

MIS 5206
Protection of Information Assets
- Unit #1a -


Case Study: Snowfall and a stolen laptop

Agenda

- Daily class schedule and - schedule of breaks
- Introductions
- Case study analysis
- Frameworks for Protecting Information Assets

Daily Schedule

8:00 AM to 10:00 AM – Unit ...a
 10:00 AM to 10:10 AM - Break
 10:10 AM to 12:00 PM – Unit ...b

Today
 Sunday
 Monday
 Tuesday
 Wednesday
Museum 
 Friday
 Saturday
 Monday
 Monday or Tuesday

Class Schedule

Unit #	Assignment Topics
0a	Video - Introduction to MIS5206
0b	Videos - Understanding an Organization's Risk Environment
1a	Case Study 1: <i>Snowfall and a stolen laptop</i>
1b	Data Classification Process and Models
2a	Risk Evaluation
2b	Case Study 2: <i>Autopsy of a Data Breach: The Target Case</i>
3a	Creating a Security Aware Organization
3b	Physical and Environmental Security
4a	Midterm Exam
4b	Case Study 3: <i>A Hospital Catches the "Millennium Bug"</i>
5a	Business Continuity and Disaster Recovery Planning
5b	Team Project Assignment
6a	Network Security
6b	Cryptography, Public Key Encryption and Digital Signatures
7a	Identity Management and Access Control
7b	Computer Application Security & Team Project Presentations
8	Team Project Presentations & Review
9	Final Exam

Introductions

Meet in groups for 5 minutes and figure out:

- What one question would you like answered about the ITACS program ?

When we return, each groups representative will:

- Tell me your name
- Ask your team's question

Full Name	Email Address	Group
Cao, Yujie	tur33221@temple.edu	1
Li, Nana	tur33222@temple.edu	1
Ma, Yue	tur44511@temple.edu	1
Xiao, Guanhua	tur26153@temple.edu	1
Zhang, Hao	tur25910@temple.edu	1
Dong, Shuyi	tur20298@temple.edu	2
Liu, Chun	tur29660@temple.edu	2
Peng, Xinyi	tur33276@temple.edu	2
Xie, Yuanjun	tur25909@temple.edu	2
Zhang, Shuting	tur29220@temple.edu	2
Du, Yawen	tur25905@temple.edu	3
Liu, Chunqi	tur26150@temple.edu	3
Shi, Xiaozhi	tur25907@temple.edu	3
Yang, Shijie	tur29662@temple.edu	3
Zheng, Xuanwen	tur45587@temple.edu	3
He, Yuming	tur31787@temple.edu	4
Liu, Yi	tur40732@temple.edu	4
Wang, Haoran	tur25908@temple.edu	4
Yao, Haixu	tur50361@temple.edu	4
Hu, Yiwei	tur42896@temple.edu	5
Lu, Guoning	tur40733@temple.edu	5
Wang, Yue	tur32144@temple.edu	5
Yunpeng, Zhang	tur29218@temple.edu	5
Li, Hao	tur44510@temple.edu	6
Ma, Hongli	tur29661@temple.edu	6
Wang, Zhaomeng	tur42897@temple.edu	6
Zhang, Chenhao	tur29219@temple.edu	6

Case Study Analysis – Group Work

1. What information security reporting or organizational governance relationship exists between Information Security and the organization(s) Ballard and Francesco report into?
 - Is this a problem?
2. What evidence is the basis for Information Security Office (ISO) conclusion that the Dean's stolen laptop did not contain personally identifiable information on RIT students, faculty, or staff?
3. Is the ISO's conclusion valid? Why or why not?

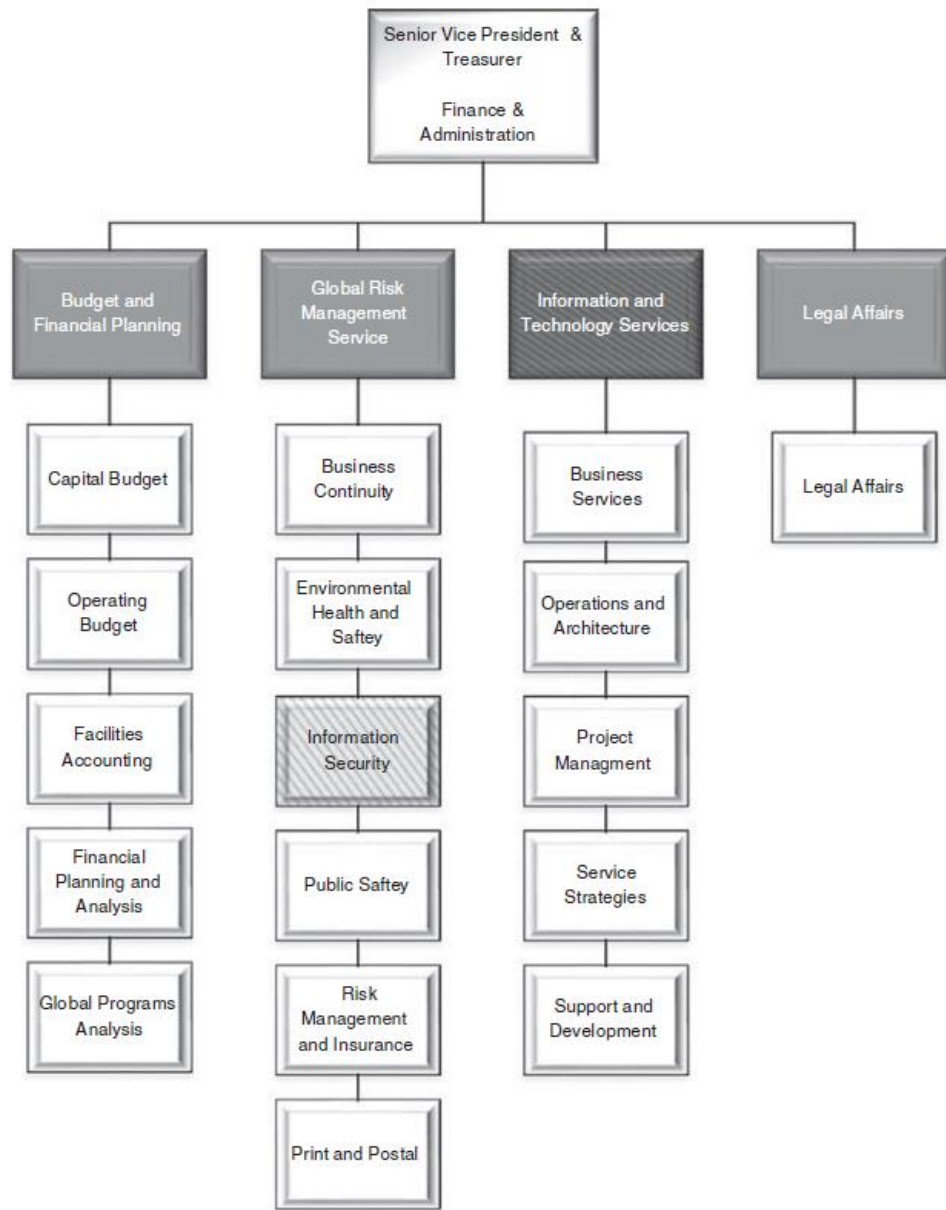
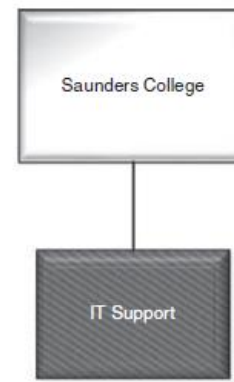


Figure C1 Partial RIT administrative organization chart.



Case Study Analysis: “Snowfall and a stolen laptop”

IT Governance Questions

1. Which organization does:

- Dave Ballard report into?
 - Network Administrator
- Nick Francesco report into?
 - Manager of Technical Services
- Where does the Information Security Office (ISO) reside?
- What information security reporting or organizational governance relationship exists between ISO and the organization(s) Ballard and Francesco report into?
- Is this a problem?
 - What kind of problem is it?

4. What evidence is the basis for Information Security Office (ISO) conclusion that the Dean's stolen laptop did not contain personally identifiable information on RIT students, faculty, or staff?
5. Is the ISO's conclusion valid? Why or why not?

Recovering deleted data files

On your computer, accessing "deleted" data may be done in 1 or two ways:

1. Recover Deleted Files from Recycle Bin

Step 1. Open Recycle Bin and find deleted files

Step 2. Select and right-click deleted files, click "Restore"

Step 3. Find recovered files at the original location

2. With one of many file undelete and data recovery programs widely available on the Internet.

These programs are touted as conveniences, which in some cases, they are

- But when it comes to security, the way your computer deletes (or doesn't delete) your data is a liability
- Someone accessing your computer remotely (i.e. a hacker) could very easily "recover" your deleted data
- The same goes for someone who buys your used computer on eBay or digs your discarded, failed hard drive out of the dumpster

<https://www.easeus.com/file-recovery/recover-deleted-files-on-ssd.html?x-clickref=1100ljxAPpG>

<https://www.stellarinfo.com/blog/ssd-recover-deleted-files/>

Francesco asked 'What student records did you have on your laptop?'

The Dean quickly replied 'None.'

Francesco clarified: "Until recently we used Social Security numbers to identify our students. Are you sure you didn't have any old class rosters, exams or other records on there?"

*The Dean took a few seconds to deeply consider what he was asked. 'No. I am not teaching this semester, and **I deleted everything from previous semesters.**'*

RIT Information Classifications

- A. **Private** – a classification for information that is confidential which could be used for identity theft and has additional requirements associated with its protection. Private information includes:
 - A. Social Security Numbers (SSNs), Taxpayer Identification Number (TIN), or other national identification number
 - B. Driver’s license numbers
 - C. Financial account information (bank account numbers (including checks), credit or debit card numbers, account numbers)
- B. **Confidential** – a classification for information that is restricted on a need to know basis, that, because of legal, contractual, ethical, or other constraints, may not be accessed or communicated without specific authorization. Confidential information includes:
 - A. Educational records governed by the Family Educational Rights & Privacy Act (FERPA) that are not defined as directory information
 - B. University Identification Numbers (UIDs)
 - C. Employee and student health information as defined by Health Insurance Portability and Accountability Act (HIPAA)
 - D. Alumni and donor information
 - E. Employee personnel records
 - F. Employee personal information including: home address and telephone number; personal e-mail addresses, usernames, or passwords; and parent’s surname before marriage
 - G. Management information, including communications or records of the Board of Trustees and senior administrators, designated as confidential
 - H. Faculty research or writing before publication or during the intellectual property protection process.
 - I. Third party information that RIT has agreed to hold confidential under a contract
- C. **Internal** – a classification for information restricted to RIT faculty, staff, students, alumni, contractors, volunteers, and business associates for the conduct of University business. Examples include online building floor plans, specific library collections, etc.
- D. **Public** – a classification for information that may be accessed or communicated by anyone without restriction.

