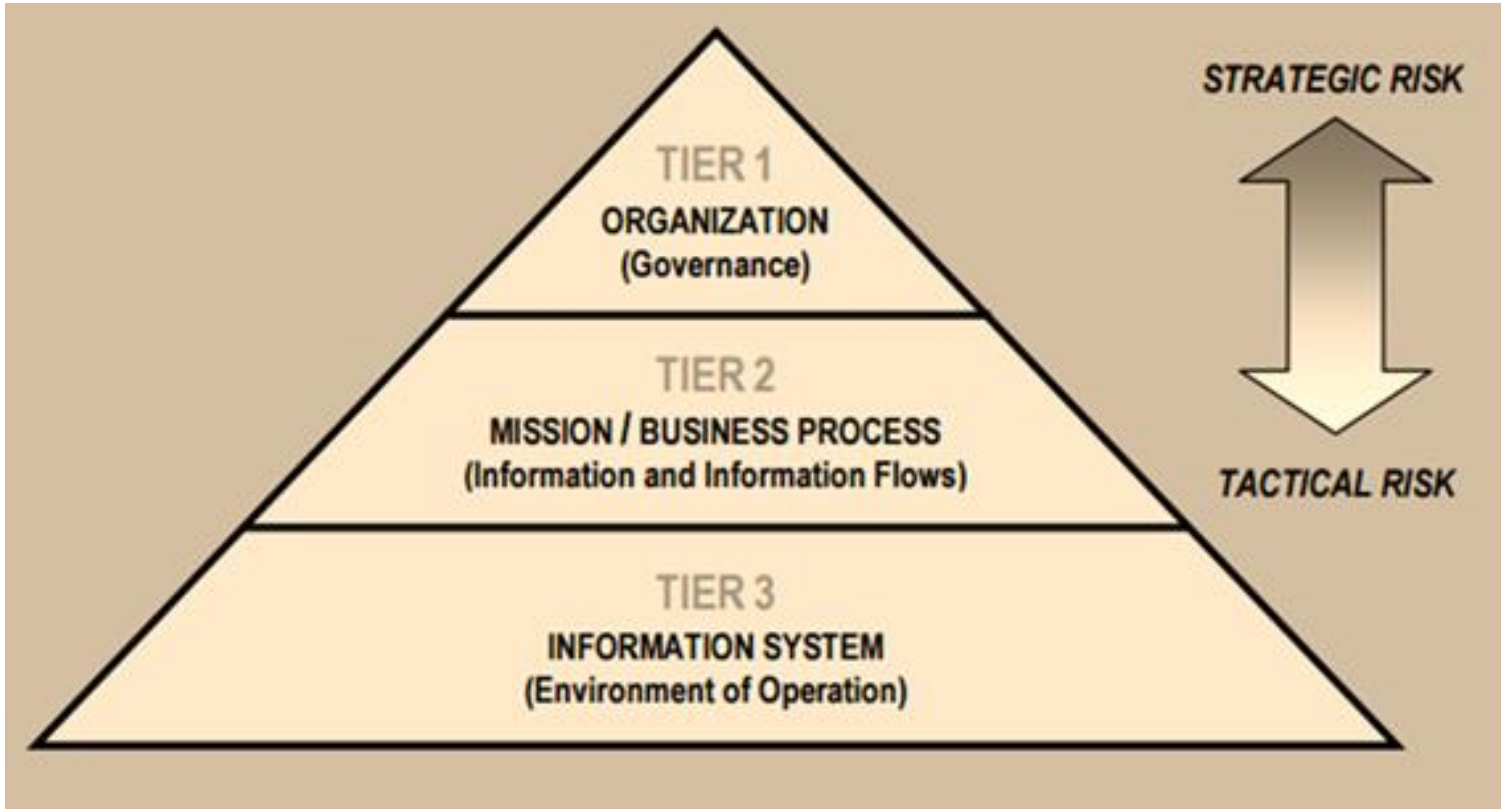
INFORMATION SECURITY

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



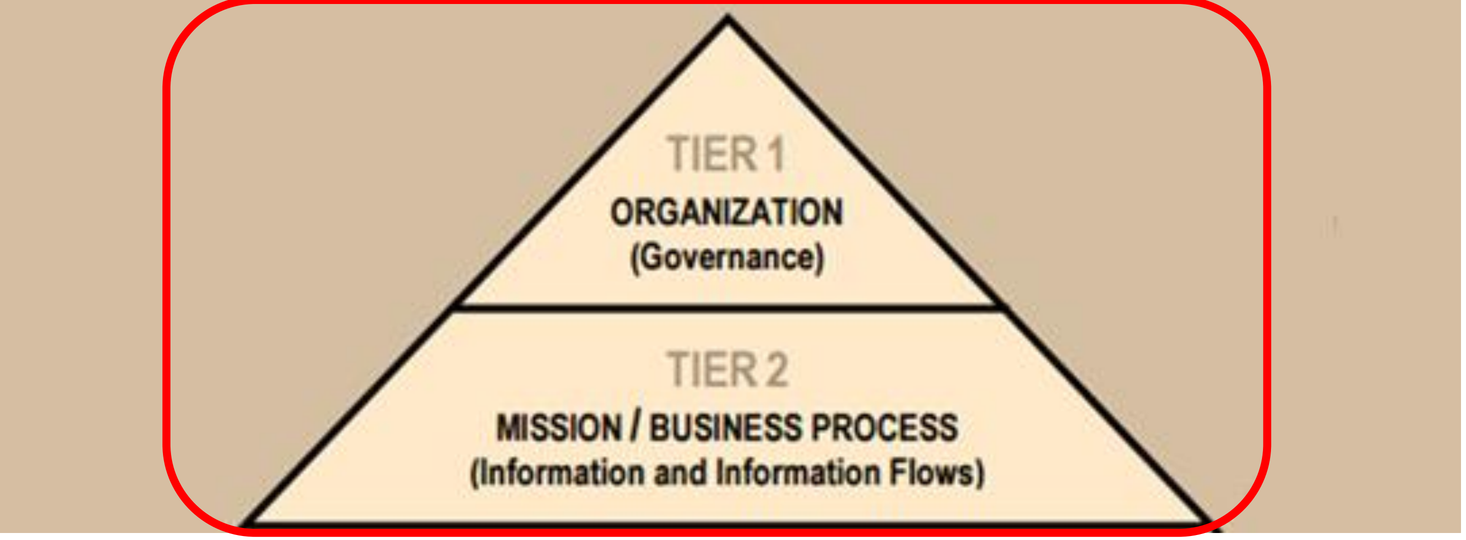
TIER 1
ORGANIZATION
(Governance)

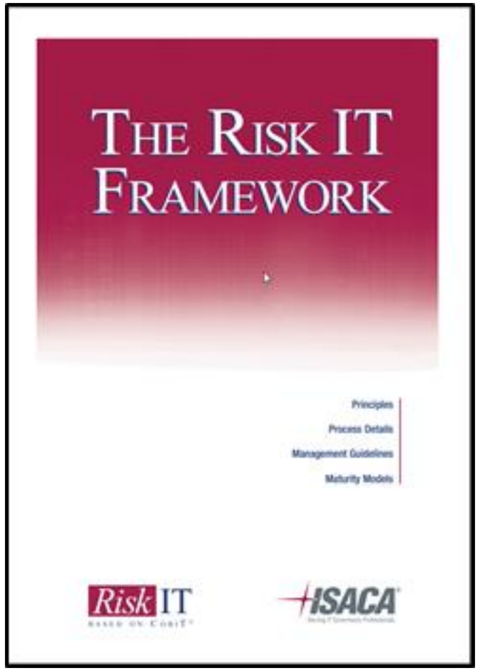
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)

