

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: “Framework for Improving Critical Infrastructure Cybersecurity”
- 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

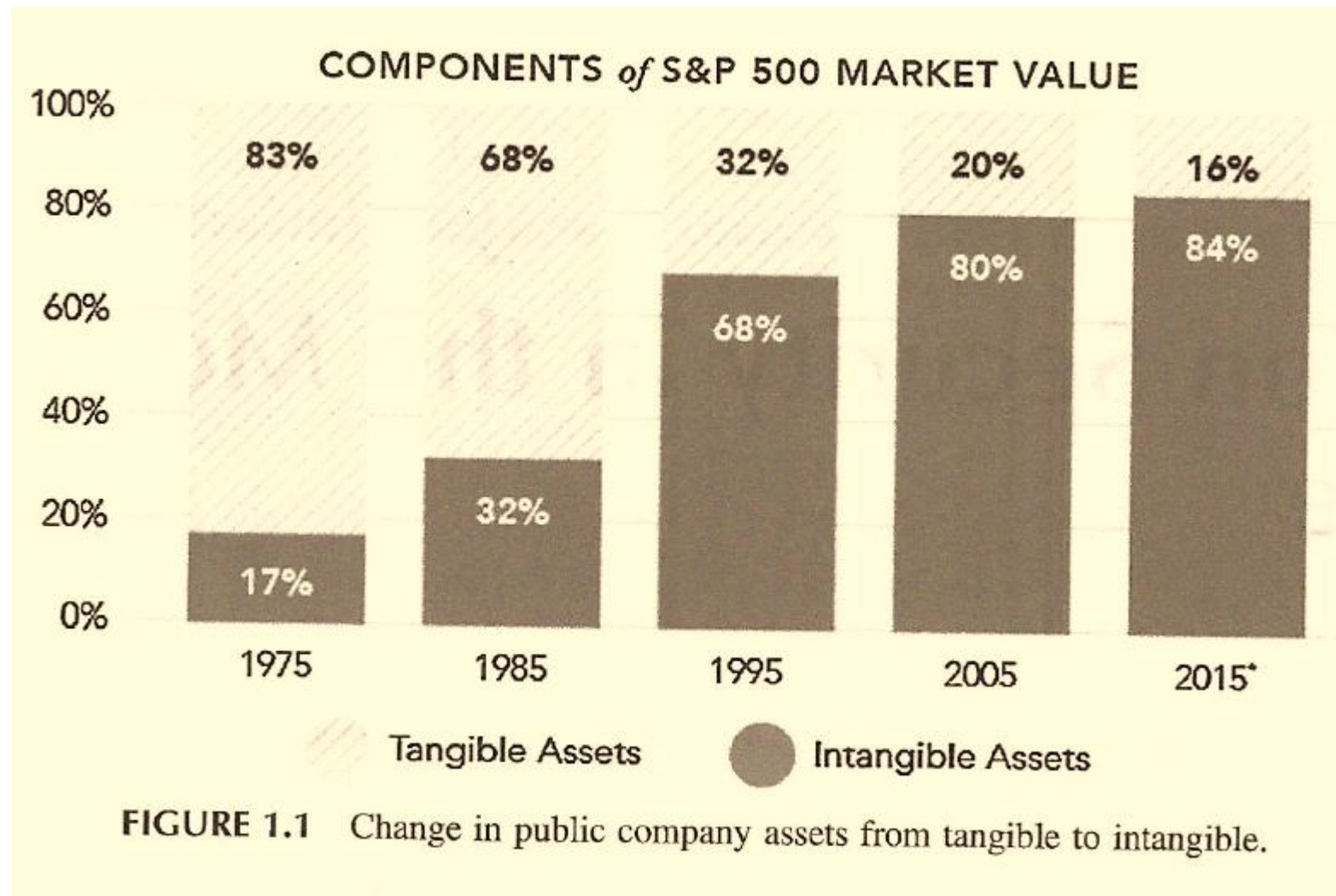
The value of business' data is at a peak

“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

MIS 5206 Protecting Information Assets



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



Type of Threat Source	Description	Characteristics
ADVERSARIAL <ul style="list-style-type: none"> - Individual <ul style="list-style-type: none"> - Outsider - Insider - Trusted Insider - Privileged Insider - Group <ul style="list-style-type: none"> - Ad hoc - Established - Organization <ul style="list-style-type: none"> - Competitor - Supplier - Partner - Customer - Nation-State 	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. Persistence

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

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

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

(McAfee, 2011)

Anatomy of an Attack

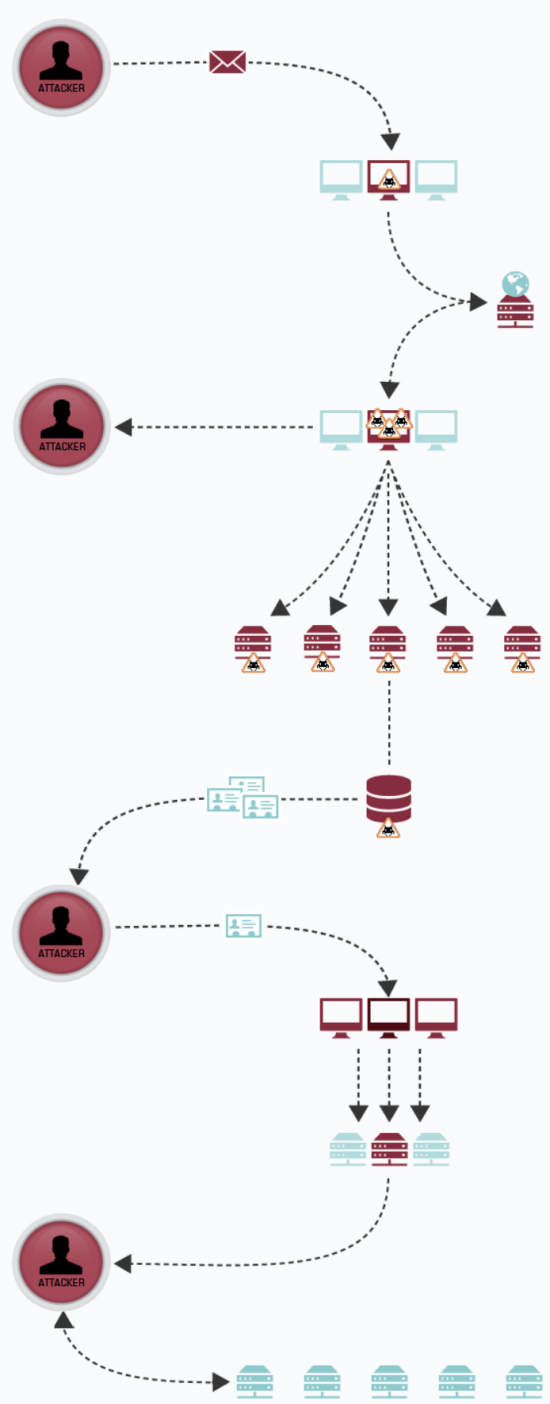
(MANDIANT, 2015)

Threat landscape

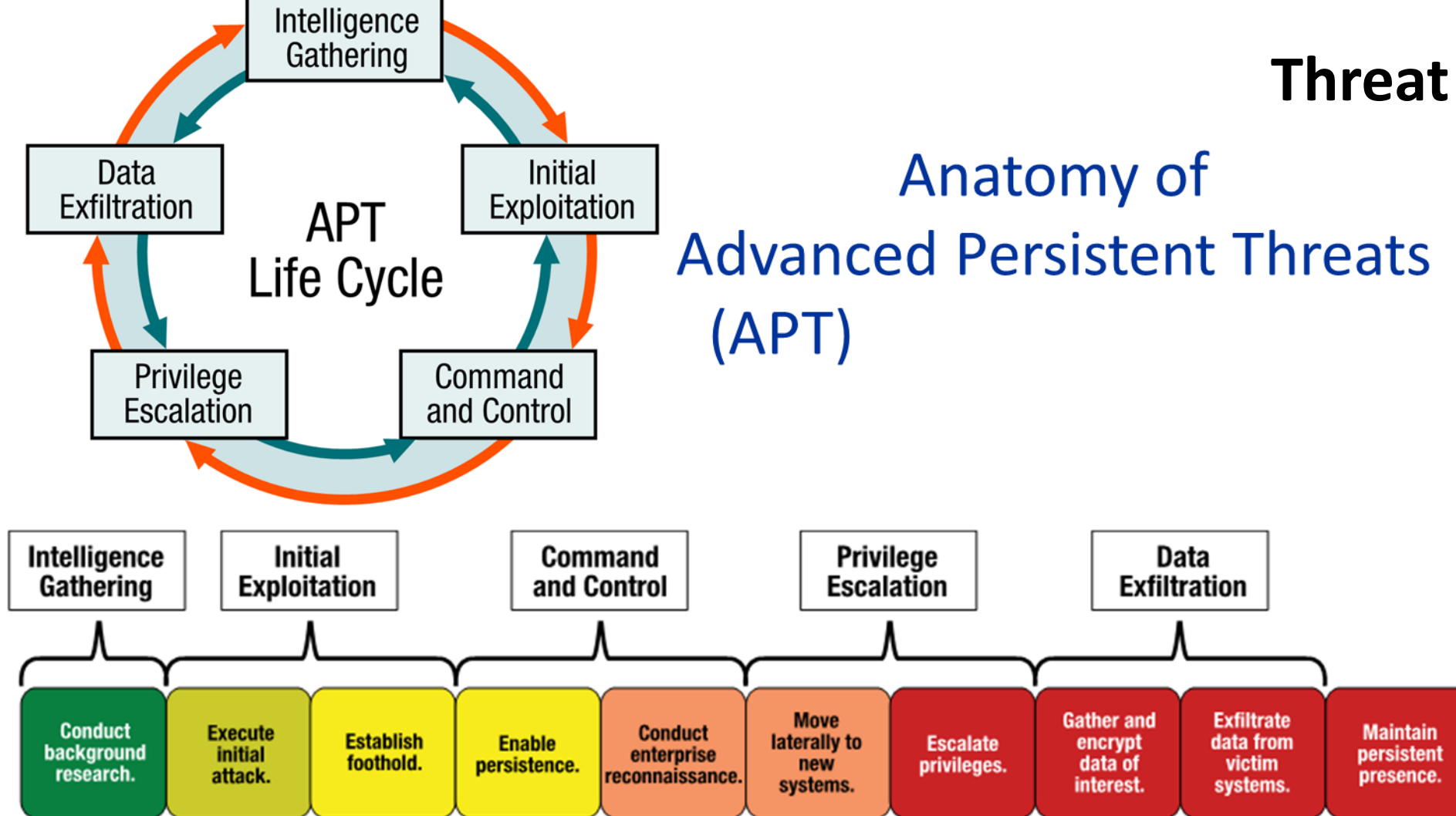
1. Attacker sends spear fishing e-mail
 - Custom malware is installed
2. Victim opens attachment
 - Custom malware communicates to control web site
3. Custom malware communicates to control web site
 - Pulls down additional malware
4. Attacker establishes multiple backdoors
5. Attacker accesses system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