*Francesco continued: ‘Think about this carefully, because it has implications much bigger than you and me. **What proprietary Saunders data did you have on that laptop?**’*

The Dean replied, ‘I really didn’t have anything too important. It was committee notes, faculty salary information, stuff like that. It may have been confidential, but not really proprietary.’

6. Was Francesco correct or mistaken in his use of the term “proprietary” Saunders data” ?

7. Specifically, how does RIT’s Information Classifications (Appendix F) relate to this case study scenario?

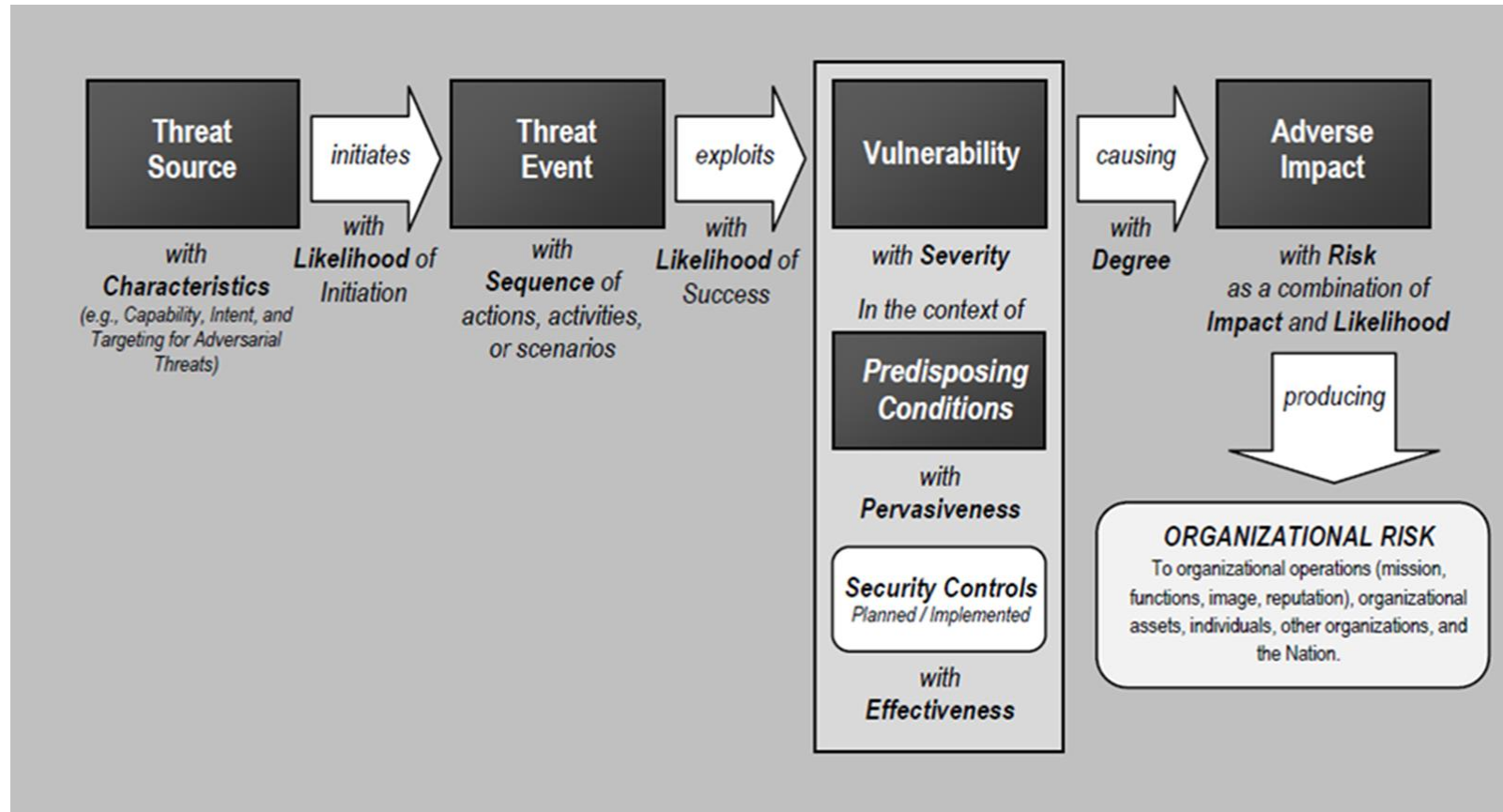
What would be the stolen laptop's additional impact on RIT if the ISO's conclusion is not valid ?

– *Who else at RIT would be concerned with this stolen laptop incident?*



How should we analyze the threat and attack leading to the Dean's lost laptop using this model?

What kind of threat source was active in the case study?



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

Taxonomy of threat sources

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

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

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

How should we analyze the threat and attack leading to the Dean's lost laptop using this model?

A. Threat source

- i. Capability
- ii. Intent
- iii. Targeting

B. Threat event

- i. Attack type
- ii. Likelihood of attack initiation

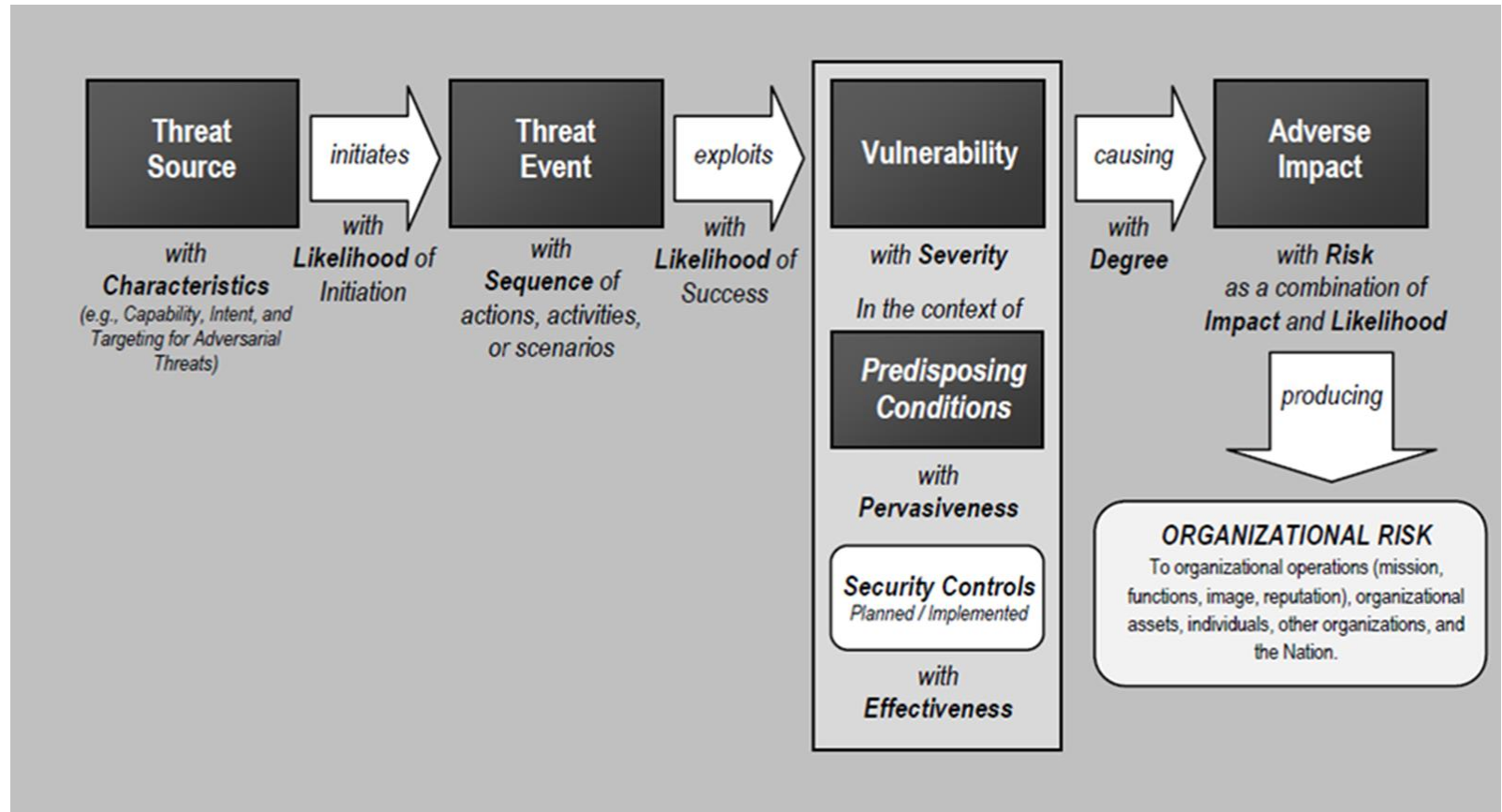
C. Vulnerability

- i. Weakness type
- ii. Likelihood attack succeeds

D. Impact

- i. Impact type
- ii. Severity of impact
- iii. Overall likelihood

E. Risk



How should we organize and present the risks?