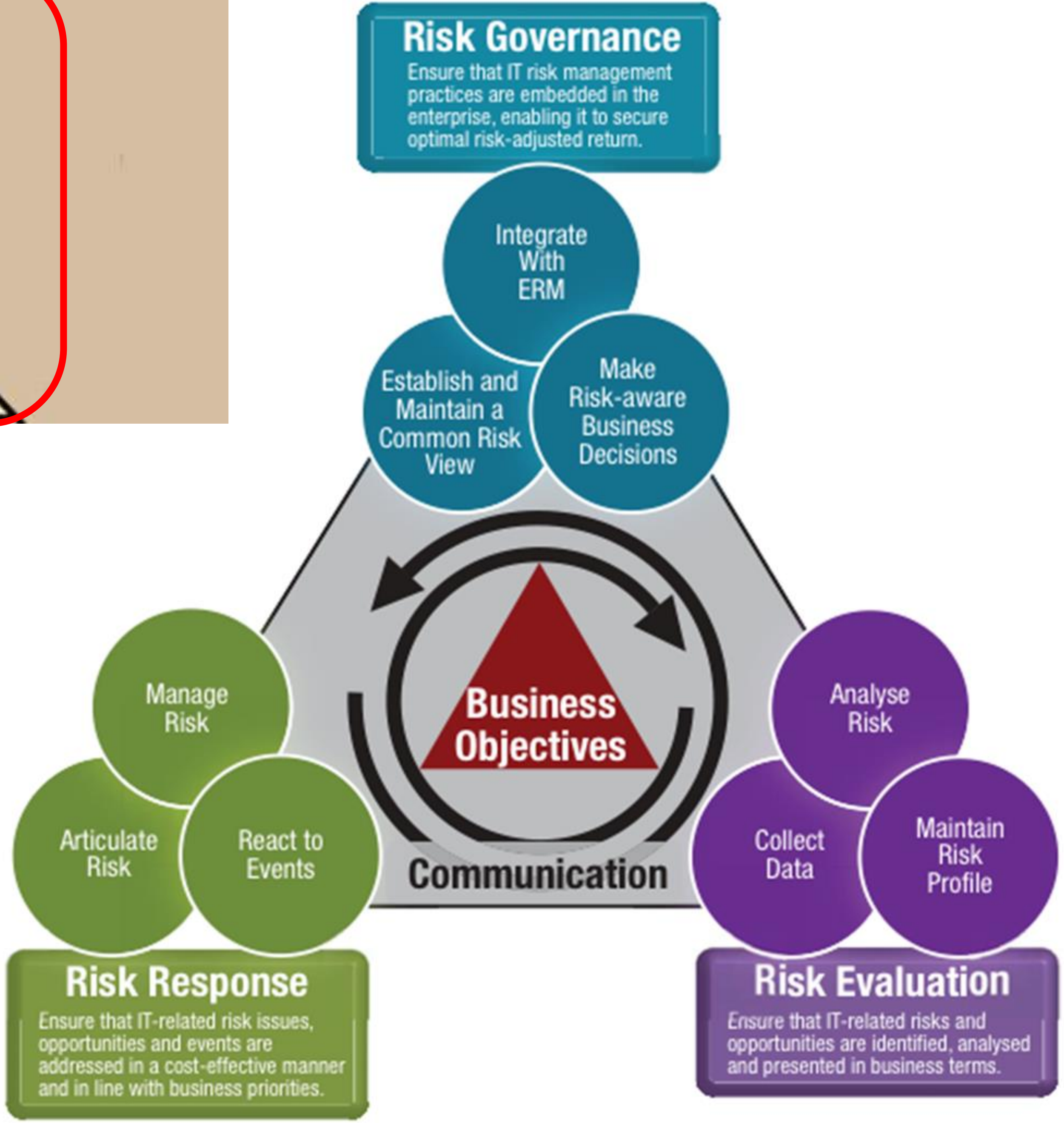
TIER 3
INFORMATION SYSTEM
(Environment of Operation)