Assets

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



Anatomy of Advanced Persistent Threats (APT)



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

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

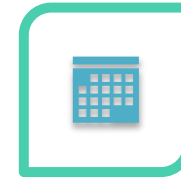
NIST SP 800-30r1 "Guide for Conducting Risk Assessments", page 66



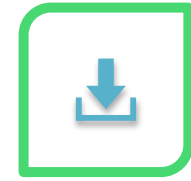
Human non-malicious threat examples and causes



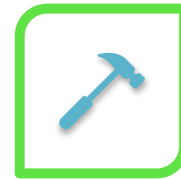
COMPUTER
OPERATOR
ERRORS



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

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

MIS 5206 Protecting Information Assets



Structural Threat Examples

- Air conditioning failure
- Building collapse
- 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)
- ...

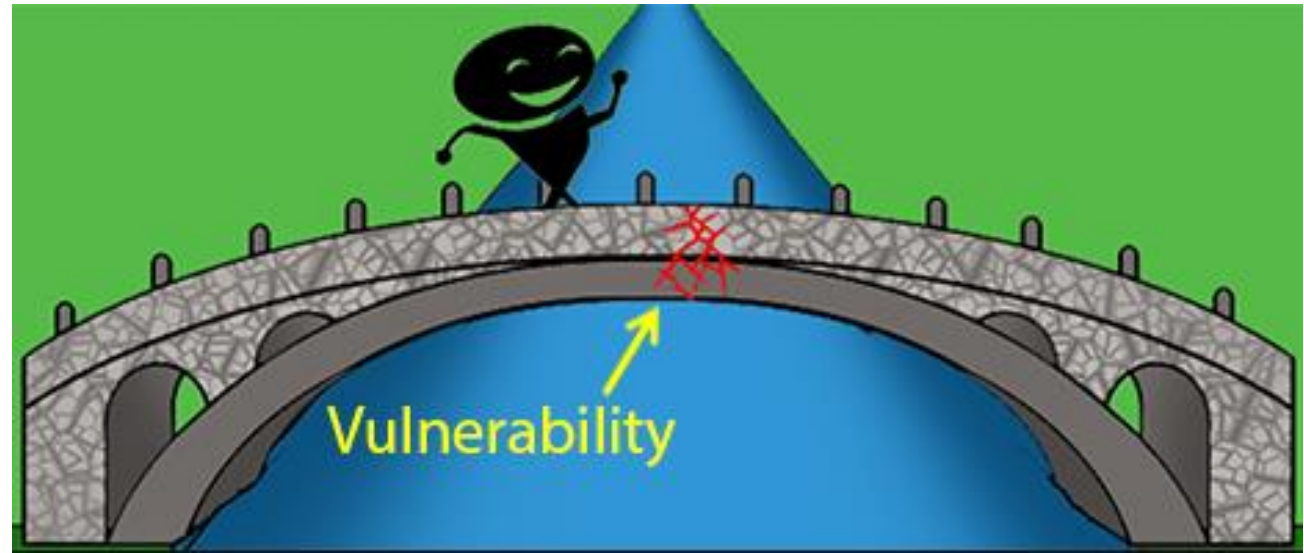
Taxonomy of cybersecurity threat sources

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

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

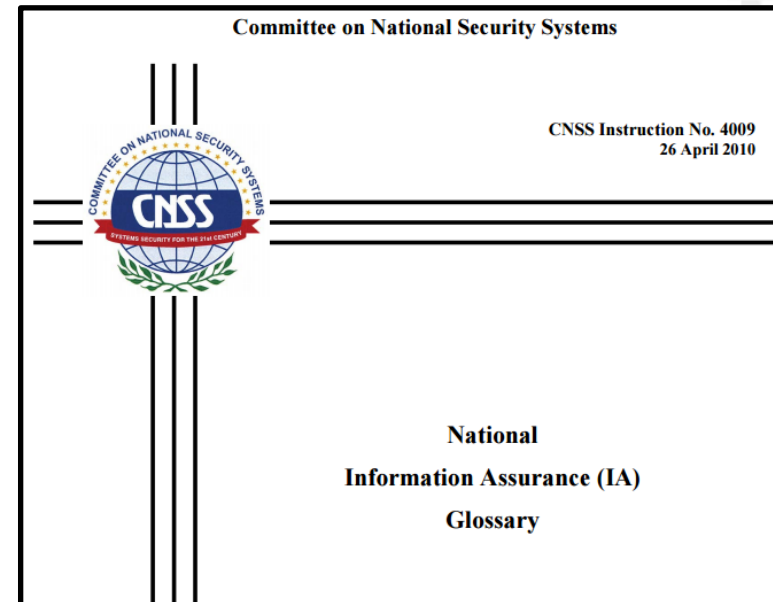
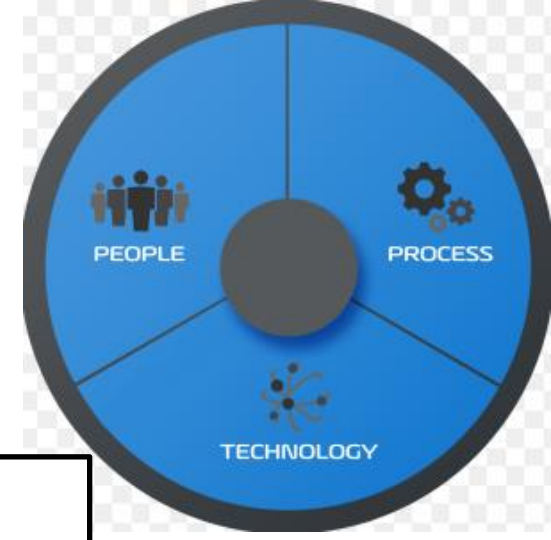


What is a Vulnerability?



What is a Vulnerability?