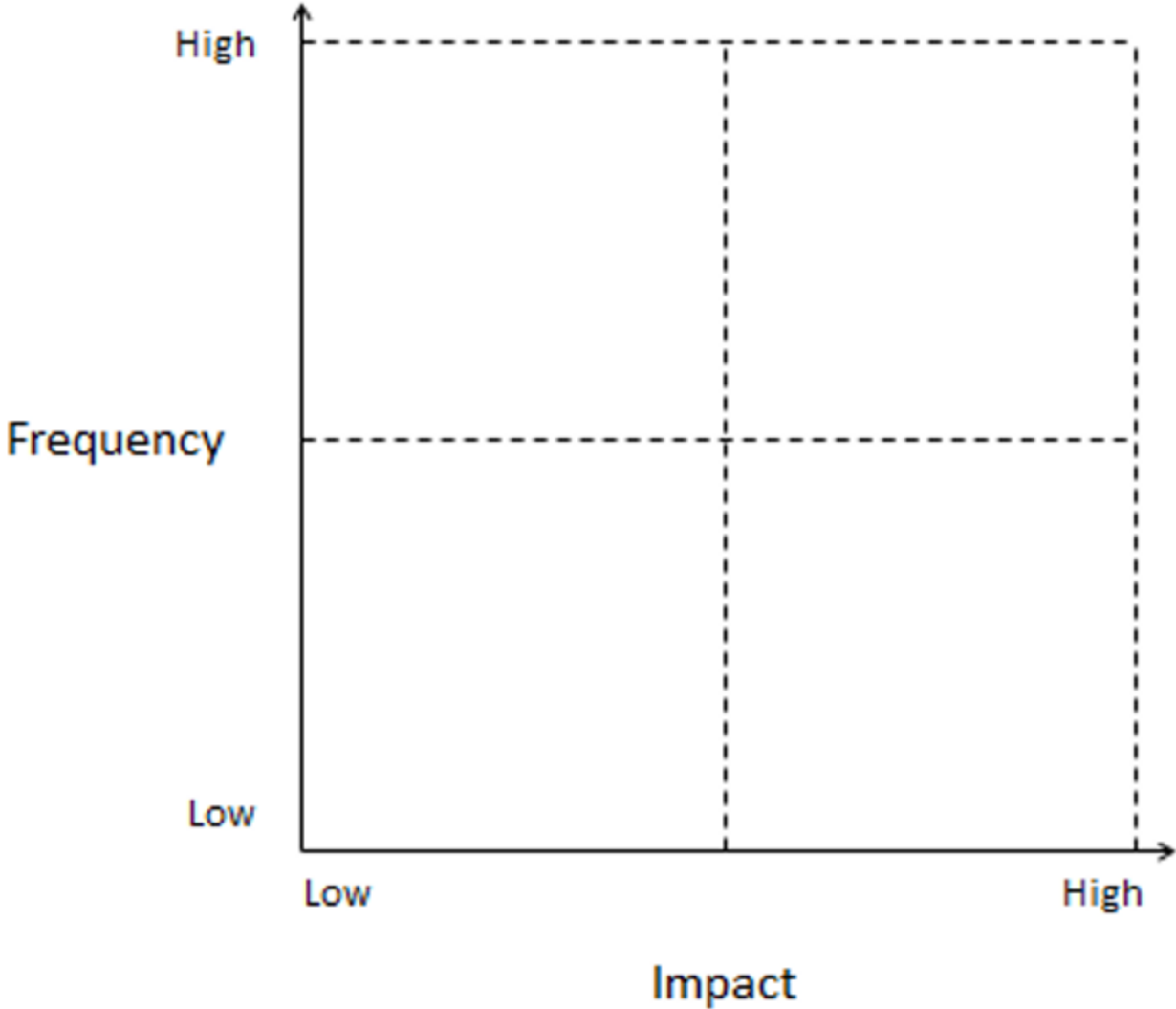


Factor Analysis of Information Risk (FAIR) framework

- Provides guidance on evaluating risks within organizations, broadly across an organization and in the context of a particular IT asset.
- Helps distinguish between:
 - Security incident frequency
 - How many laptop thefts per year?
 - Impacts on the organization
 - How many employee-hours to investigate, resolve, and recover from the incident?
 - How much money spent on credit monitoring for theft victims?

10. How should we organize and present the risks?

Risk	Impact	Frequency



Case Study epilogue

- I. Government numbers (Social Security Numbers) were eliminated as identifiers at the University
 - This change required modifications to every IT system used at RIT
- II. RIT implemented 2-layered approach to protecting data
 1. New software purchased to identify (and report) potential personally identifiable information on laptops
 - *In the case of a theft, RIT was able to identify what personal information may have been at risk*
 2. RIT implemented enterprise full disk encryption technologies on laptops to limit financial risks resulting from lost Personally Identifiable Information (PII)
 - Solution included ability to report on the state of the data (i.e. report when data is decrypted)

Case Study wrap-up



Saunders College of Business

Rochester Institute of Technology (RIT)



Ashok Rao



Janis Gogan • 3rd

Professor at Bentley U and President at Cases for Action
Bentley University • Harvard University

Greater Boston Area • 274 [88](#)

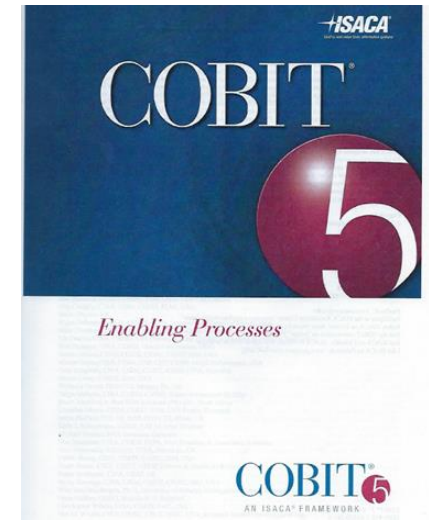
Frameworks for Protecting Information Assets...



A leading example of information security risk management

- First published in 2005, updated in 2013, and again in 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
- Now part of the [ISO/IEC 27000 series](#)

A screenshot of the NIST Risk Management Framework (RMF) website. The header includes the NIST logo, "Information Technology Laboratory", "COMPUTER SECURITY RESOURCE CENTER", and a search bar. Below the header, there are tabs for "PROJECTS" and "NIST RISK MANAGEMENT FRAMEWORK". The main content area is titled "NIST Risk Management Framework RMF" and includes a sub-header "About the Risk Management Framework (RMF)" and a description: "A Comprehensive, Flexible, Risk-Based Approach". The description states: "The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. Managing organizational risk is paramount to effective information security and privacy programs; the RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., IoT, control systems), and within any type of organization regardless of size or sector." To the right of the main content is a "PROJECT LINKS" sidebar with links to Overview, FAQs, News & Updates, Events, Publications, Presentations, and additional pages like FISMA Background, About the RMF, Prepare Step, Categorize Step, Select Step, Implement Step, Assess Step, Authorize Step, Monitor Step, SP 800-53 Controls, Release Search, Downloads, and Control Catalog Public Comments Overview.





**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

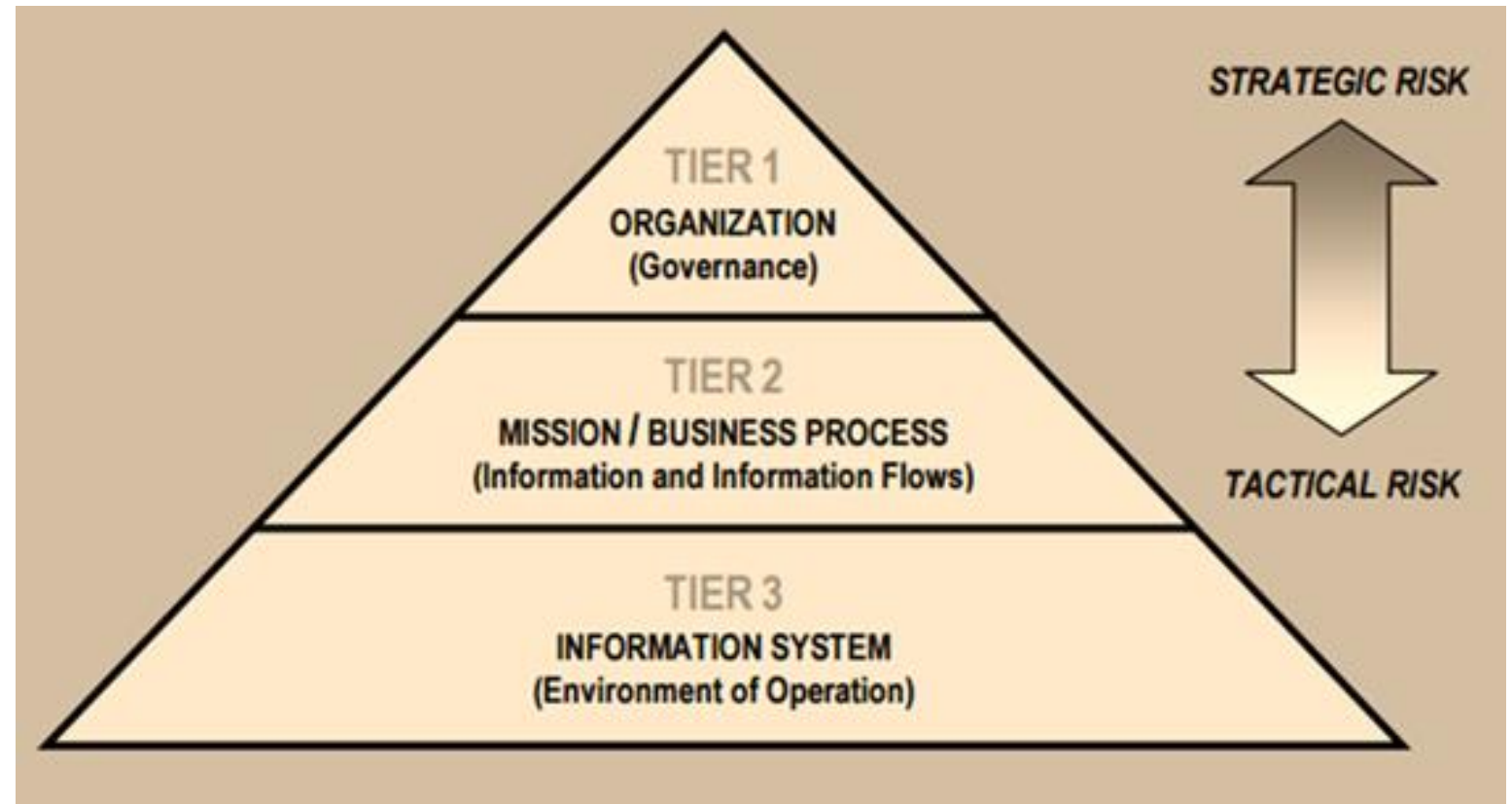
March 2011

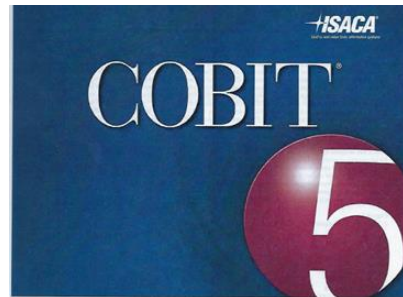


U.S. Department of Commerce
Gary Locke, Secretary

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

An Overview of Frameworks for Protecting Information Assets





Enabling Processes



MIS 5206 Protecting Information Assets

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure
Governance
Framework Setting
and Maintenance