STRATEGIC RISK

TACTICAL RISK


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

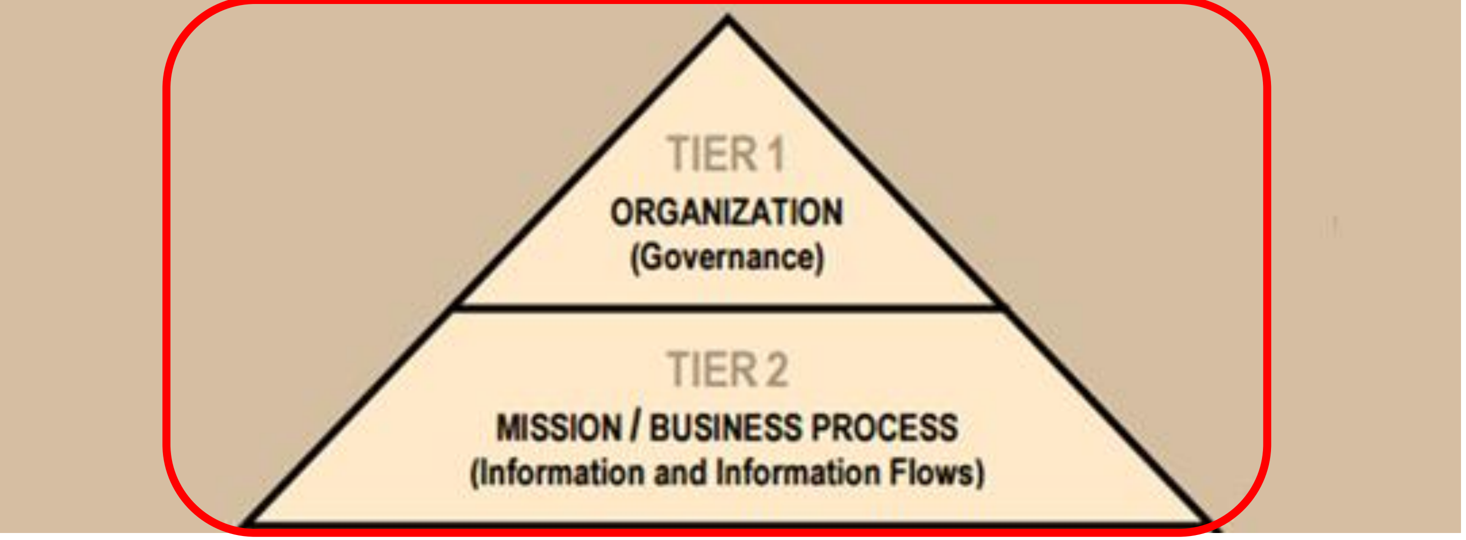


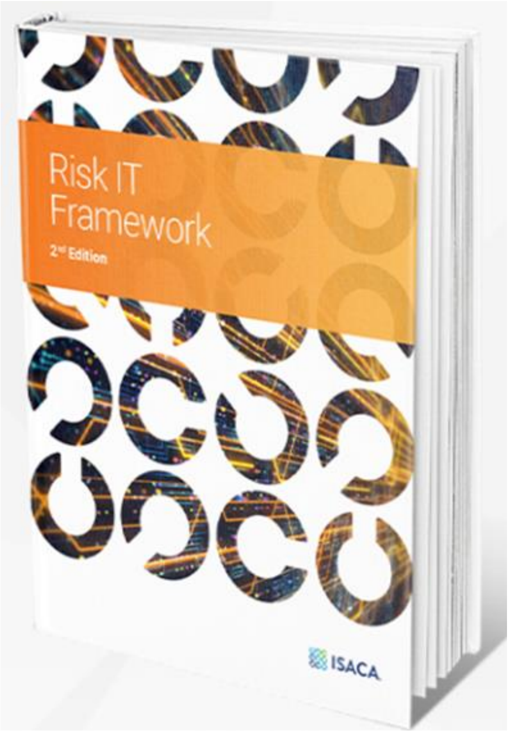


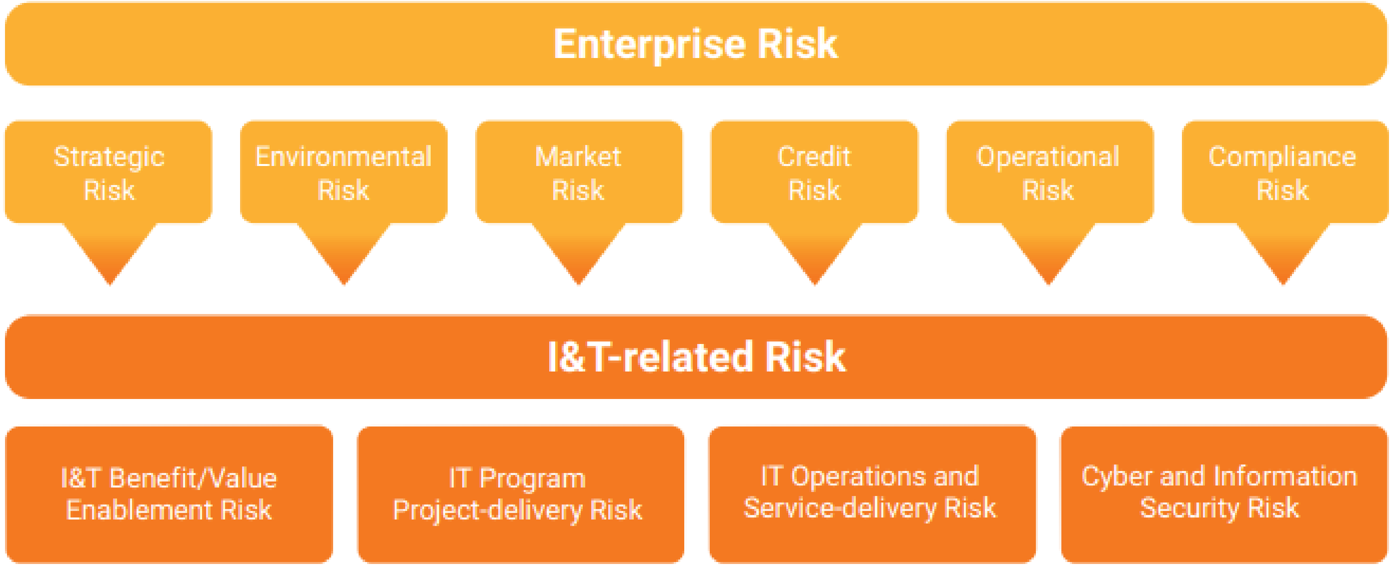
Risk Governance: Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.

Risk Response: Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

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)





Enterprise Risk

Strategic Risk

Environmental Risk

Market Risk

Credit Risk

Operational Risk

Compliance Risk

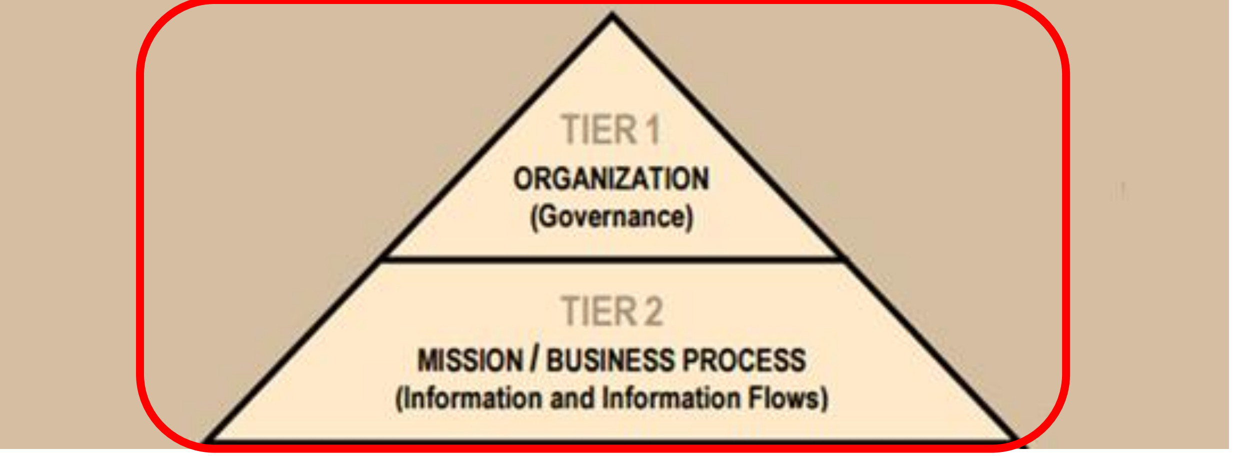
I&T-related Risk

I&T Benefit/Value Enablement Risk

IT Program Project-delivery Risk

IT Operations and Service-delivery Risk

Cyber and Information Security Risk



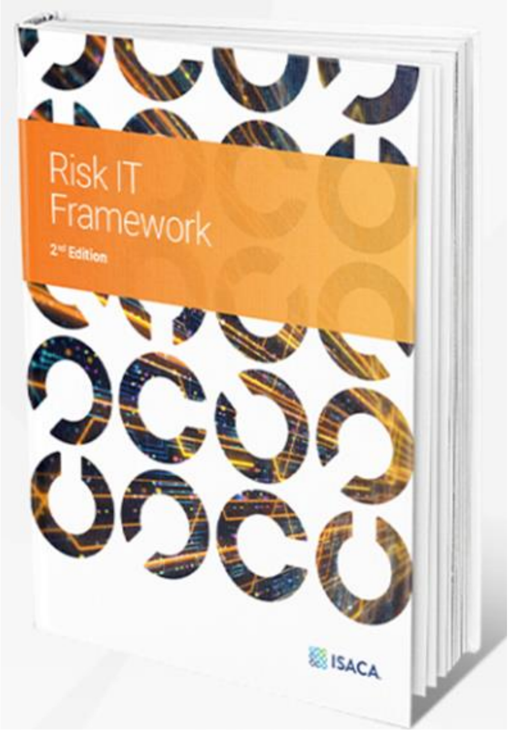
TIER 1

ORGANIZATION
(Governance)

TIER 2

MISSION / BUSINESS PROCESS
(Information and Information Flows)

- **Risk Capacity** = “objective magnitude or amount of loss than an enterprise can tolerate without risking its continued existence”
- **Risk Appetite** “generally reflects a board or management decision regarding how much risk is desirable”



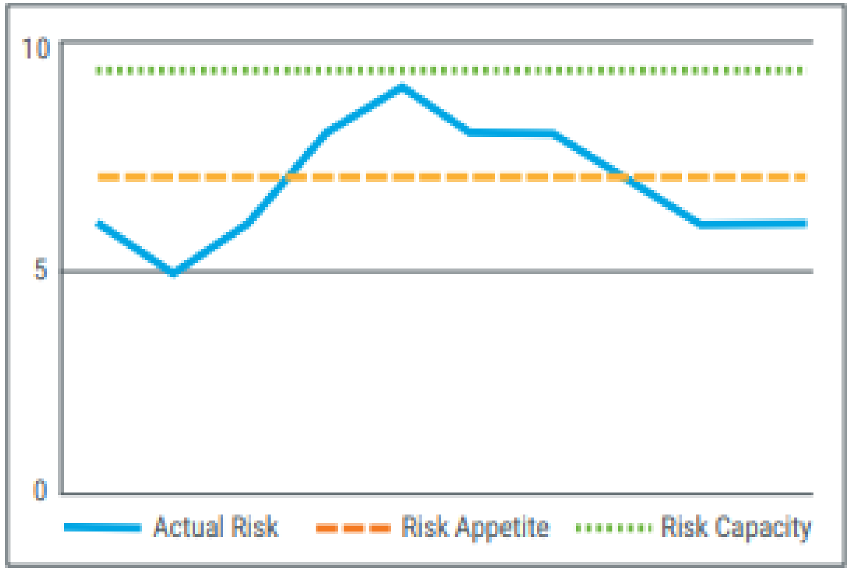


Diagram show a relatively sustainable situation

- Risk appetite is lower than risk capacity
- Actual risk exceeds risk appetite, but remains below risk capacity