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



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

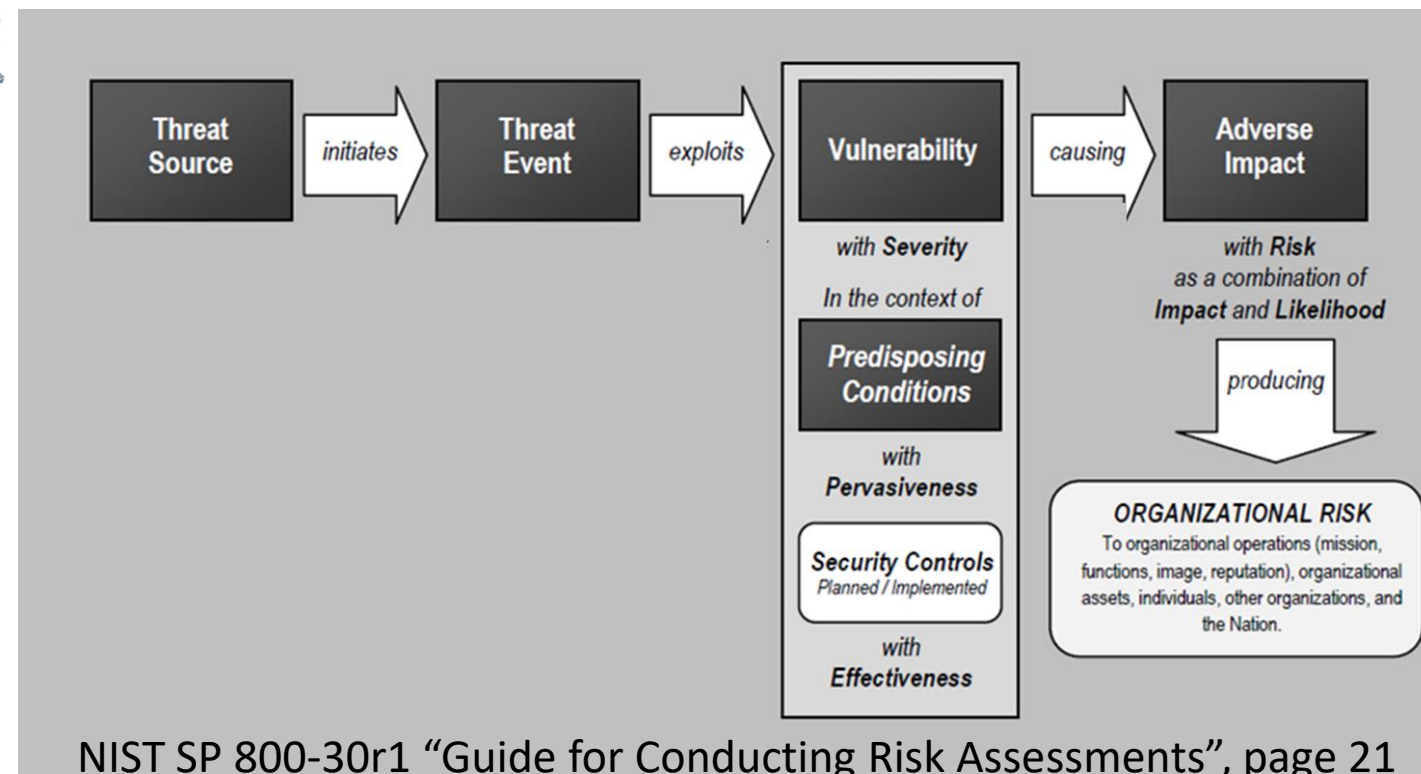


- Loss of life
- Losses due to fraud, theft, larceny, bribery
- Impact of
 - lost competitive edge
 - lost data
 - lost time
 - lost productivity
 - lost business

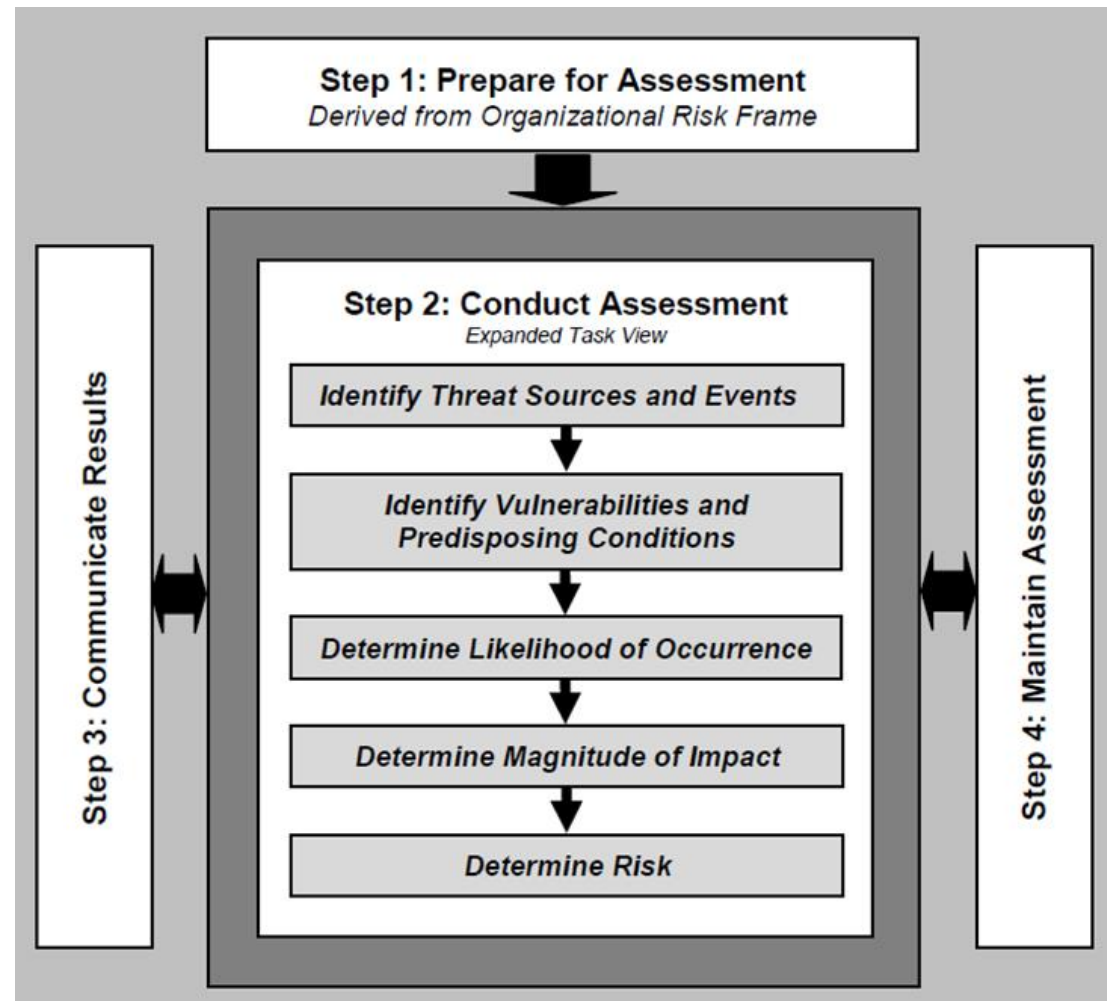
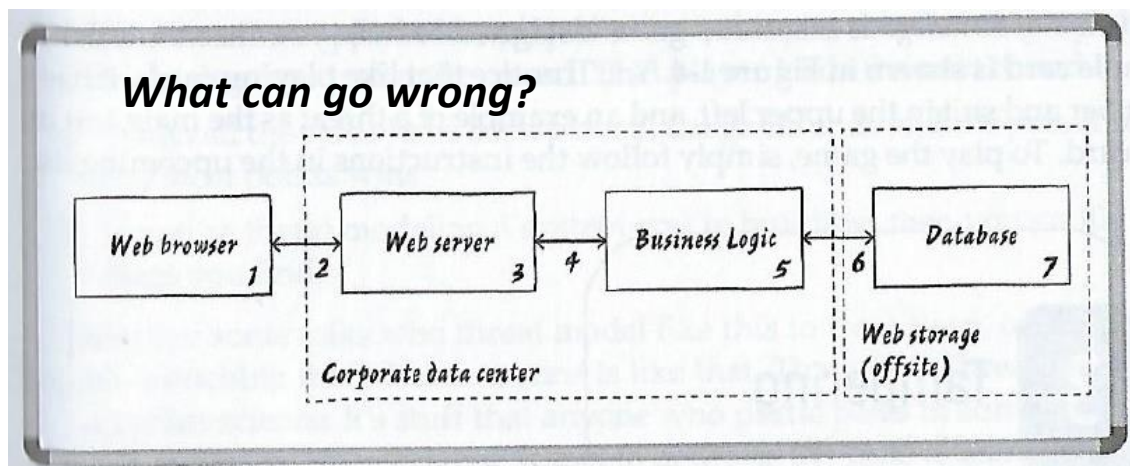
- Bankruptcy
- Business interruption
- Frustration
- Ill will
- Injury
- Impacts of inaccurate data

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



Process for Assessing IT risk



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

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)

$$\mathbf{ALE = SLE \times ARO}$$

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:

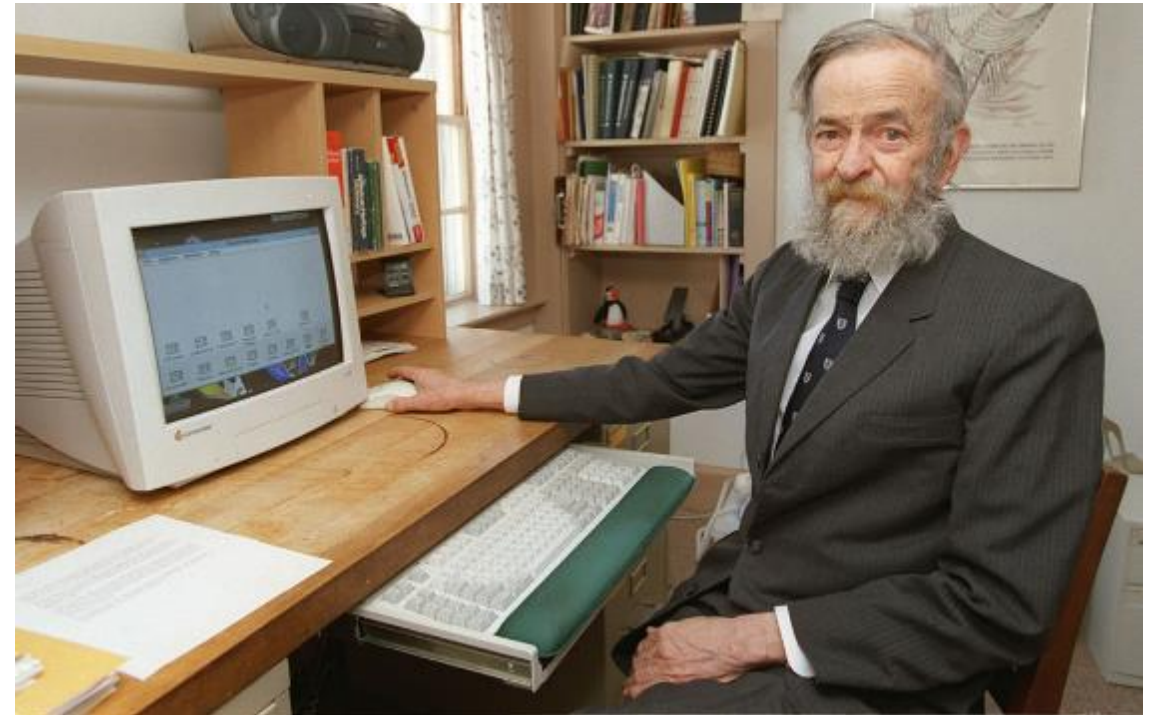
1. Avoidance
2. Acceptance
3. Transfer
4. Mitigation (“Controls”)