EDM02 Ensure
Benefits Delivery

EDM03 Ensure
Risk Optimisation

EDM04 Ensure
Resource
Optimisation

EDM05 Ensure
Stakeholder
Transparency

Align, Plan and Organise

AP001 Manage
the IT Management
Framework

AP002 Manage
Strategy

AP003 Manage
Enterprise
Architecture

AP004 Manage
Innovation

AP005 Manage
Portfolio

AP006 Manage
Budget and Costs

AP007 Manage
Human Resources

AP008 Manage
Relationships

AP009 Manage
Service
Agreements

AP010 Manage
Suppliers

AP011 Manage
Quality

AP012 Manage
Risk

AP013 Manage
Security

Build, Acquire and Implement

BAI01 Manage
Programmes and
Projects

BAI02 Manage
Requirements
Definition

BAI03 Manage
Solutions
Identification
and Build

BAI04 Manage
Availability
and Capacity

BAI05 Manage
Organisational
Change
Enablement

BAI06 Manage
Changes

BAI07 Manage
Change
Acceptance and
Transitioning

BAI08 Manage
Knowledge

BAI09 Manage
Assets

BAI10 Manage
Configuration

Deliver, Service and Support

DSS01 Manage
Operations

DSS02 Manage
Service Requests
and Incidents

DSS03 Manage
Problems

DSS04 Manage
Continuity

DSS05 Manage
Security
Services

DSS06 Manage
Business
Process Controls

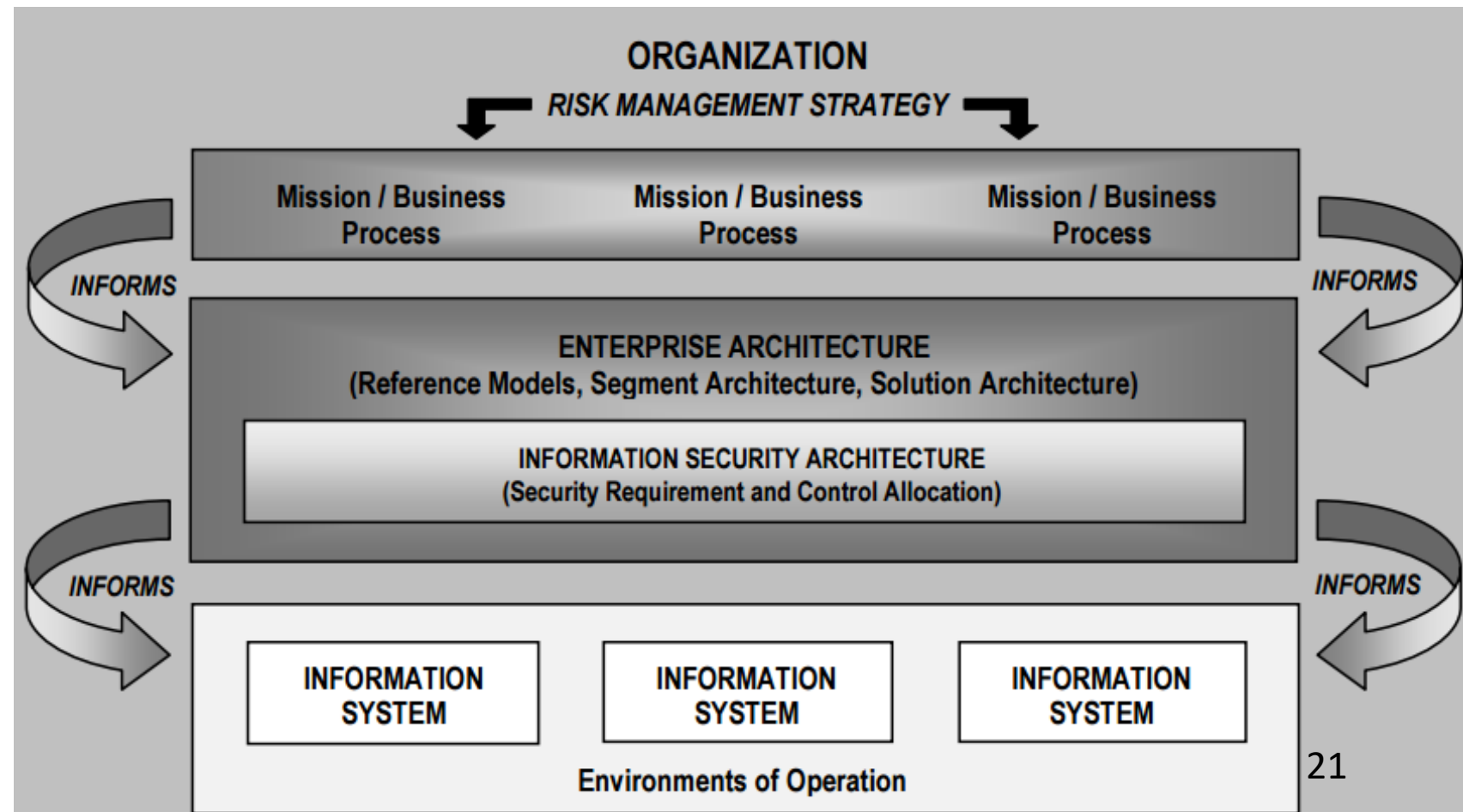
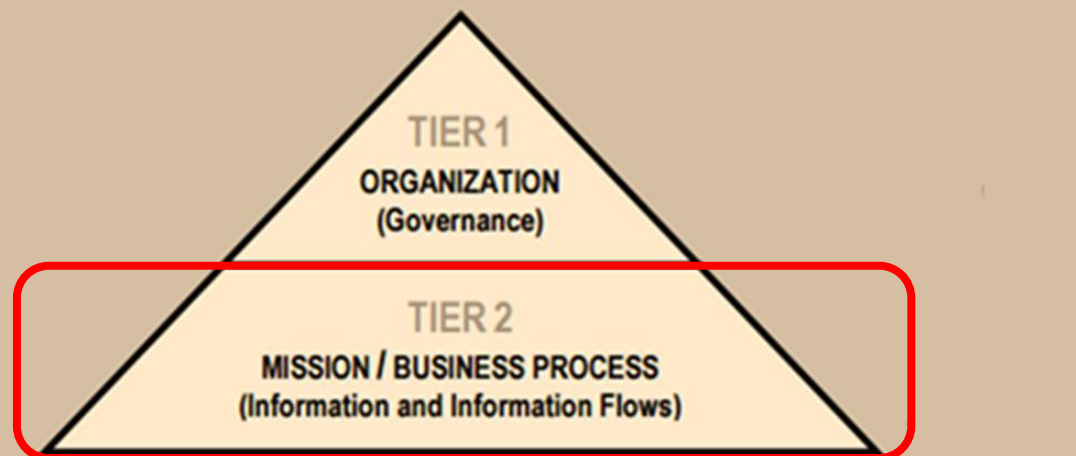
Monitor, Evaluate and Assess

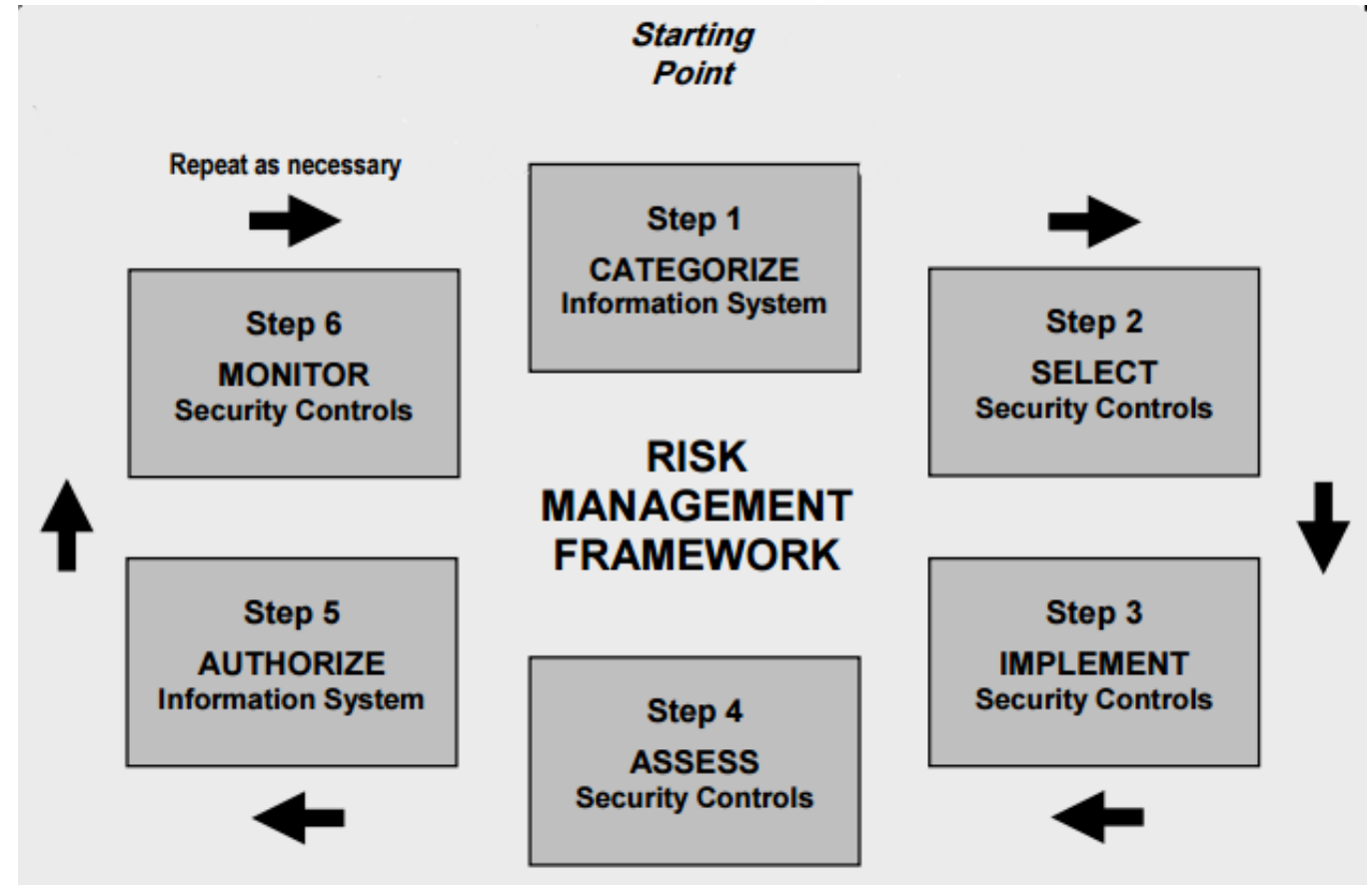
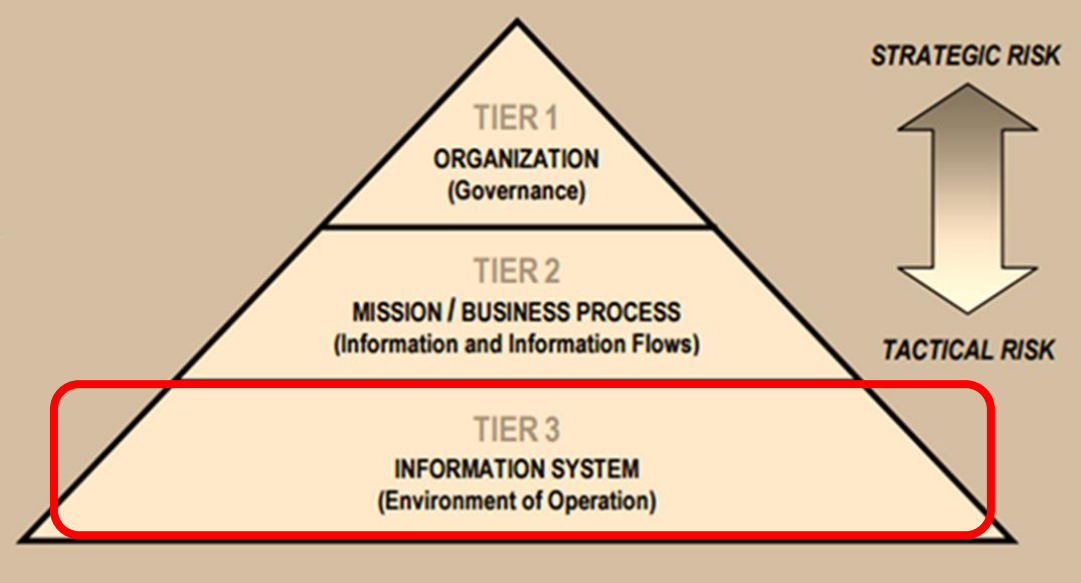
MEA01 Monitor,
Evaluate and Assess
Performance and
Conformance