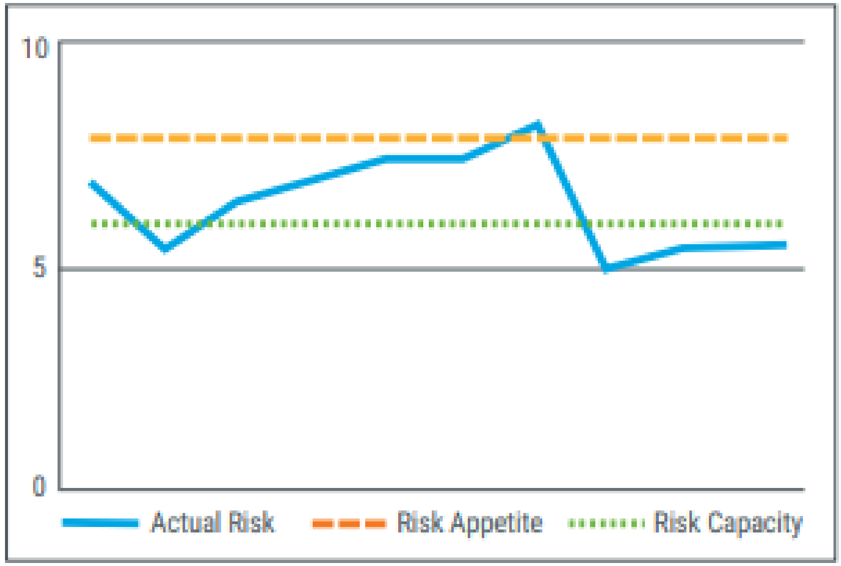
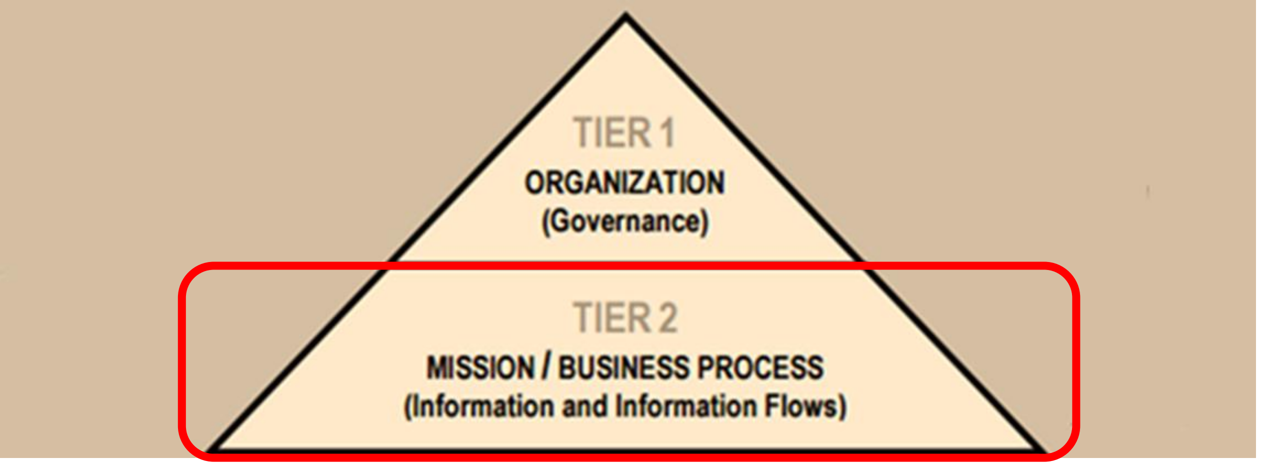
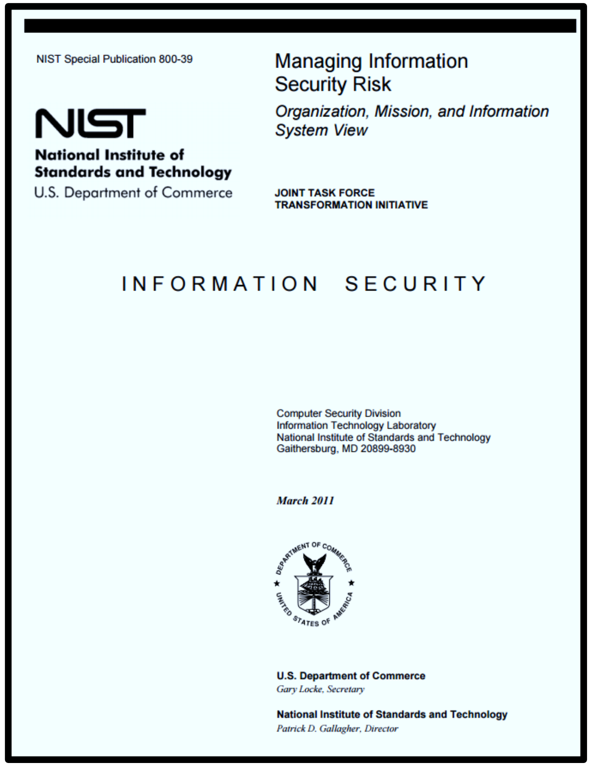


Diagram show an unsustainable situation

- Risk appetite is defined by management as a level beyond risk capacity (i.e. management is OK to accept risk and absorb loss)
- Actual risk routinely exceeds risk capacity, despite remaining below risk appetite level most of the time