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*

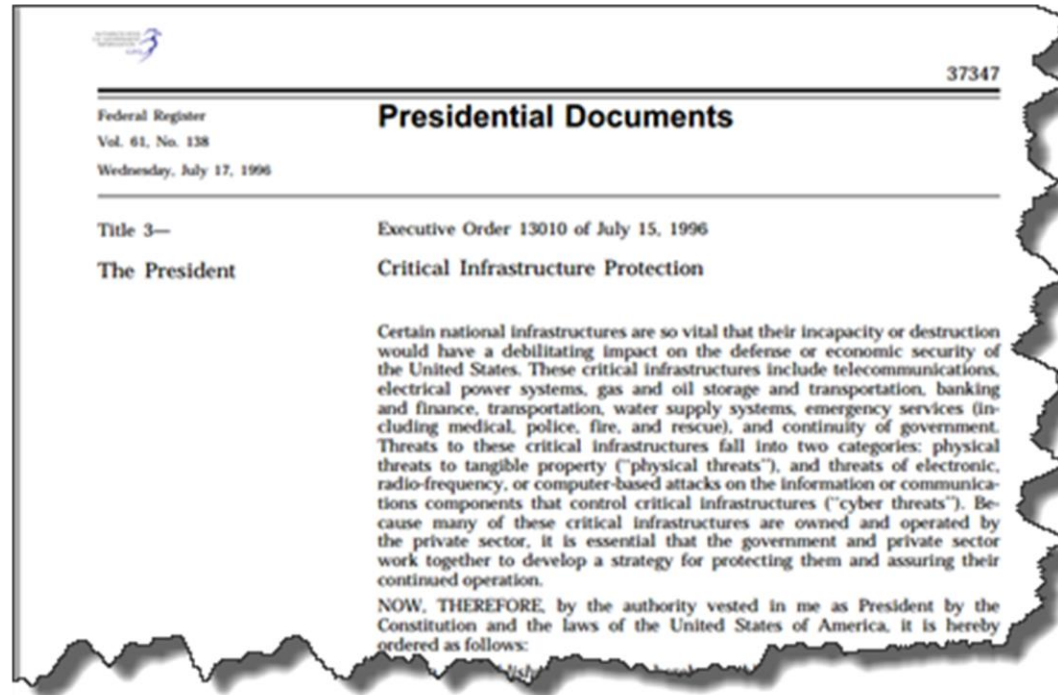
- Antivirus software
- Authentication/authorization servers
- Biometrics (thumbprints, retina scans, voice, face)
- Callback modems
- **Canine patrols**
- Card-activated locks
- Certificate authority
- *Code of sanctions against vendors/suppliers/contractors*
- *Color-coded ID badges*
- Content scanners
- 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



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

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



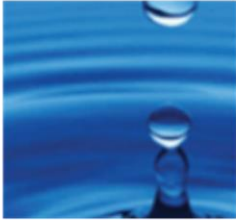
Energy



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

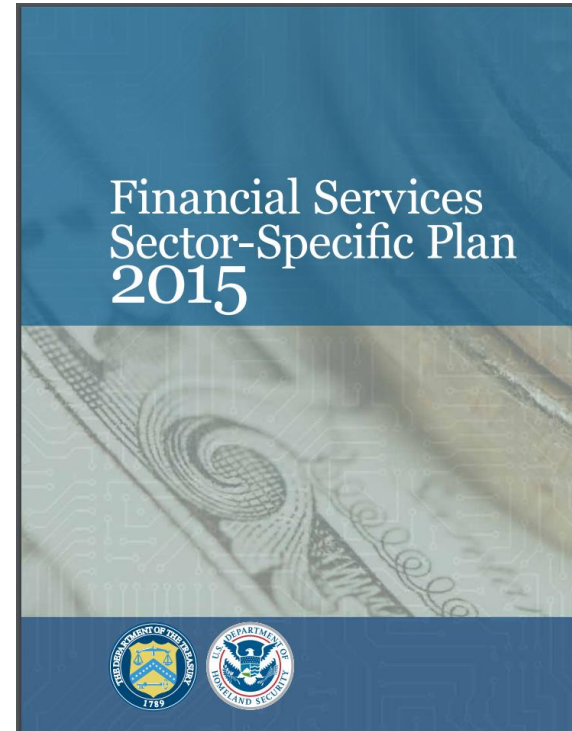
Protected System –any physical or computer-based system, information or data, process or procedure that directly or indirectly affects the viability of a facility or critical infrastructure



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

The screenshot shows the CISA website interface. At the top left is the CISA logo. To its right is a search bar and two buttons: 'COVID Questions' and 'Report Cyber Issue'. Below this is a navigation menu with icons for Cybersecurity, Infrastructure Security, Emergency Communications, National Risk Management, About CISA, and Media. The main content area is titled 'National Infrastructure Protection Plan' and includes a description of the plan's purpose. A left sidebar contains a 'Supporting Policy and Doctrine' section with a dropdown menu for 'National Infrastructure Protection Plan'. Below this is a 'National Infrastructure Protection Plan' section with a link to 'NIPP Security and Resilience Challenge'. A red arrow points to the 'Sector-Specific Plans' link in the sidebar. The main content area lists several links with green plus signs: 'NIPP 2013 Partnering for Critical Infrastructure Security and Resilience', 'NIPP 2013 Supplements', '2017 NIPP Security and Resilience Challenge', 'Sector-Specific Plans', 'More on the National Infrastructure Protection Plan', 'Training Courses', and 'Authorities'.



Financial Services Sector-Specific Plan 2015

Table of Contents

Introductory Comments.....	1
Executive Summary.....	3
Introduction.....	5
Sector Overview.....	6
Sector Profile.....	6
Deposit, Consumer Credit, and Payment Systems Products.....	6
Credit and Liquidity Products.....	7
Investment Products.....	7
Risk Transfer Products (Including Insurance).....	7
Sector Risks.....	8
Critical Infrastructure Partners.....	10
Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security Structure.....	11
Financial and Banking Information Infrastructure Committee Structure.....	11
Collaboration.....	12
Strategic Framework.....	13
Achieving Sector Goals.....	15
Information Sharing.....	15
Best Practices.....	16
Incident Response and Recovery.....	17
Policy Support.....	17
Measuring Effectiveness.....	18
Appendix A: Contribution of Sector Priorities to the Joint National Priorities and NIPP Goals..	19

Financial Services Sector-Specific Plan 2015

<i>Information Sharing</i>	
GOAL 1	<i>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.</i>
PRIORITY	<ol style="list-style-type: none"> 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.

<i>Best Practices</i>	
GOAL 2	<i>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.</i>
PRIORITY	<ol style="list-style-type: none"> 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.

<i>Incident Response and Recovery</i>	
GOAL 3	<i>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.</i>
PRIORITY	<ol style="list-style-type: none"> 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.

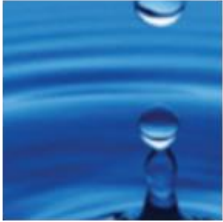
<i>Policy Support</i>	
GOAL 4	<i>Discuss policy and regulatory initiatives that advance infrastructure security and resilience priorities through robust coordination between government and industry.</i>
PRIORITY	<ol style="list-style-type: none"> 1. Identify, prioritize, and support government research 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



Water and
Wastewater
Systems



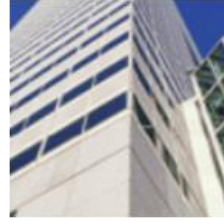
Dams



Emergency
Services



Commercial
Facilities



Nuclear
Reactors,
Materials, and
Waste



Defense
Industrial Base



Communications



Energy



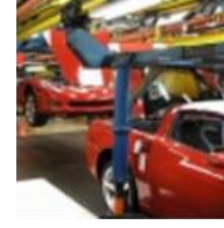
Chemical



Government
Facilities



Critical
Manufacturing



Healthcare
and Public
Health



Information
Technology



Food and
Agriculture



Financial
Services



Transportation sector - 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!