MEA02 Monitor,
Evaluate and Assess
the System of Internal
Control

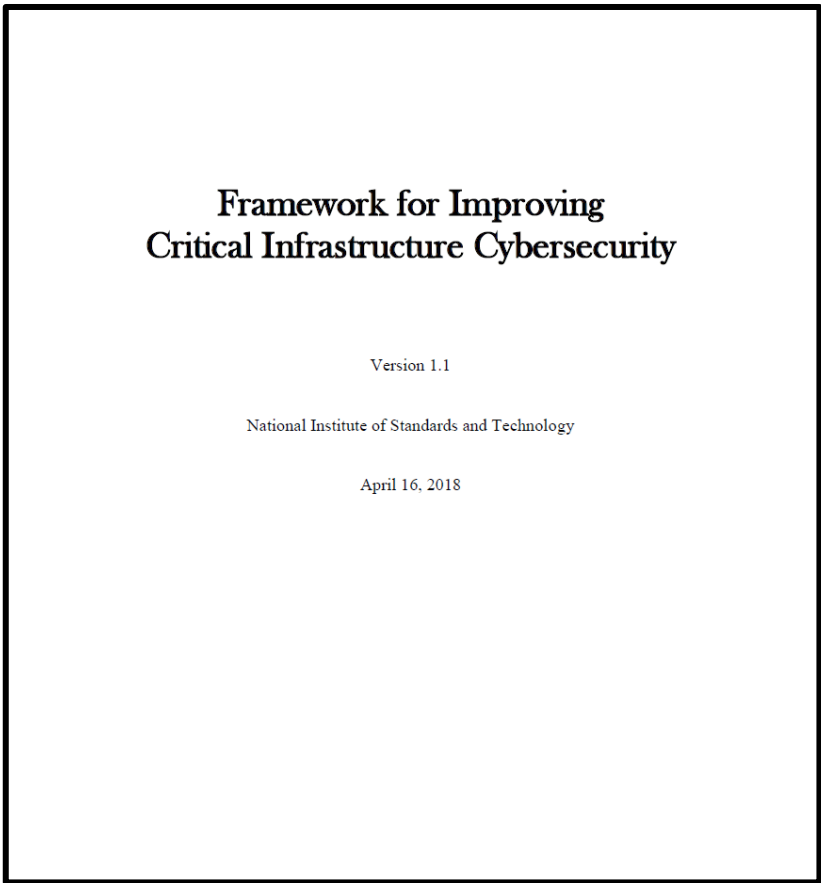
MEA03 Monitor,
Evaluate and Assess
Compliance With
External Requirements

Processes for Management of Enterprise IT





NIST Cybersecurity Framework

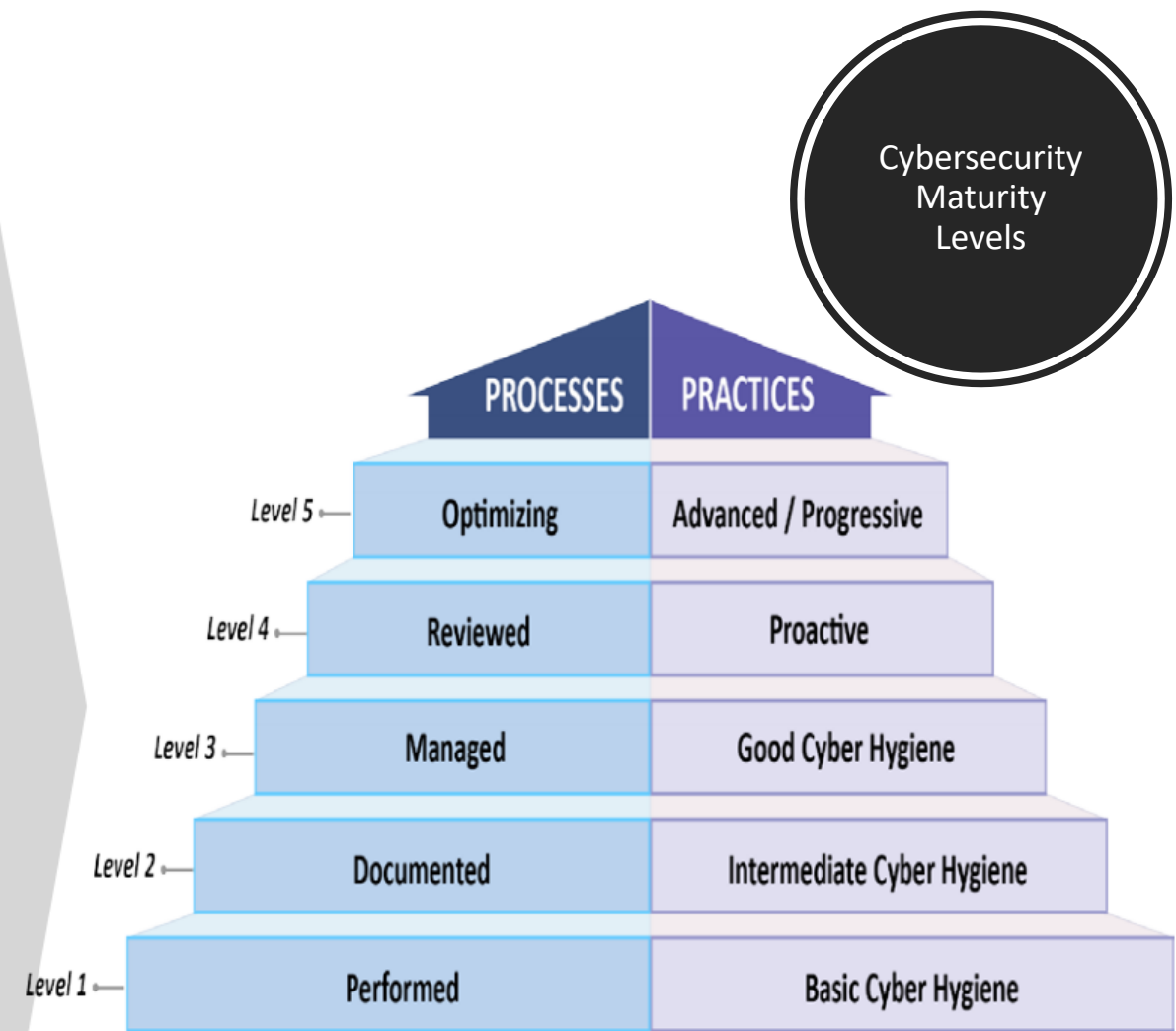


Refers to and builds on many principles of ISO/IEC 27001 standard
Goes way beyond IT and physical security environment

- ...by also including:
- Governance and management
 - Staff policies and procedures
 - Training
 - Supply chain management

Functions	Categories
IDENTIFY	
PROTECT	
DETECT	
RESPOND	
RECOVER	
	23

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





Organized as a Workflow



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

NIST CYBERSECURITY FRAMEWORK (CSF)



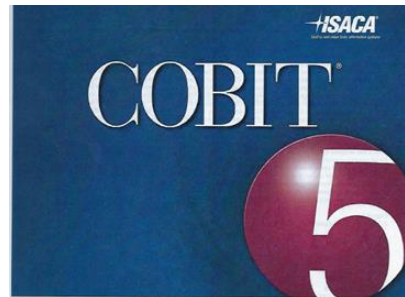
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		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

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Each Category of cybersecurity activities is further broken down into subcategories

Each subcategory or activity is associated or cross-referenced to information references

NIST SP 800 information references pertain to specific information security controls
COBIT references pertain to Governance and Management processes



Enabling Processes



MIS 5206 Protecting Information Assets

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure
Governance
Framework Setting
and Maintenance