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


NIST Special Publication 800-39

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

Managing Information
Security Risk

*Organization, Mission, and Information
System View*

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

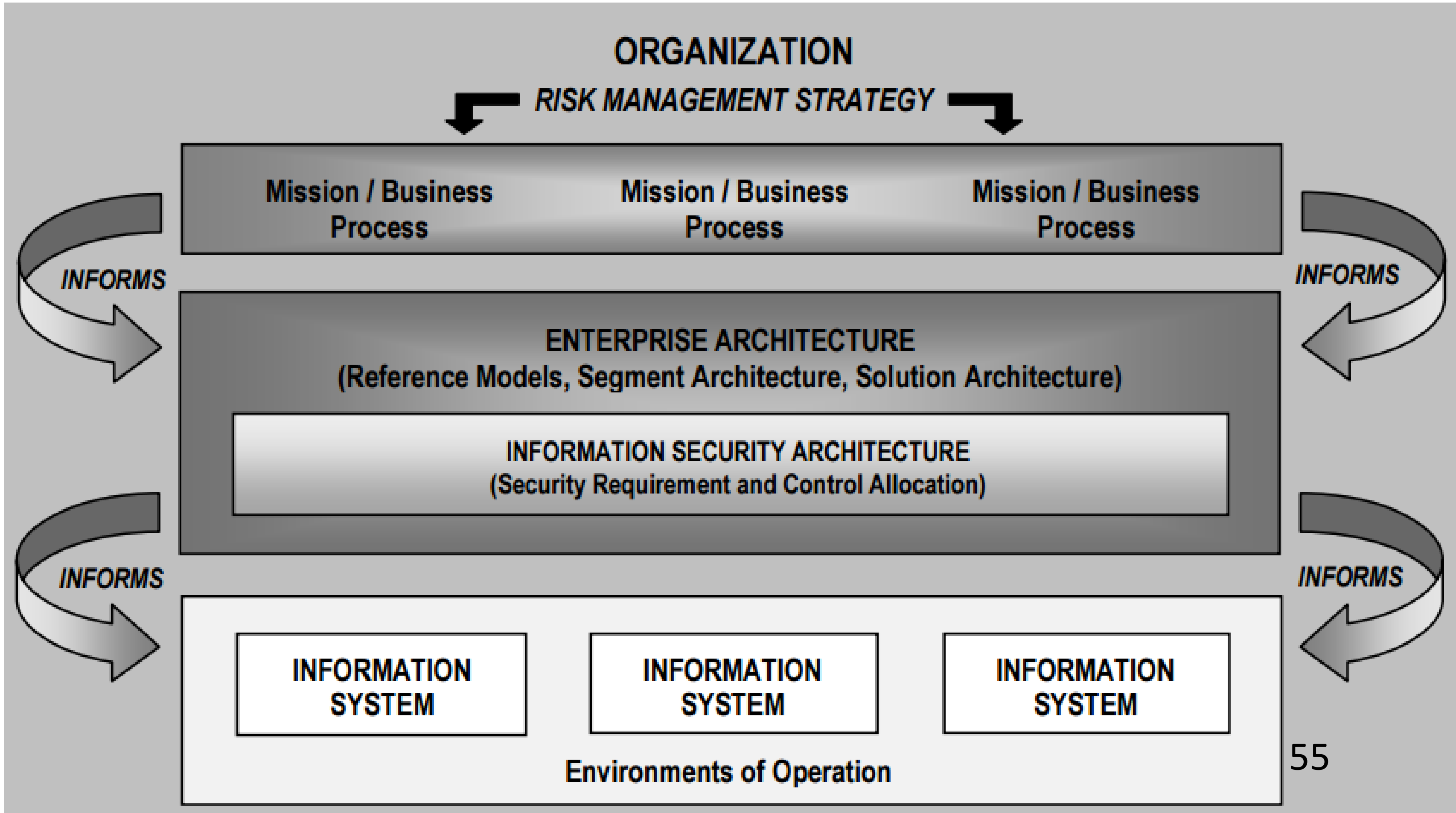
INFORMATION SECURITY

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

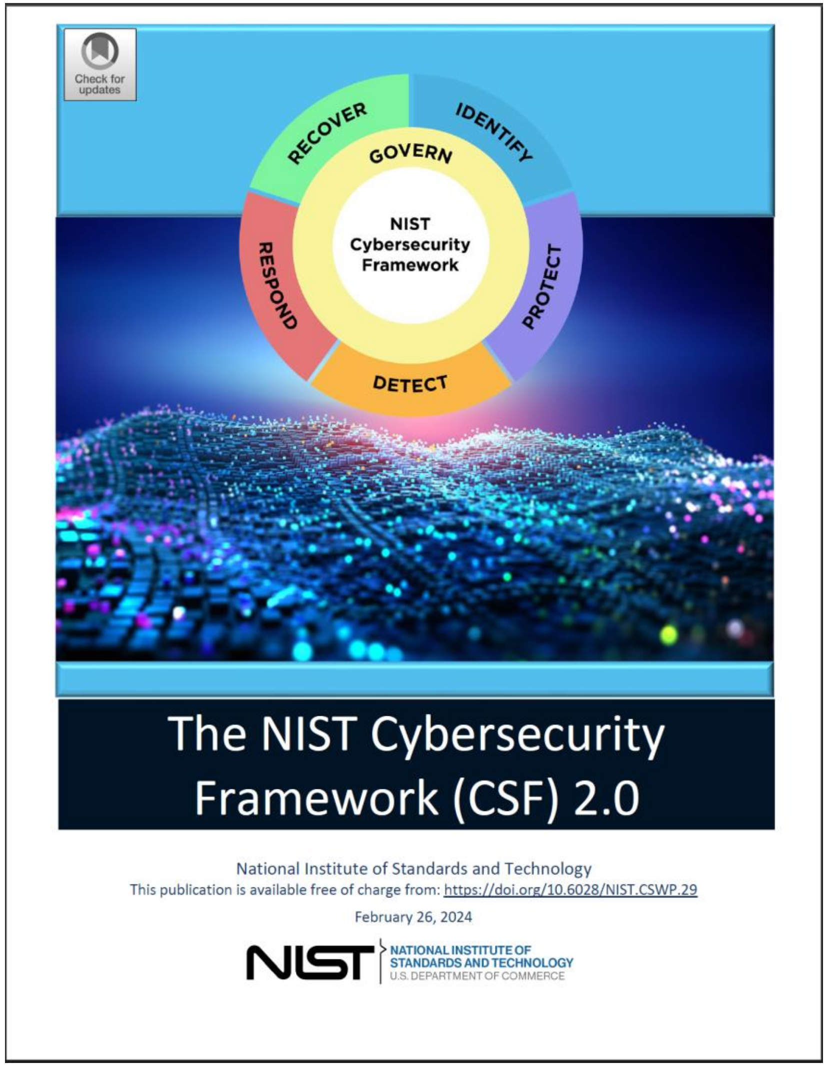
March 2011

U.S. Department of Commerce
Gary Locke, Secretary

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


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

NIST Cybersecurity Framework



The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29

February 26, 2024

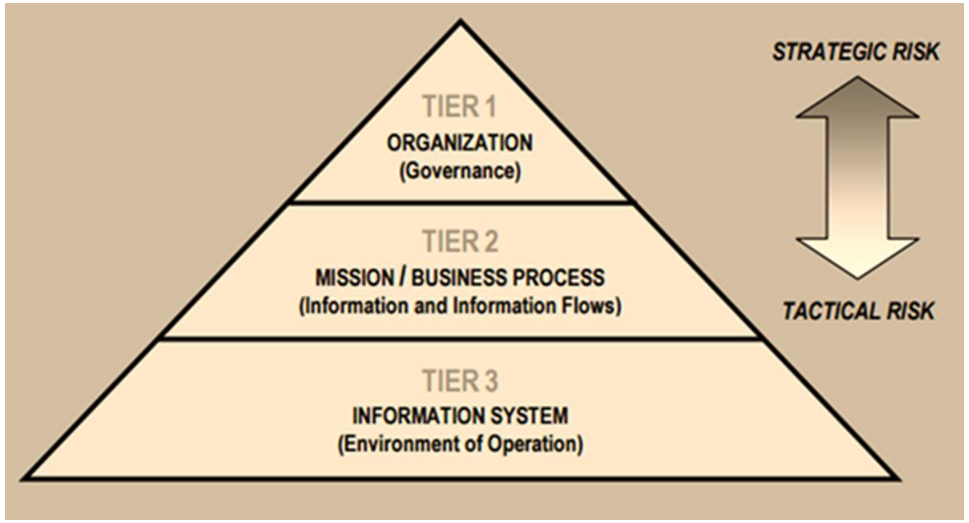
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

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


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

NIST Cybersecurity Framework

What is the organization’s cybersecurity risk management strategy, expectations, and policy?

What assets need protection?

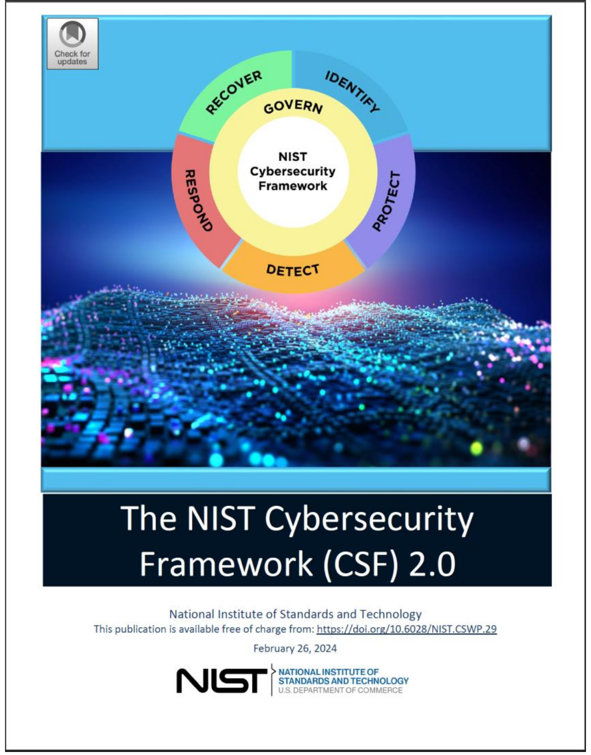
What safeguards are available?

What techniques can detect incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

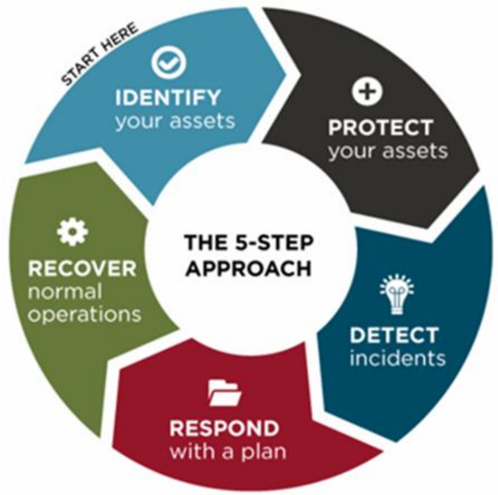


The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29

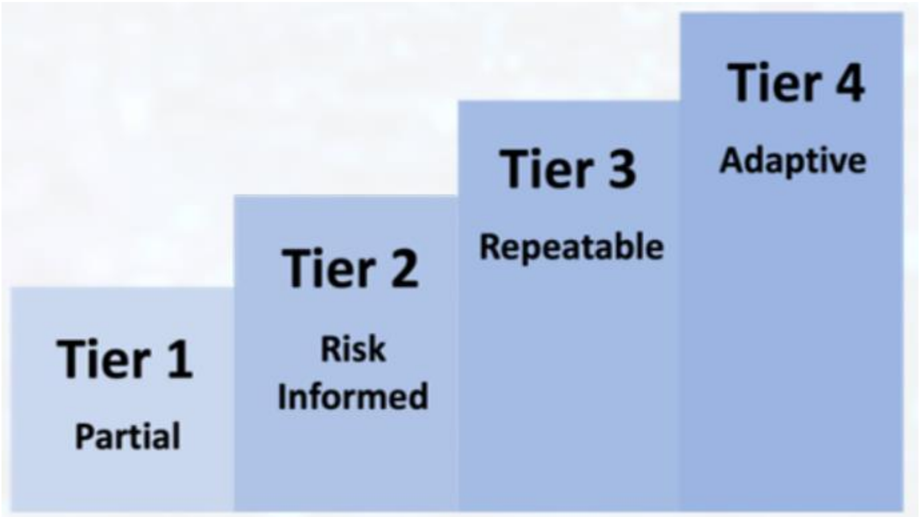
February 26, 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