Critical Infrastructure Sectors

Transportation



Commercial
Facilities



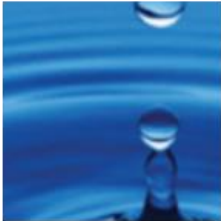
Energy



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

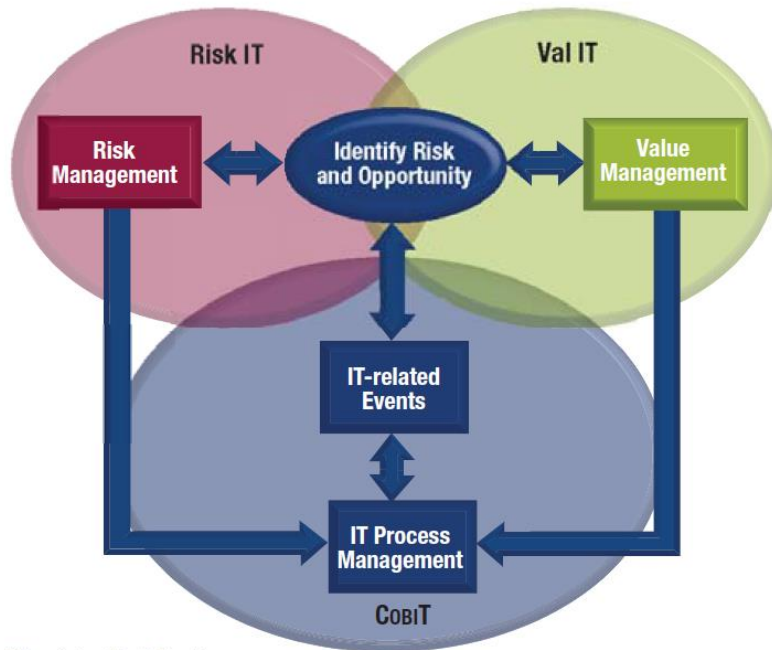
Vitek Boden worked for Hunter Watertech, an Australian firm that installed SCADA radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia (a rural area of great natural beauty and a tourist destination)

- 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



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 Information 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

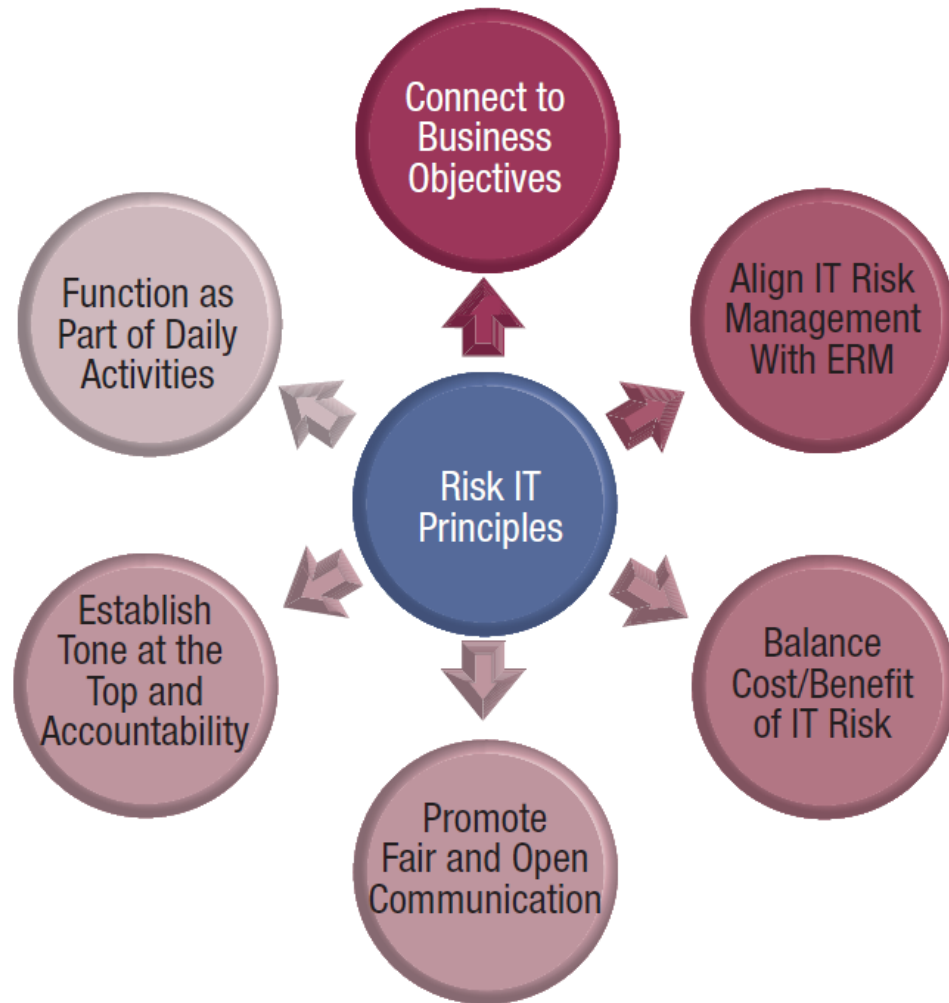
Groups key activities into three domains

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

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?



- 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)

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

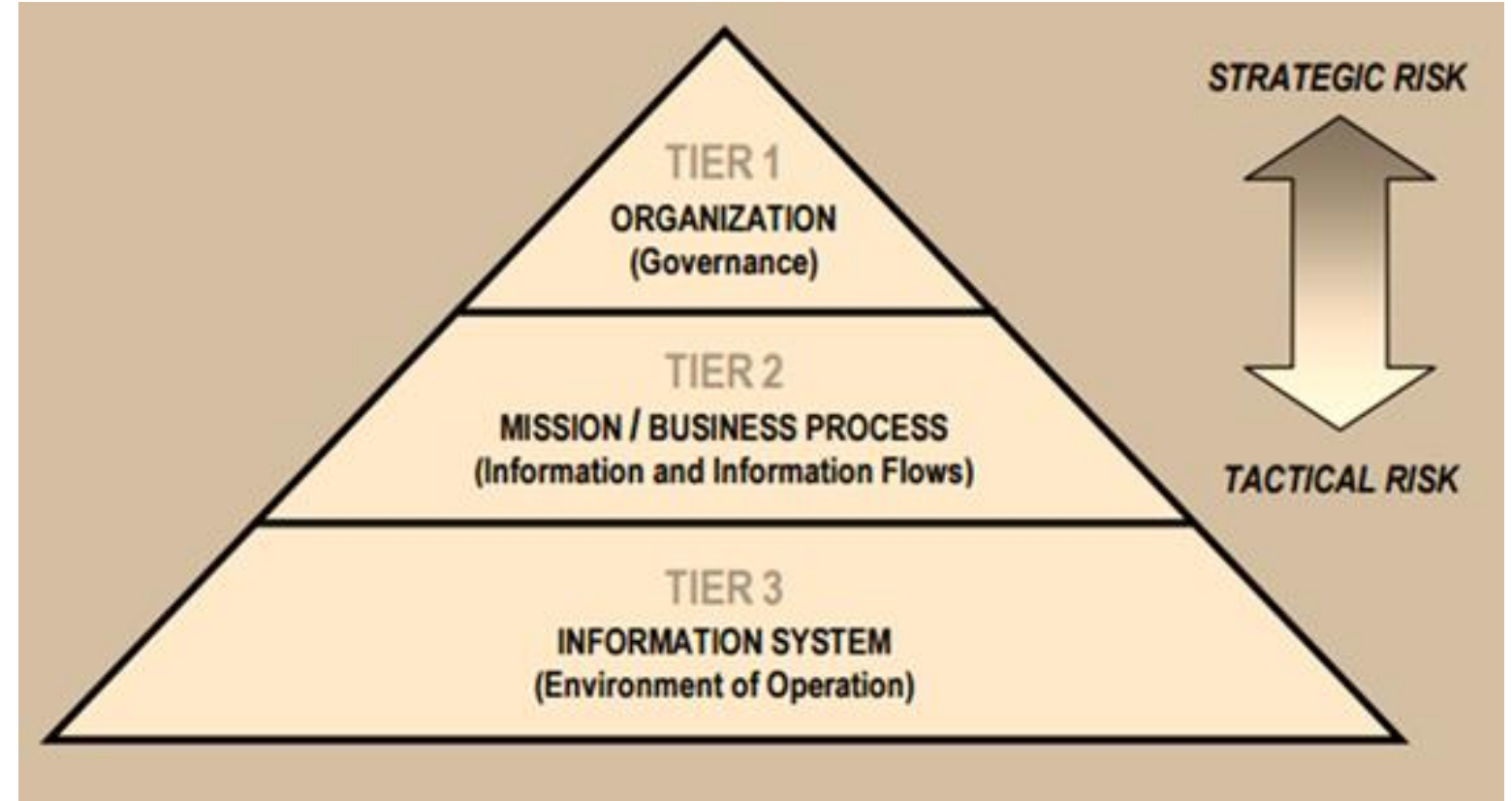
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