EDM02 Ensure
Benefits Delivery

EDM03 Ensure
Risk Optimisation

EDM04 Ensure
Resource
Optimisation

EDM05 Ensure
Stakeholder
Transparency

Align, Plan and Organise

AP001 Manage
the IT Management
Framework

AP002 Manage
Strategy

AP003 Manage
Enterprise
Architecture

AP004 Manage
Innovation

AP005 Manage
Portfolio

AP006 Manage
Budget and Costs

AP007 Manage
Human Resources

AP008 Manage
Relationships

AP009 Manage
Service
Agreements

AP010 Manage
Suppliers

AP011 Manage
Quality

AP012 Manage
Risk

AP013 Manage
Security

Build, Acquire and Implement

BAI01 Manage
Programmes and
Projects

BAI02 Manage
Requirements
Definition

BAI03 Manage
Solutions
Identification
and Build

BAI04 Manage
Availability
and Capacity

BAI05 Manage
Organisational
Change
Enablement

BAI06 Manage
Changes

BAI07 Manage
Change
Acceptance and
Transitioning

BAI08 Manage
Knowledge

BAI09 Manage
Assets

BAI10 Manage
Configuration

Deliver, Service and Support

DSS01 Manage
Operations

DSS02 Manage
Service Requests
and Incidents

DSS03 Manage
Problems

DSS04 Manage
Continuity

DSS05 Manage
Security
Services

DSS06 Manage
Business
Process Controls

Monitor, Evaluate and Assess

MEA01 Monitor,
Evaluate and Assess
Performance and
Conformance

MEA02 Monitor,
Evaluate and Assess
the System of Internal
Control

MEA03 Monitor,
Evaluate and Assess
Compliance With
External Requirements

Processes for Management of Enterprise IT

BAI09 Manage Assets		Area: Management Domain: Build, Acquire and Implement
Process Description Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licences to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with licence agreements.		
Process Purpose Statement Account for all IT assets and optimise the value provided by these assets.		
The process supports the achievement of a set of primary IT-related goals:		
IT-related Goal	Related Metrics	
06 Transparency of IT costs, benefits and risk	<ul style="list-style-type: none">• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits• Percent of IT services with clearly defined and approved operational costs and expected benefits• Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information	
11 Optimisation of IT assets, resources and capabilities	<ul style="list-style-type: none">• Frequency of capability maturity and cost optimisation assessments• Trend of assessment results• Satisfaction levels of business and IT executives with IT-related costs and capabilities	
Process Goals and Metrics		
Process Goal	Related Metrics	
1. Licences are compliant and aligned with business need.	<ul style="list-style-type: none">• Percent of used licences against paid-for licences	
2. Assets are maintained at optimal levels.	<ul style="list-style-type: none">• Number of assets not utilised• Benchmark costs• Number of obsolete assets	

BAI09 RACI Chart																										
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI09.01 Identify and record current assets			C			C												I	C	C	A	R	C			
BAI09.02 Manage critical assets																									C	
<div> ID.AM-1: Physical devices and systems within the organization are inventoried <div> CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5 </div> </div>																										

BAI09 Process Practices, Inputs/Outputs and Activities				
Management Practice	Inputs		Outputs	
BAI09.01 Identify and record current assets. Maintain an up-to-date and accurate record of all IT assets required to deliver services and ensure alignment with configuration management and financial management.	From	Description	Description	To
	BAI03.04	Updates to asset inventory	Asset register	AP006.01 BAI10.03
	BAI10.02	Configuration repository	Results of physical inventory checks	BAI10.03 BAI10.04 DSS05.03
			Results of fit-for-purpose reviews	AP002.02
Activities				
1. Identify all owned assets in an asset register that records current status. Maintain alignment with the change management and configuration management processes, the configuration management system, and the financial accounting records.				
2. Identify legal, regulatory or contractual requirements that need to be addressed when managing the asset.				
3. Verify the existence of all owned assets by performing regular physical and logical inventory checks and reconciliation including the use of software discovery tools.				
4. Verify that the assets are fit for purpose (i.e., in a useful condition).				
5. Determine on a regular basis whether each asset continues to provide value and, if so, estimate the expected useful life for delivering value.				
6. Ensure accounting for all assets.				
Management Practice	Inputs		Outputs	
BAI09.02 Manage critical assets. Identify assets that are critical in providing service capability and take steps to maximise their reliability and availability to support business needs.	From	Description	Description	To
			Communication of planned maintenance downtime	AP008.04
			Maintenance agreements	Internal
Activities				
1. Identify assets that are critical in providing service capability by referencing requirements in service definitions, SLAs and the configuration management system.				
2. Monitor performance of critical assets by examining incident trends and, where necessary, take action to repair or replace.				
3. On a regular basis, consider the risk of failure or need for replacement of each critical asset.				
4. Maintain the resilience of critical assets by applying regular preventive maintenance, monitoring performance, and, if required, providing alternative and/or additional assets to minimise the likelihood of failure.				
5. Establish a preventive maintenance plan for all hardware, considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors.				
6. Establish maintenance agreements involving third-party access to organisational IT facilities for on-site and off-site activities (e.g., outsourcing). Establish formal service contracts containing or referring to all necessary security conditions, including access authorisation procedures, to ensure compliance with the organisational security policies and standards.				
7. Communicate to affected customers and users the expected impact (e.g., performance restrictions) of maintenance activities.				
8. Ensure that remote access services and user profiles (or other means used for maintenance or diagnosis) are active only when required.				
9. Incorporate planned downtime in an overall production schedule, and schedule the maintenance activities to minimise the adverse impact on business processes.				

Each subcategory or activity is associated or cross-referenced to information references

COBIT references pertain to Governance and Management processes
NIST SP 800 information references pertain to specific information security controls

PUBLICATIONS

SP 800-53 Rev. 5

Security and Privacy Controls for Information Systems and Organizations



Date Published: September 2020 (Includes updates as of Dec. 10, 2020)

Supersedes: SP 800-53 Rev. 5 (09/23/2020)

Planning Note (7/13/2022):

A minor (errata) release of SP 800-53 Rev. 5 is now available for public comment using the SP 800-53 Public Comment Site. Submit your comments by August 12, 2022. [Learn more!](#)

Summary of supplemental files:

- Control Catalog Spreadsheet (NEW)**
The entire security and privacy control catalog in spreadsheet format. Note: For a spreadsheet of control baselines, see the [SP 800-53B details](#).
- Analysis of updates between 800-53 Rev. 5 and Rev. 4** (Updated 1/07/22)
Describes the changes to each control and control enhancement, provides a brief summary of the changes, and includes an assessment of the significance of the changes. Note that this comparison was authored by The MITRE Corporation for the Director of National Intelligence (DNI) and is being shared with permission by DNI.
- Mapping of Appendix J Privacy Controls (Rev. 4) to Rev. 5**
Supports organizations using the privacy controls in Appendix J of SP 800-53 Rev. 4 that are transitioning to the integrated control catalog in Rev. 5.
- Mappings between 800-53 Rev. 5 and other frameworks and standards** (NIST Cybersecurity Framework and NIST Privacy Framework; ISO/IEC 27001 (updated 1/22/21))
The mappings provide organizations a general indication of SP 800-53 control coverage with respect to other frameworks and standards. When leveraging the mappings, it is important to consider the intended scope of each publication and how each publication is used; organizations should not assume equivalency based solely on the mapping tables because mappings are not always one-to-one and there is a degree of subjectivity in the mapping analysis.

Also available:

- Security and Privacy Control Collaboration Index Template** (Excel & Word)
The collaboration index template supports information security and privacy program collaboration to help ensure that the objectives of both disciplines are met and that risks are appropriately managed. It is an optional tool for information security and privacy programs to identify the degree of collaboration needed between security and privacy programs with respect to the selection and/or implementation of controls in Rev. 5.
- OSCAL version of 800-53 Rev. 5 controls**
Rev. 5 controls are provided using the [Open Security Controls Assessment Language](#) (OSCAL); currently available in JSON, XML, and HTML.

DOCUMENTATION

Publication:

- SP 800-53 Rev. 5 (DOI)
- Local Download

Supplemental Material:

- Control Catalog (spreadsheet) (xls)
- Analysis of updates between 800-53 Rev. 5 and Rev. 4 by MITRE Corp. for ODNI (xls)
- Mapping: Appendix J Privacy Controls (Rev. 4) to Rev. 5 (xls)
- Mappings: Cybersecurity Framework and Privacy Framework to Rev. 5 (xls)
- Mapping: Rev. 5 to ISO/IEC 27001 (word)
- OSCAL Version of Rev. 5 controls (web)
- Control Collaboration Index Template (xls)
- Control Collaboration Index Template (word)
- Blog post (web)

Other Parts of this Publication:

[SP 800-53B](#)

Document History:

12/10/20: SP 800-53 Rev. 5 (Final)

TOPICS

Security and Privacy

[privacy controls](#); [security controls](#); [security programs & operations](#)

Laws and Regulations

[E-Government Act: Federal Information Security Modernization Act: Homeland Security Presidential Directive 12: Homeland Security Presidential Directive 7: OMB Circular A-11: OMB Circular A-130](#)

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



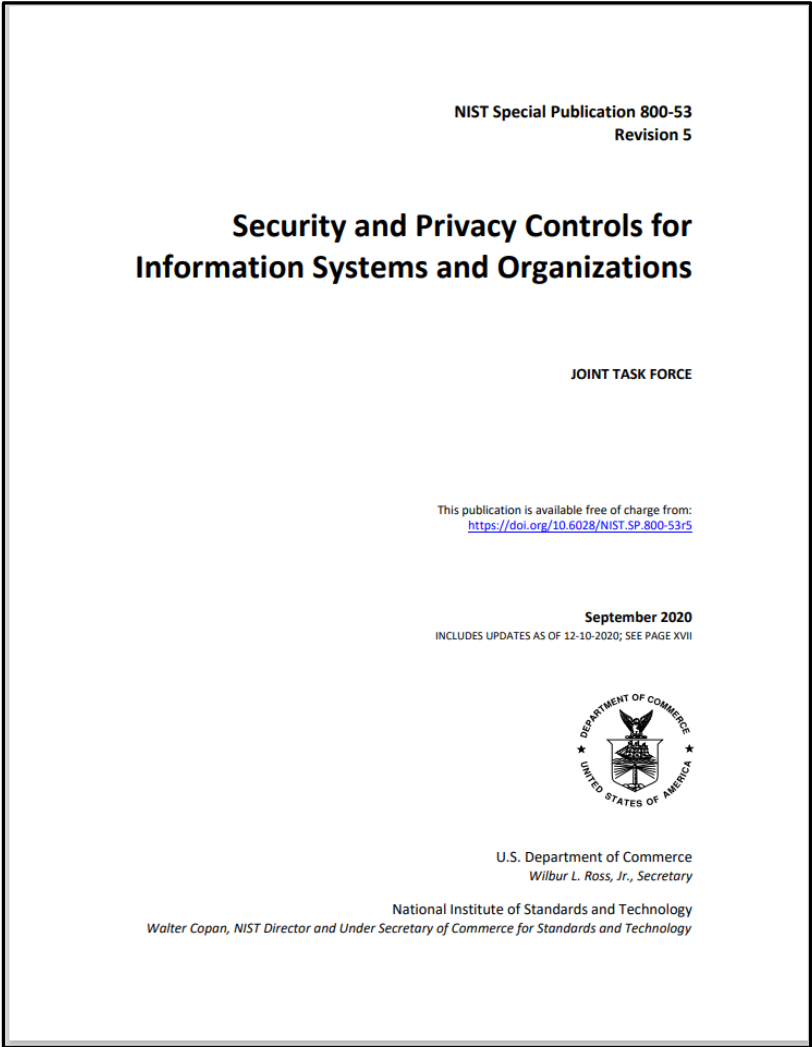
U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

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

MIS 5206 Protecting Information Assets

<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
--	---



2.2 CONTROL STRUCTURE AND ORGANIZATION

Security and privacy controls described in this publication have a well-defined organization and structure. For ease of use in the security and privacy control selection and specification process, controls are organized into 20 *families*.²⁵ Each family contains controls that are related to the specific topic of the family. A two-character identifier uniquely identifies each control family (e.g., *PS* for Personnel Security). Security and privacy controls may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms that are implemented by systems or actions by individuals. Table 1 lists the security and privacy control families and their associated family identifiers.