NIST Cybersecurity Framework

Cybersecurity Framework Tiers



A characterization of the rigor of an organization’s cybersecurity risk governance and management practices

Tier 1: Partial

- Organizational cybersecurity risk strategy, prioritization, and management is ad hoc and not based on objectives nor threat environment

Tier 2: Risk Informed

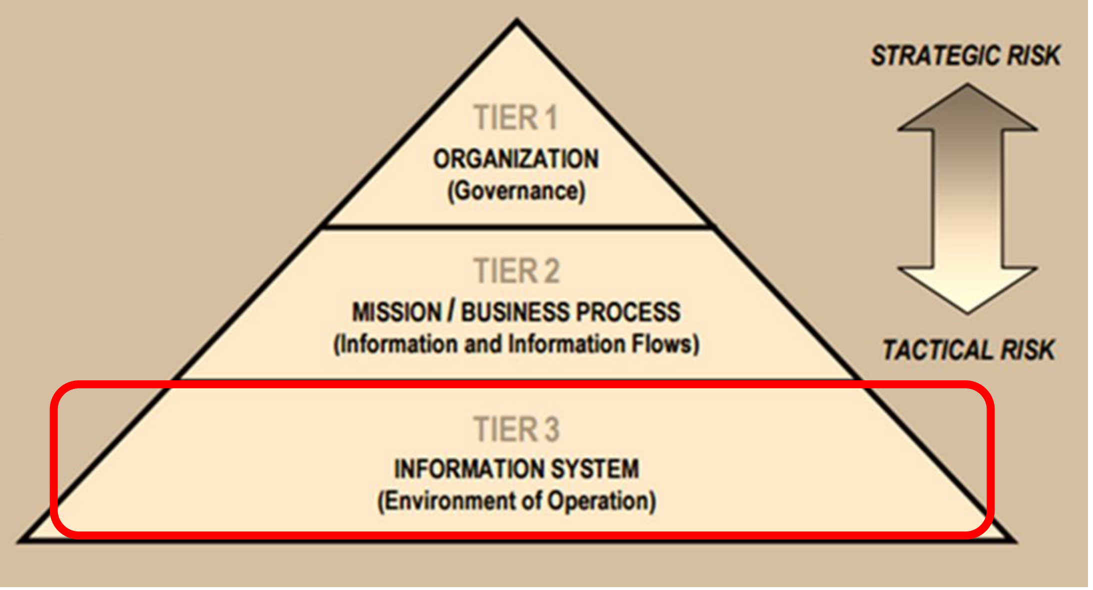
- There is awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks is not established.