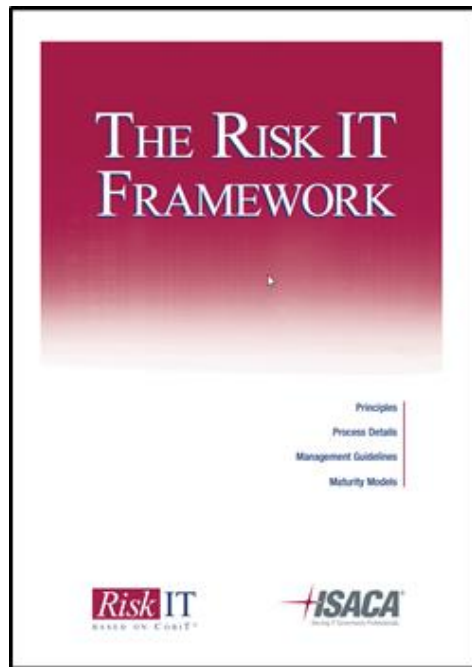
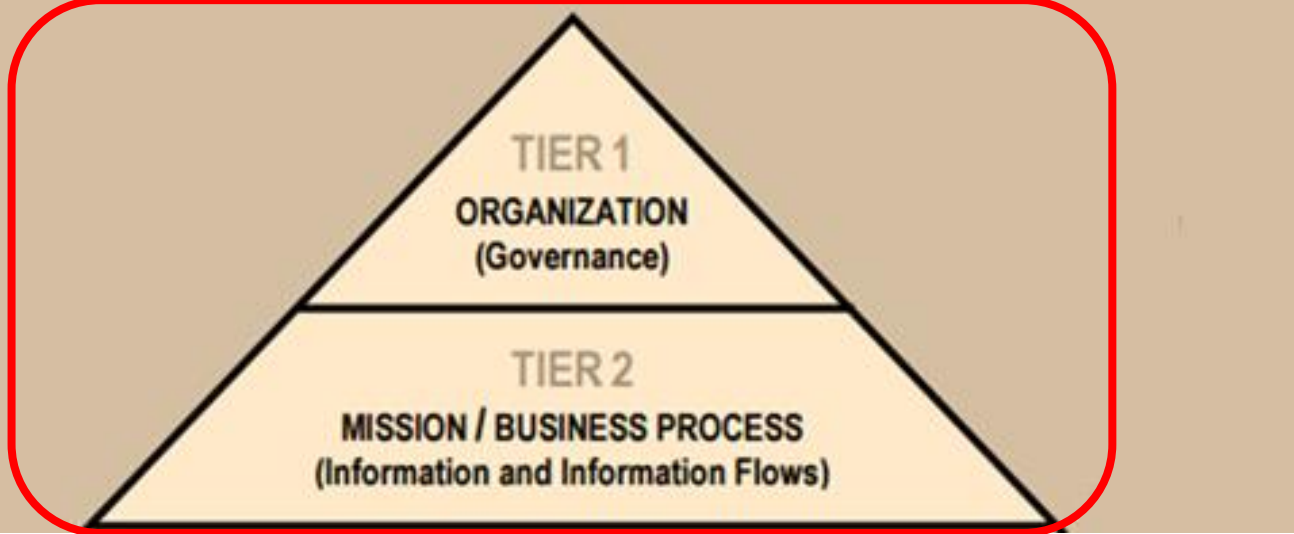
March 2011

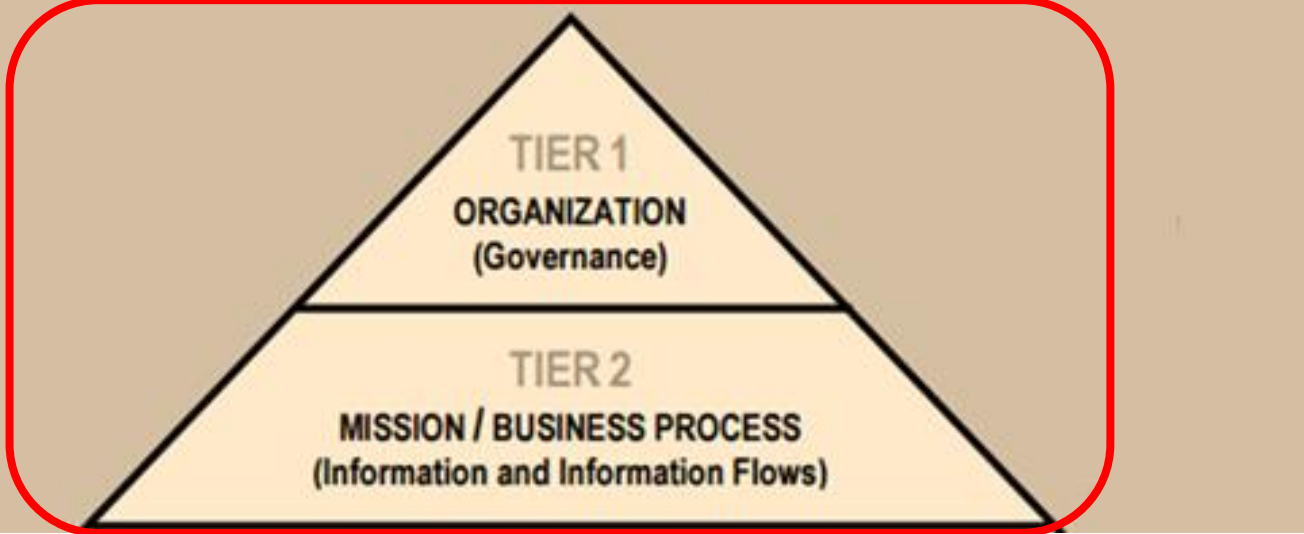


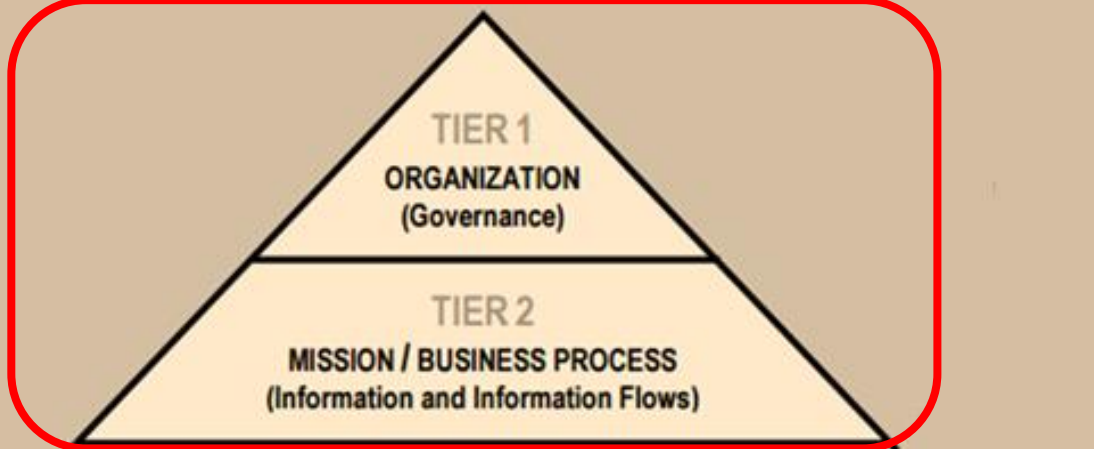
U.S. Department of Commerce
Gary Locke, Secretary

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









- **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”