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

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

Table of Contents

CHAPTER ONE INTRODUCTION	1
1.1 PURPOSE AND APPLICABILITY	2
1.2 TARGET AUDIENCE	3
1.3 ORGANIZATIONAL RESPONSIBILITIES.....	3
1.4 RELATIONSHIP TO OTHER PUBLICATIONS.....	5
1.5 REVISIONS AND EXTENSIONS.....	5
1.6 PUBLICATION ORGANIZATION	5
CHAPTER TWO THE FUNDAMENTALS.....	7
2.1 REQUIREMENTS AND CONTROLS	7
2.2 CONTROL STRUCTURE AND ORGANIZATION	8
2.3 CONTROL IMPLEMENTATION APPROACHES.....	11
2.4 SECURITY AND PRIVACY CONTROLS.....	13
2.5 TRUSTWORTHINESS AND ASSURANCE.....	14
CHAPTER THREE THE CONTROLS	16
3.1 ACCESS CONTROL	18
3.2 AWARENESS AND TRAINING.....	59
3.3 AUDIT AND ACCOUNTABILITY	65
3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING.....	83
3.5 CONFIGURATION MANAGEMENT	96
3.6 CONTINGENCY PLANNING.....	115
3.7 IDENTIFICATION AND AUTHENTICATION	131
3.8 INCIDENT RESPONSE.....	149
3.9 MAINTENANCE.....	162
3.10 MEDIA PROTECTION	171
3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION	179
3.12 PLANNING	194
3.13 PROGRAM MANAGEMENT	203
3.14 PERSONNEL SECURITY.....	222
3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY	229
3.16 RISK ASSESSMENT.....	238
3.17 SYSTEM AND SERVICES ACQUISITION	249
3.18 SYSTEM AND COMMUNICATIONS PROTECTION	292
3.19 SYSTEM AND INFORMATION INTEGRITY	332
3.20 SUPPLY CHAIN RISK MANAGEMENT.....	363
REFERENCES	374
APPENDIX A GLOSSARY.....	394
APPENDIX B ACRONYMS.....	424
APPENDIX C CONTROL SUMMARIES.....	428

ID.AM-1: Physical devices and systems within the organization are inventoried

CIS CSC 1

COBIT 5 BAI09.01, BAI09.02

ISA 62443-2-1:2009 4.2.3.4

ISA 62443-3-3:2013 SR 7.8

ISO/IEC 27001:2013 A.8.1.1, A.8.1.2

NIST SP 800-53 Rev. 4 CM-8, PM-5

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

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

CM-8 SYSTEM COMPONENT INVENTORY

Control:

- Develop and document an inventory of system components that:
 - Accurately reflects the system;
 - Includes all components within the system;
 - Does not include duplicate accounting of components or components assigned to any other system;
 - Is at the level of granularity deemed necessary for tracking and reporting; and
 - Includes the following information to achieve system component accountability:
[Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and
- Review and update the system component inventory *[Assignment: organization-defined frequency]*.

PUBLICATIONS

SP 800-53A Rev. 5

Assessing Security and Privacy Controls in Information Systems and Organizations



Date Published: January 2022

Supersedes: [SP 800-53A Rev. 4 \(12/18/2014\)](#)

Planning Note (3/30/2022):

As stakeholders use NIST SP 800-53A and its derivative data formats, updates are identified to improve the quality of the publication. Updates can include corrections, clarifications, or other minor changes in the publication that are either editorial or substantive in nature. Any potential updates for SP 800-53A and its derivative data formats that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified. Please report any potential updates to sec-cert@nist.gov.

Author(s)

Joint Task Force

Abstract

This publication provides a methodology and set of procedures for conducting assessments of security and privacy controls employed within systems and organizations within an effective risk management framework. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST Special Publication 800-53, Revision 5. The procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security and privacy control assessments that support organizational risk management processes and are aligned with the stated risk tolerance of the organization. Information on building effective security and privacy assessment plans is also provided with guidance on analyzing assessment results.

Keywords

assessment; assessment plan; assurance; control assessment; FISMA; Privacy Act; privacy controls; Open Security Controls Assessment Language; OSCAL; privacy requirements; Risk Management Framework; security controls; security requirements

Control Families

None selected

DOCUMENTATION

Publication:

[SP 800-53A Rev. 5 \(DOI\)](#)[Local Download](#)

Supplemental Material:

[Potential Updates \[3-30-2022\] \(xls\)](#)[Download Spreadsheet \(xls\)](#)[Download Plain Text \(txt\)](#)[Download CSV \(other\)](#)[README for CSV \(txt\)](#)[OSCAL GitHub \(web\)](#)

Other Parts of this Publication:

[SP 800-53 Rev. 5](#)[SP 800-53B](#)

Document History:

08/03/21: [SP 800-53A Rev. 5 \(Draft\)](#)01/25/22: [SP 800-53A Rev. 5 \(Final\)](#)

TOPICS

Security and Privacy

[controls assessment](#)

Laws and Regulations

[Federal Information Security Modernization Act](#)NIST Special Publication 800-53A
Revision 5Assessing Security and Privacy Controls
in Information Systems and
Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53Ar5>

January 2022

U.S. Department of Commerce
Gina M. Raimondo, SecretaryNational Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology<https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final>

MIS 5206 Protecting Information Assets

Table of Contents

CHAPTER ONE INTRODUCTION	1
1.1 PURPOSE AND APPLICABILITY	1
1.2 TARGET AUDIENCE	4
1.3 RELATED PUBLICATIONS AND ASSESSMENT PROCESSES	4
1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION	5
CHAPTER TWO THE FUNDAMENTALS	6
2.1 ASSESSMENTS WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE	6
2.2 STRATEGY FOR CONDUCTING CONTROL ASSESSMENTS	7
2.3 BUILDING AN EFFECTIVE ASSURANCE CASE	8
2.4 ASSESSMENT PROCEDURES	9
CHAPTER THREE THE PROCESS	14
3.1 PREPARING FOR SECURITY AND PRIVACY CONTROL ASSESSMENTS	14
3.2 DEVELOPING SECURITY AND PRIVACY ASSESSMENT PLANS	17
3.3 CONDUCTING SECURITY AND PRIVACY CONTROL ASSESSMENTS	23
3.4 ANALYZING ASSESSMENT REPORT RESULTS	25
3.5 ASSESSING SECURITY AND PRIVACY CAPABILITIES	26
APPENDIX A REFERENCES	A-1
APPENDIX B GLOSSARY	B-1
APPENDIX C ACRONYMS	C-1
APPENDIX D ASSESSMENT METHOD DESCRIPTIONS	D-1
APPENDIX E PENETRATION TESTING	E-1
APPENDIX F SECURITY ASSESSMENT PROCEDURES	F-1
APPENDIX G ASSESSMENT REPORTS	G-1
APPENDIX H ASSESSMENT CASES	H-1
APPENDIX I ONGOING ASSESSMENT AND AUTOMATION	I-1
APPENDIX J PRIVACY ASSESSMENT PROCEDURES	J-1

ID.AM-1: Physical devices and systems within the organization are inventoried

CIS CSC 1
COBIT 5 BAI09.01, BAI09.02
ISA 62443-2-1:2009 4.2.3.4
ISA 62443-3-3:2013 SR 7.8
ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
NIST SP 800-53 Rev. 4 CM-8, PM-5

CM-8		INFORMATION SYSTEM COMPONENT INVENTORY	
ASSESSMENT OBJECTIVE: <i>Determine if the organization:</i>			
CM-8(a)	CM-8(a)(1)	<i>develops and documents an inventory of information system components that accurately reflects the current information system;</i>	
	CM-8(a)(2)	<i>develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system;</i>	
	CM-8(a)(3)	<i>develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting;</i>	
	CM-8(a)(4)	CM-8(a)(4)[1]	<i>defines the information deemed necessary to achieve effective information system component accountability;</i>
		CM-8(a)(4)[2]	<i>develops and documents an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability;</i>
CM-8(b)	CM-8(b)[1]	<i>defines the frequency to review and update the information system component inventory; and</i>	
	CM-8(b)[2]	<i>reviews and updates the information system component inventory with the organization-defined frequency.</i>	
POTENTIAL ASSESSMENT METHODS AND OBJECTS:			
Examine: [SELECT FROM: Configuration management policy; procedures addressing information system component inventory; configuration management plan; security plan; information system inventory records; inventory reviews and update records; other relevant documents or records].			
Interview: [SELECT FROM: Organizational personnel with responsibilities for information system component inventory; organizational personnel with information security responsibilities; system/network administrators].			
Test: [SELECT FROM: Organizational processes for developing and documenting an inventory of information system components; automated mechanisms supporting and/or implementing the information system component inventory].			

<https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final>

MIS 5206 Protecting Information Assets

Which Asset Management Subcategories of activities relate to a Risk Assessment (RA) of impacts resulting from a breach in data confidentiality, integrity and/or availability?