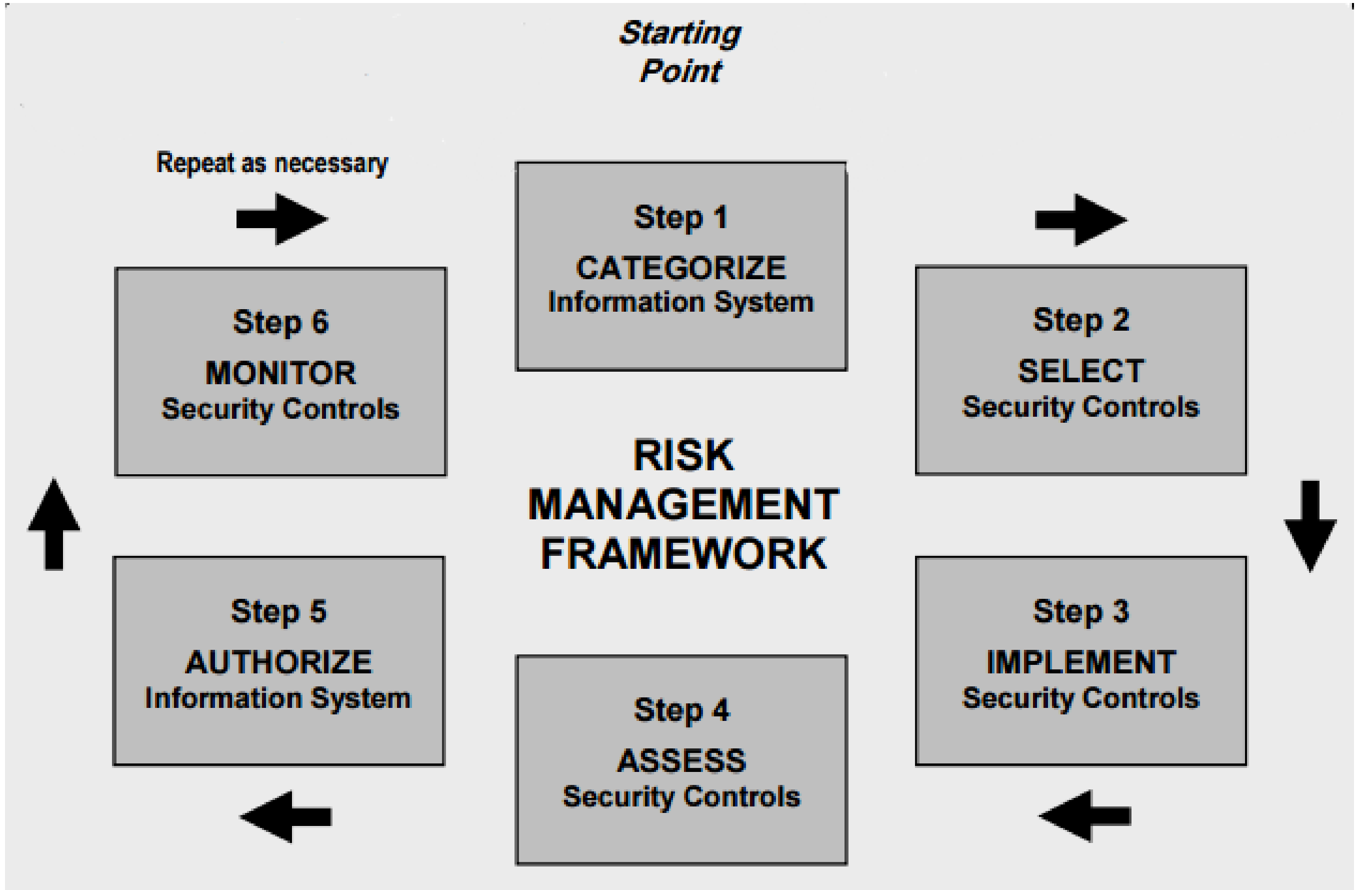
Tier 3: Repeatable

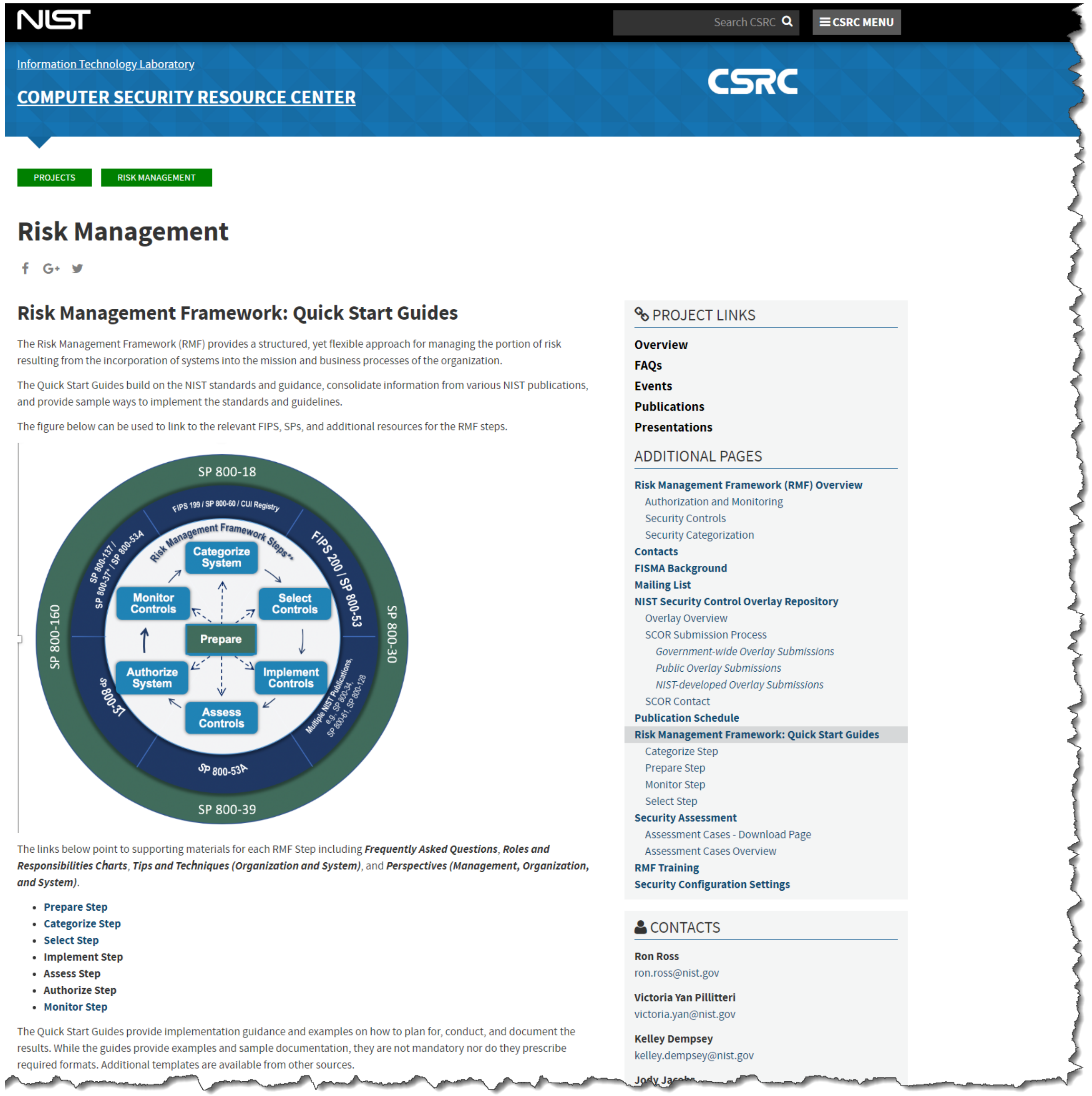
- Organization risk management practices are formally expressed as policy and in place to manage cybersecurity risks.

Tier 4: Adaptive

- Cybersecurity risk management is part of the organizational culture. The organization adapts its cybersecurity practices based on experience with previous and current cybersecurity activities, lessons learned, predictive indicators, advances in technology, and changes in the threat environment.


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

Search CSRC

☰ CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

PROJECTS | RISK MANAGEMENT

Risk Management

Risk Management Framework: Quick Start Guides

The Risk Management Framework (RMF) provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of systems into the mission and business processes of the organization.

The Quick Start Guides build on the NIST standards and guidance, consolidate information from various NIST publications, and provide sample ways to implement the standards and guidelines.

The figure below can be used to link to the relevant FIPS, SPs, and additional resources for the RMF steps.

The links below point to supporting materials for each RMF Step including ***Frequently Asked Questions***, ***Roles and Responsibilities Charts***, ***Tips and Techniques (Organization and System)***, and ***Perspectives (Management, Organization, and System)***.

- **Prepare Step**
- **Categorize Step**
- **Select Step**
- **Implement Step**
- **Assess Step**
- **Authorize Step**
- **Monitor Step**

The Quick Start Guides provide implementation guidance and examples on how to plan for, conduct, and document the results. While the guides provide examples and sample documentation, they are not mandatory nor do they prescribe required formats. Additional templates are available from other sources.

PROJECT LINKS

Overview
FAQs
Events
Publications
Presentations

ADDITIONAL PAGES

Risk Management Framework (RMF) Overview
Authorization and Monitoring
Security Controls
Security Categorization
Contacts
FISMA Background
Mailing List
NIST Security Control Overlay Repository
Overlay Overview
SCOR Submission Process
Government-wide Overlay Submissions
Public Overlay Submissions
NIST-developed Overlay Submissions
SCOR Contact
Publication Schedule
Risk Management Framework: Quick Start Guides
Categorize Step
Prepare Step
Monitor Step
Select Step
Security Assessment
Assessment Cases - Download Page
Assessment Cases Overview
RMF Training
Security Configuration Settings