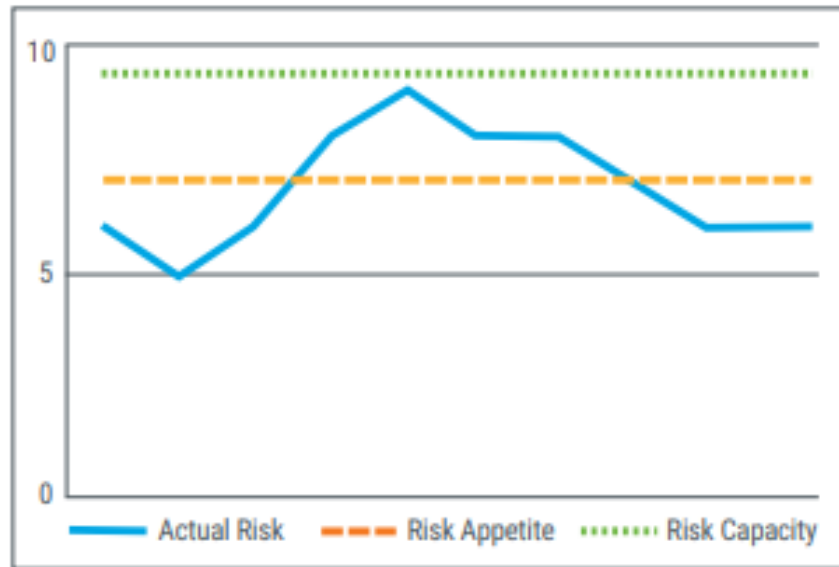


Diagram show a relatively sustainable situation

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

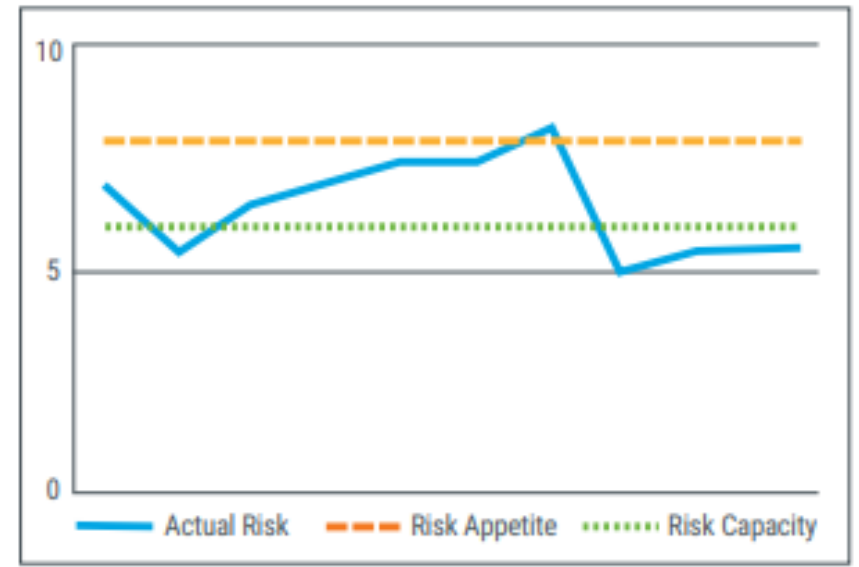
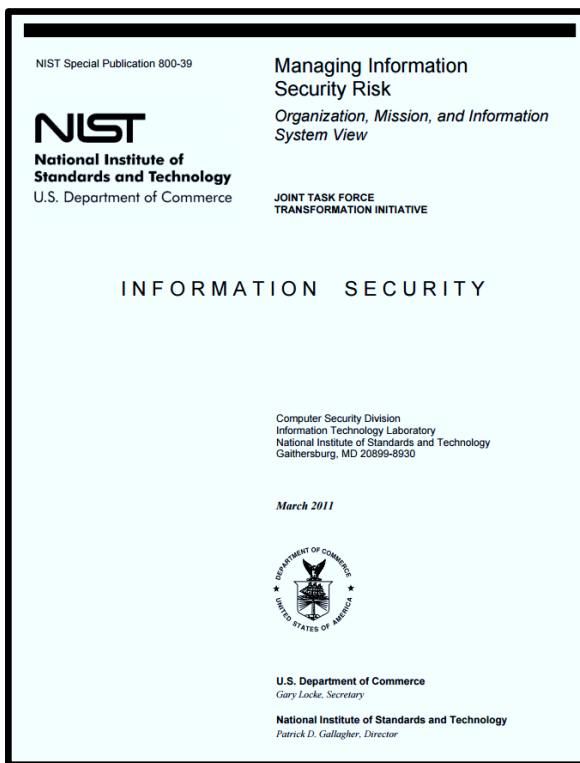
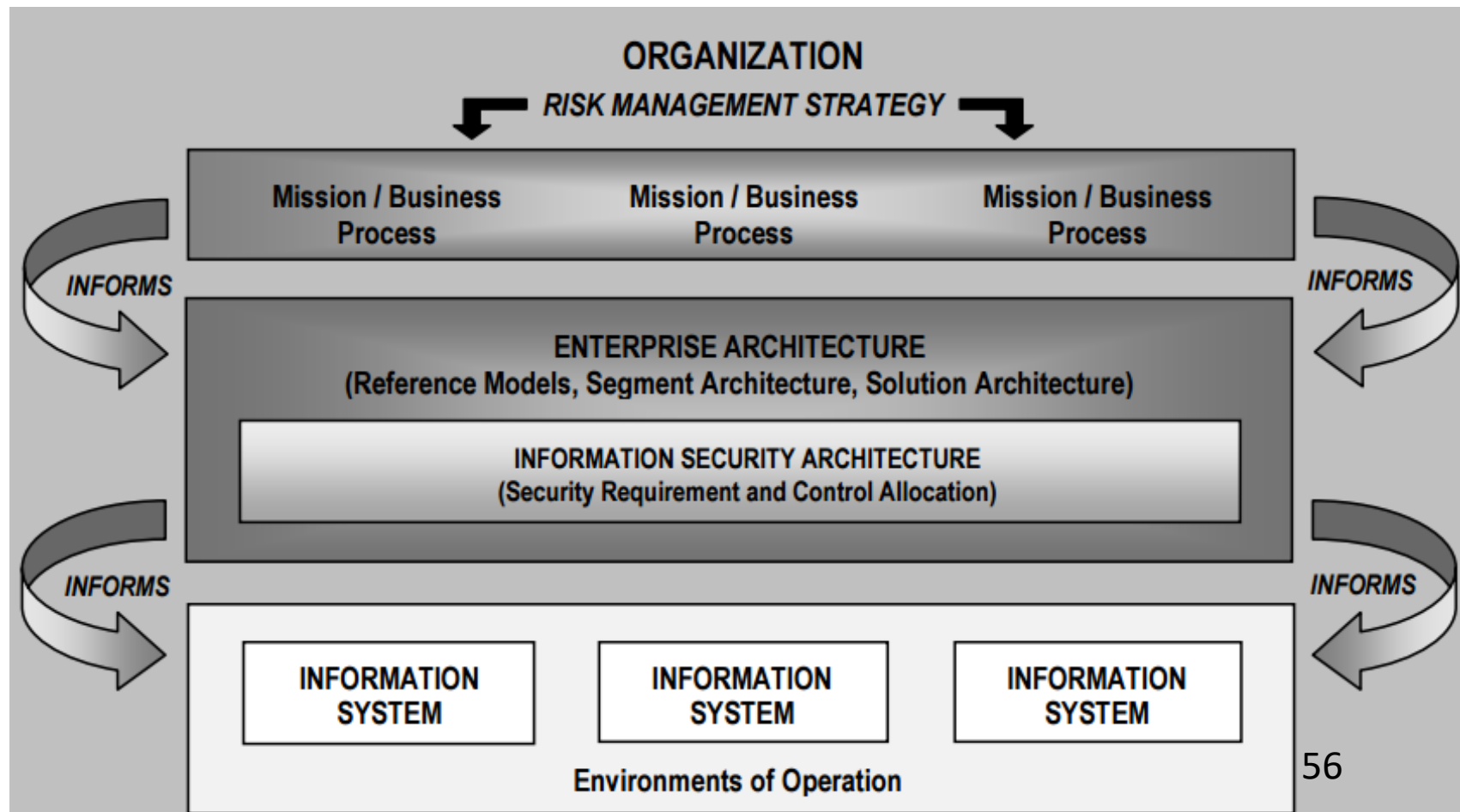