Function Unique Identifier	Function	Category Unique Identifier	Category	Function	Category	Subcategory	Informative References				
ID	Identify	ID.AM	Asset Management	IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5				
		ID.BE	Business Environment			ID.AM-2: Software platforms and	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5				
		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	IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-2: Software platforms and	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8				
DE		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value									
RS		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value									
RC	Recover	RS.AN	Analysis				CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6				
		RS.MI	Mitigation								
		RS.IM	Improvements								
		RC.RP	Recovery Planning								
		RC.IM	Improvements				CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9				
		RC.CO	Communications								
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value				ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6				
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value				ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11				

MIS 5206 Protecting Information Assets

NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53Ar5>

January 2022



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology

RA-02	SECURITY CATEGORIZATION	
	ASSESSMENT OBJECTIVE: <i>Determine if:</i>	
	RA-02a.	the system and the information it processes, stores, and transmits are categorized;
	RA-02b.	the security categorization results, including supporting rationale, are documented in the security plan for the system;
	RA-02c.	the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-02-Examine	[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing security categorization of organizational information and systems; security categorization documentation; system security plan; privacy plan; other relevant documents or records].
	RA-02-Interview	[SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities; organizational personnel with security and privacy responsibilities].
	RA-02-Test	[SELECT FROM: Organizational processes for security categorization].

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

Each function of the NIST Cybersecurity Framework's workflow is associated with a set of categories of cybersecurity "activities". These are

- ***Sorted alphabetically by their Category Unique Identifier***
- ***Not organized as an ordered hierarchy or sequence of activities***

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

Framework's alphabetical ordering of activities is problematic...

Category	Subcategory	Informative References
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
	ID.RA-3: Threats, both internal and external, are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
	ID.RA-4: Potential business impacts and likelihoods are identified	CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
	ID.RA-6: Risk responses are identified and prioritized	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9

NIST Risk Assessment Controls

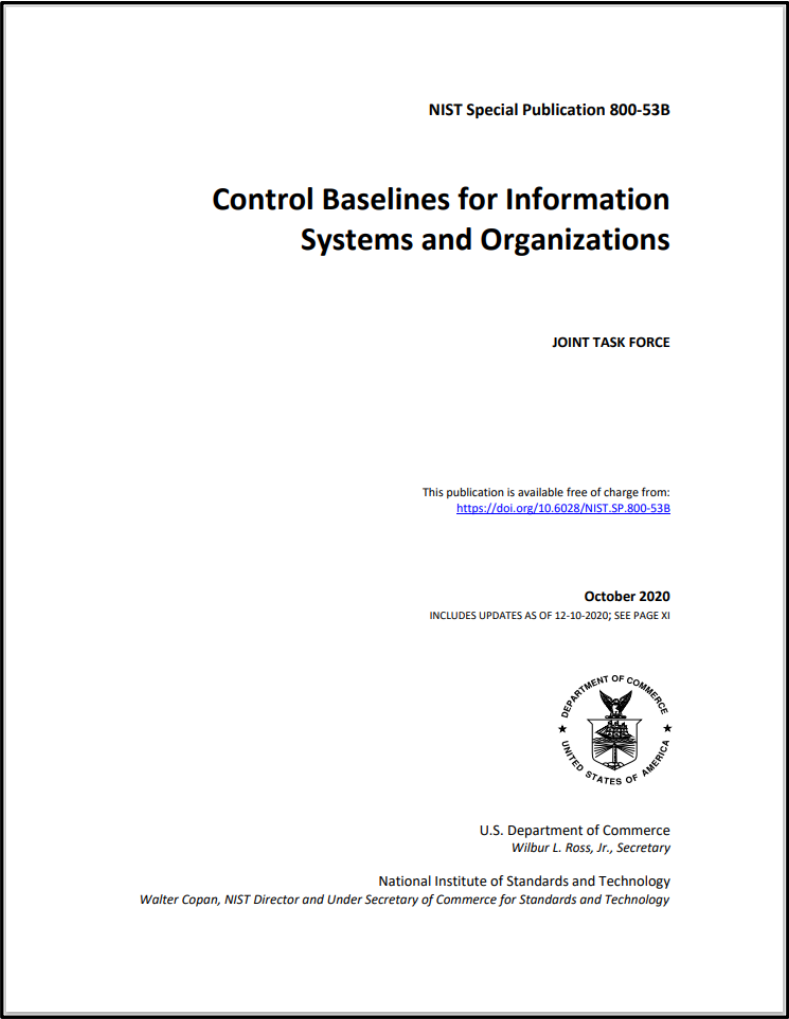


TABLE 3-16: RISK ASSESSMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
RA-1	Policy and Procedures	X	X	X	X
RA-2	Security Categorization		X	X	X
RA-2(1)	IMPACT-LEVEL PRIORITIZATION				
RA-3	Risk Assessment	X	X	X	X
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT		X	X	X
RA-3(2)	USE OF ALL-SOURCE INTELLIGENCE				
RA-3(3)	DYNAMIC THREAT AWARENESS				
RA-3(4)	PREDICTIVE CYBER ANALYTICS				
RA-4	Risk Assessment Update	W: Incorporated into RA-3.			
RA-5	Vulnerability Monitoring and Scanning		X	X	X
RA-5(1)	UPDATE TOOL CAPABILITY	W: Incorporated into RA-5.			
RA-5(2)	UPDATE VULNERABILITIES TO BE SCANNED		X	X	X
RA-5(3)	BREADTH AND DEPTH OF COVERAGE				
RA-5(4)	DISCOVERABLE INFORMATION				X
RA-5(5)	PRIVILEGED ACCESS			X	X
RA-5(6)	AUTOMATED TREND ANALYSES				
RA-5(7)	AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	W: Incorporated into CM-8.			
RA-5(8)	REVIEW HISTORIC AUDIT LOGS				
RA-5(9)	PENETRATION TESTING AND ANALYSES	W: Incorporated into CA-8.			
RA-5(10)	CORRELATE SCANNING INFORMATION				
RA-5(11)	PUBLIC DISCLOSURE PROGRAM		X	X	X
RA-6	Technical Surveillance Countermeasures Survey				
RA-7	Risk Response	X	X	X	X
RA-8	Privacy Impact Assessments	X			
RA-9	Criticality Analysis			X	X
RA-10	Threat Hunting				

A better way than alphabetical organization for thinking about information security control families...

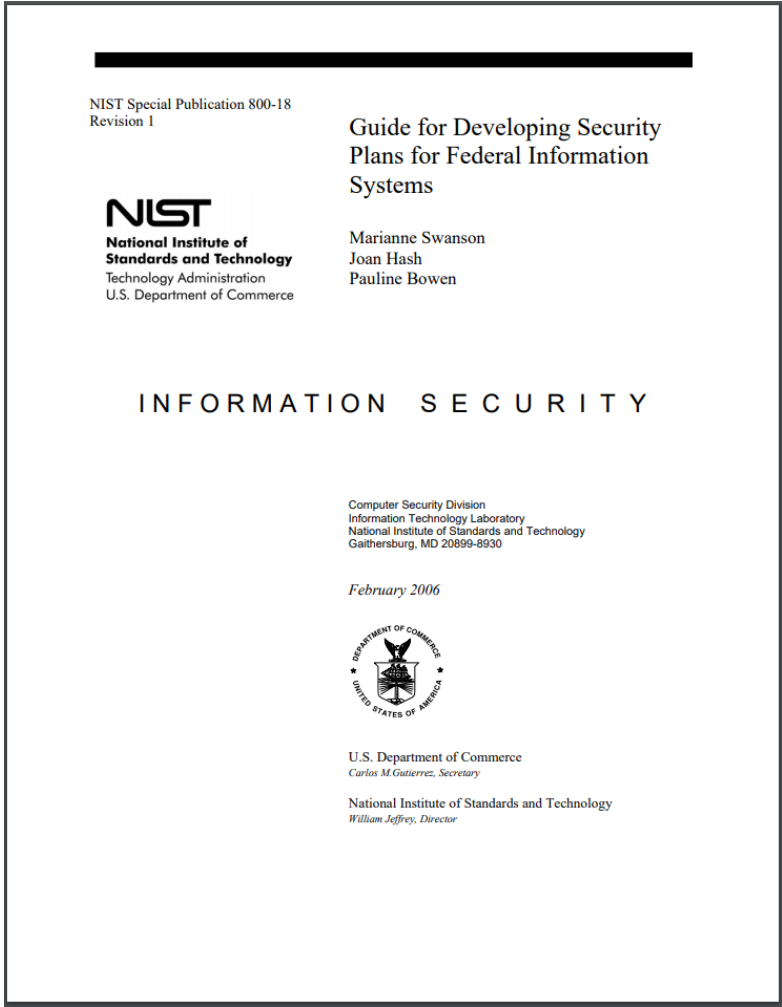


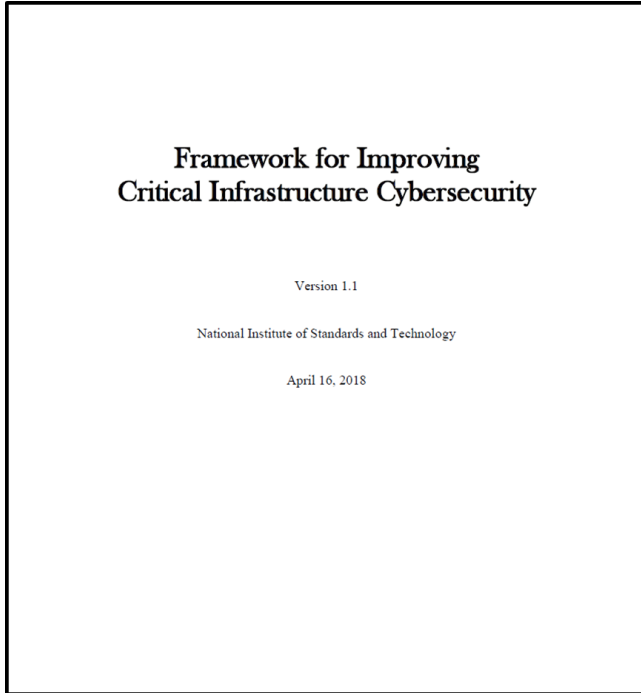
TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

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

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Overlapping, complementary IT security frameworks



NIST Cybersecurity Framework provides a workflow of activities used to identify gaps and measure maturity of an organization's information security

MIS 5206 Protecting Information Assets



COBIT provides guidance for enterprise IT governance and management



NIST SP 800-53 outlines baselines of cybersecurity controls for information systems and checklists for auditing the controls

Agenda

- ✓ Daily class schedule – and schedule of breaks
- ✓ Introductions
- ✓ Case study analysis
- ✓ Frameworks for Protecting Information Assets