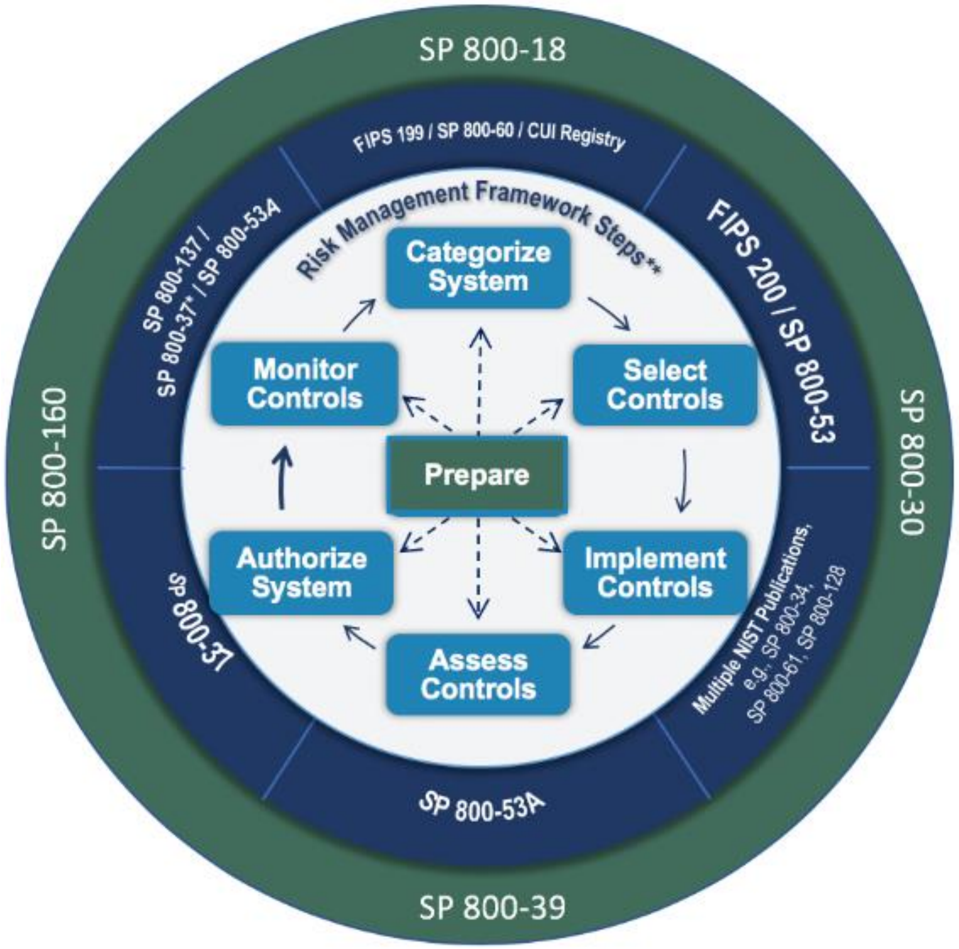
CONTACTS

Ron Ross
ron.ross@nist.gov

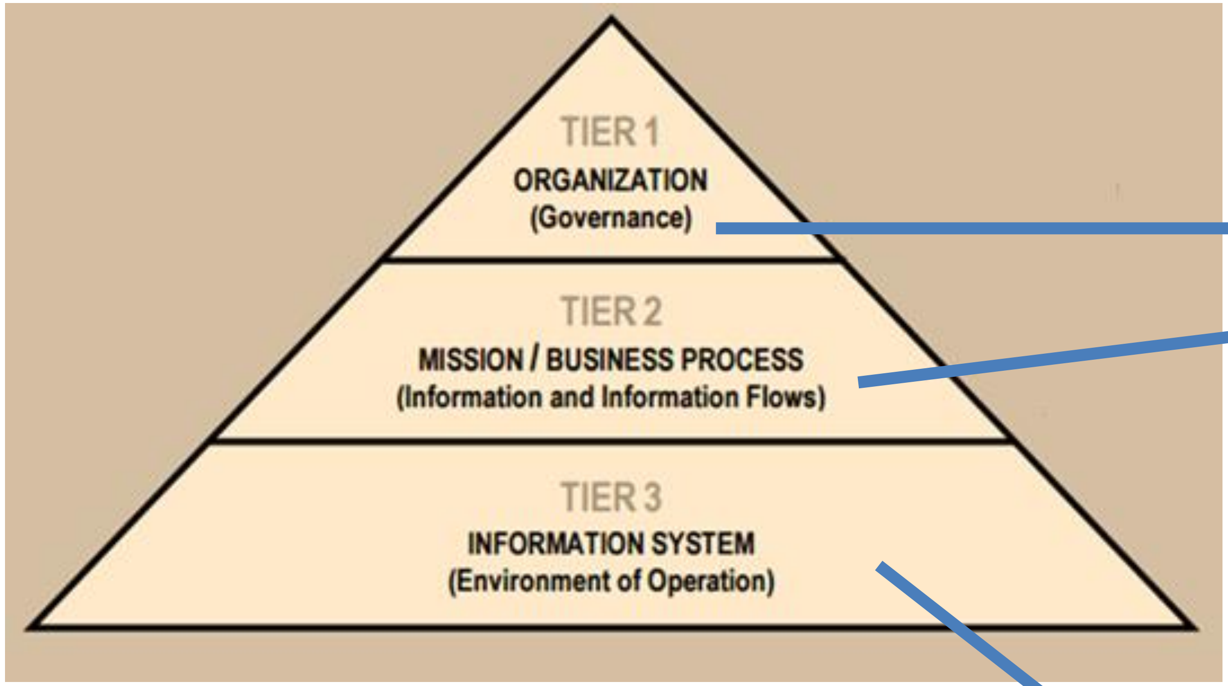
Victoria Yan Pillitteri
victoria.yan@nist.gov

Kelley Dempsey
kelley.dempsey@nist.gov

Jody Jacobs



In summary…

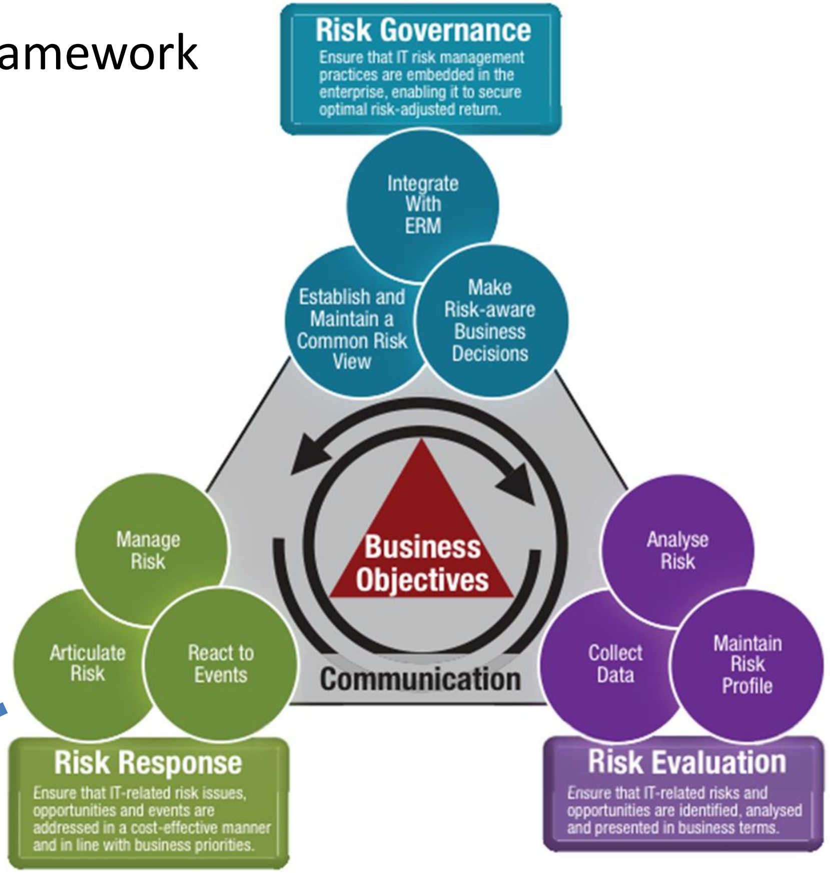


TIER 1
ORGANIZATION
(Governance)

TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)

TIER 3
INFORMATION SYSTEM
(Environment of Operation)

The RiskIT Framework



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.

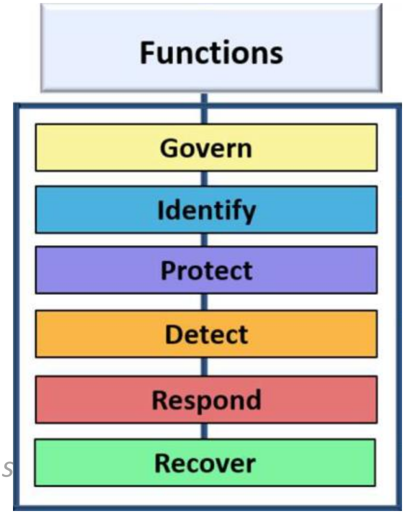
Analyse Risk

Collect Data

Maintain Risk Profile

Risk Evaluation
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

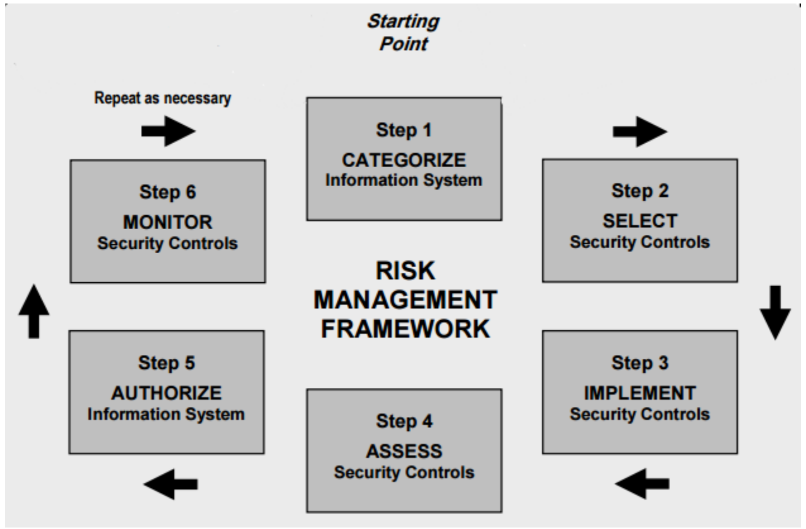
NISTCybersecurity
Framework



Functions

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

NIST
Risk Management
Framework



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

Next time:

Case Study #1 “Snowfall and a stolen laptop…”

Data Classification Process and Models

Ashok Rao

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 #1b

Understanding an Organization’s Risk Environment