Diagram show an unsustainable situation

- 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



MIS 5206 Protecting Information Assets



NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

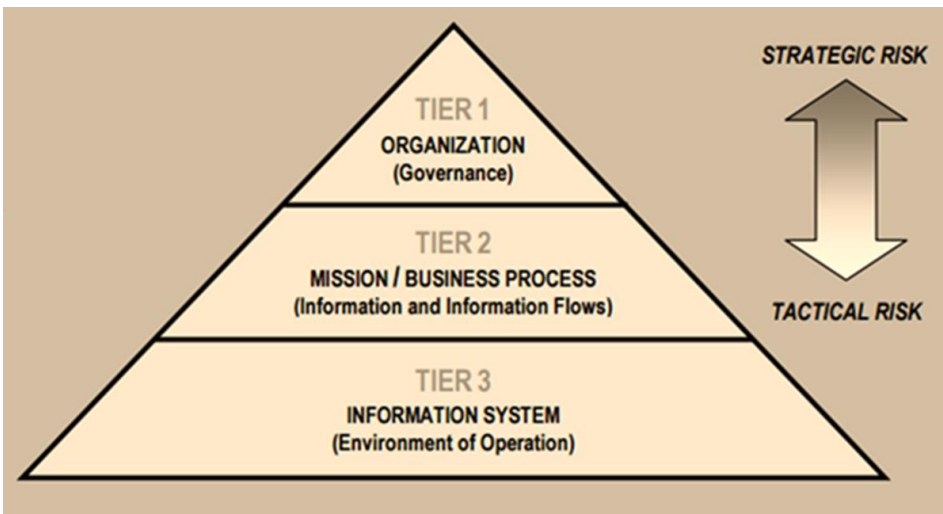
April 16, 2018

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



Functions	Categories
IDENTIFY	
PROTECT	
DETECT	
RESPOND	
RECOVER	
	57

NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



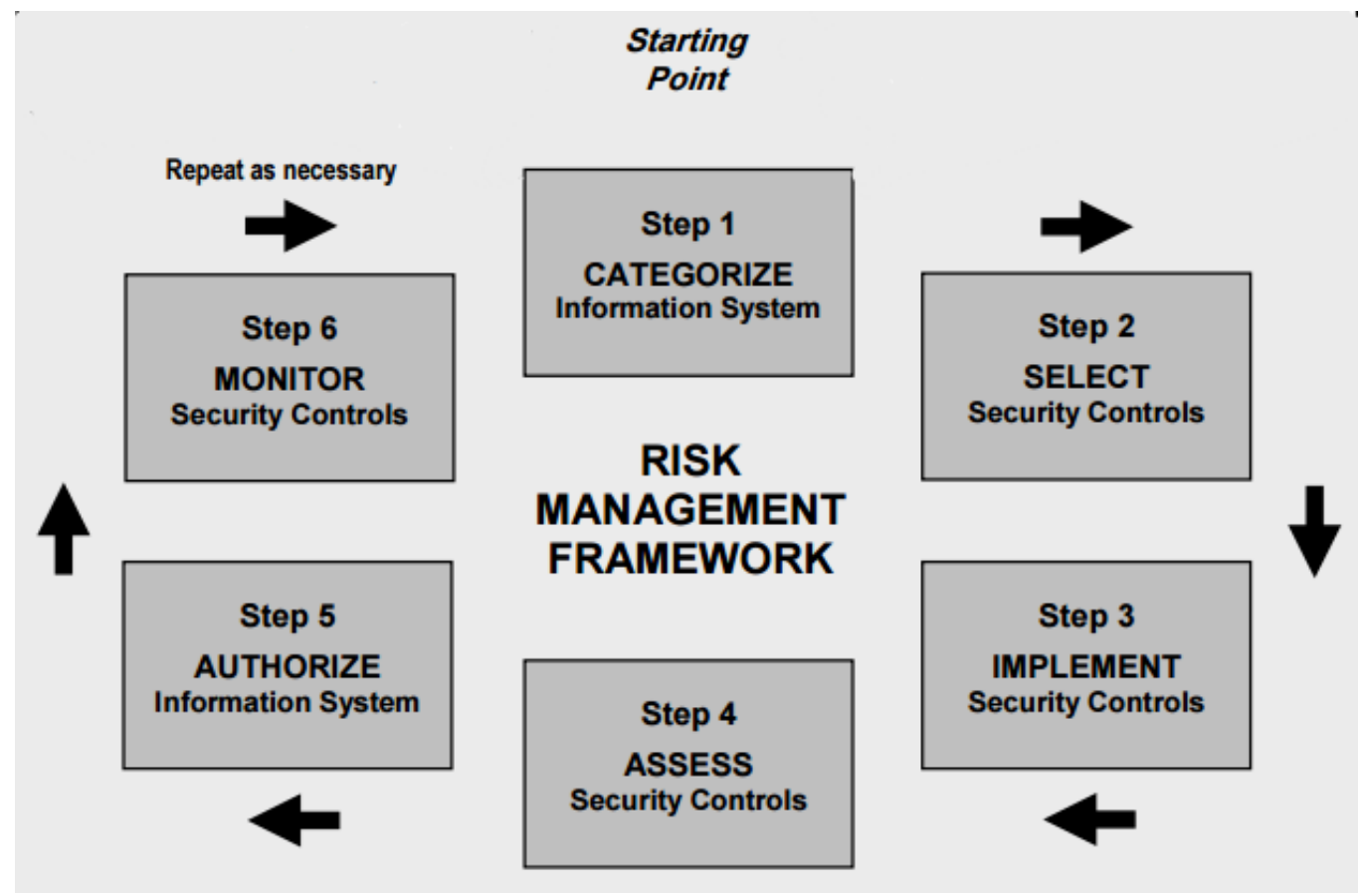
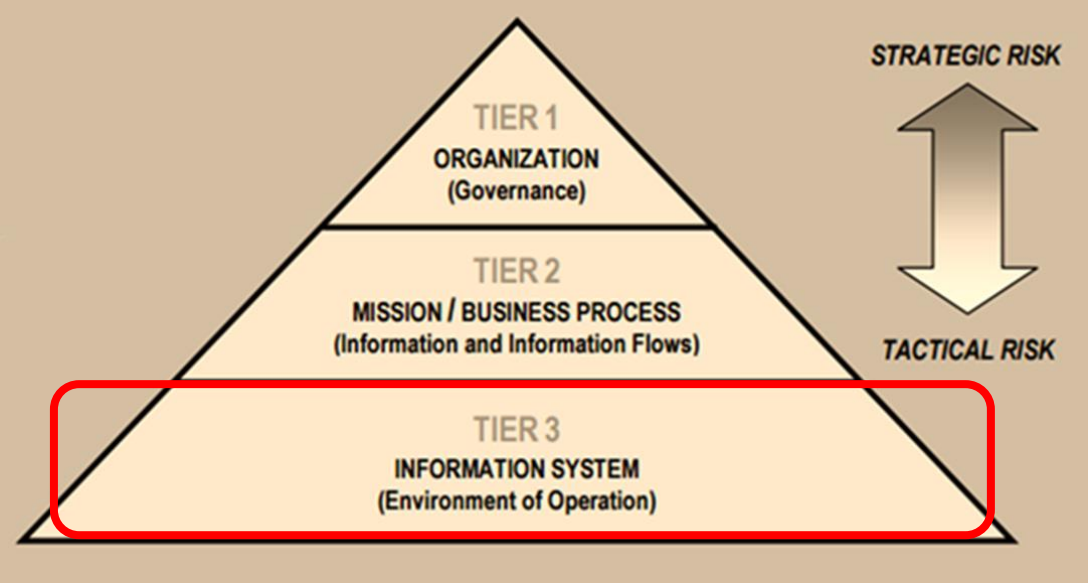
NIST Cybersecurity Framework

Cybersecurity Maturity Model Certification (CMMC) levels

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

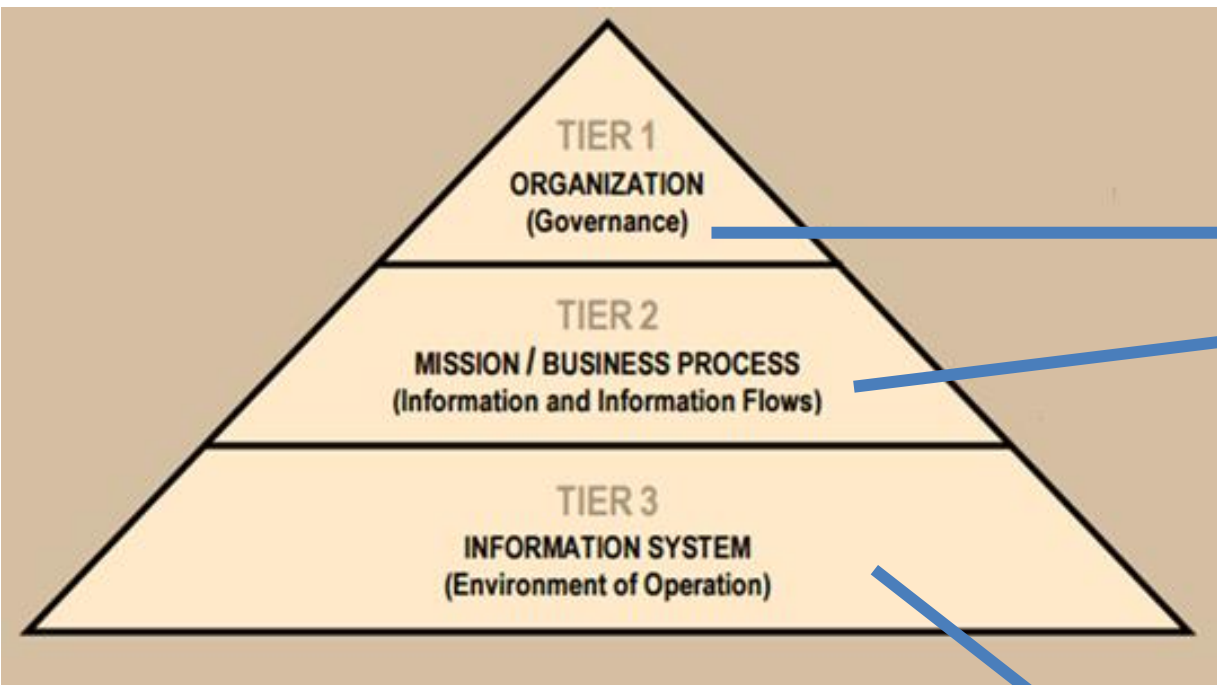


Is used to assess an organization's cybersecurity capability maturity level, and recommend steps for improvement



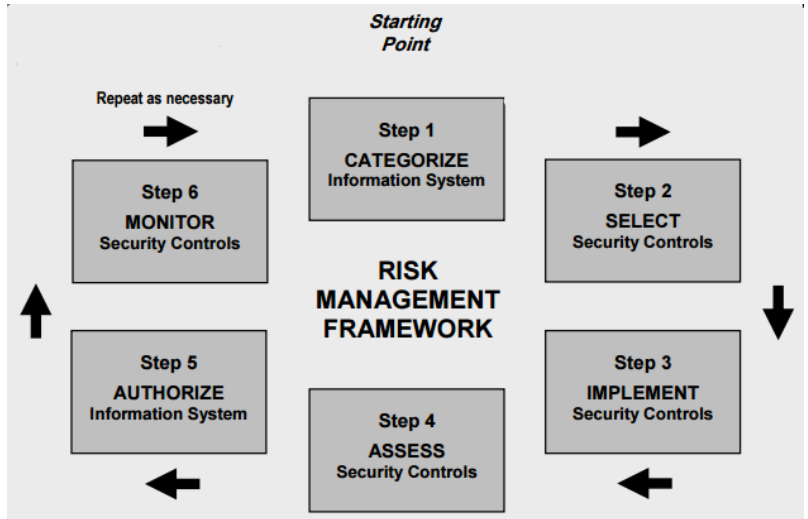
In summary...

The RiskIT Framework



NIST Critical Infrastructure Cyber Security Framework

NIST 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

