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
- Test taking tip
- Quiz

Introductions

Meet in Teams via Zoom Break Out Rooms for 10 minutes and figure out:

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

When we return, each team's representative will:

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

Case Study Analysis – Group Work – Meet in Breakout Rooms

1. IT governance questions:
   - Which organization does Dave Ballard report into?
   - Which organization does Nick Francesco report into?
   - 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?
2. Is this a problem?
   - If so, what kind of problem is it?
3. What evidence is the basis for Information Security Office (IS0) conclusion that the Dean's stolen laptop did not contain personally identifiable information on RIT students, faculty, or staff?
4. Is the ISO's conclusion valid? Why or why not?

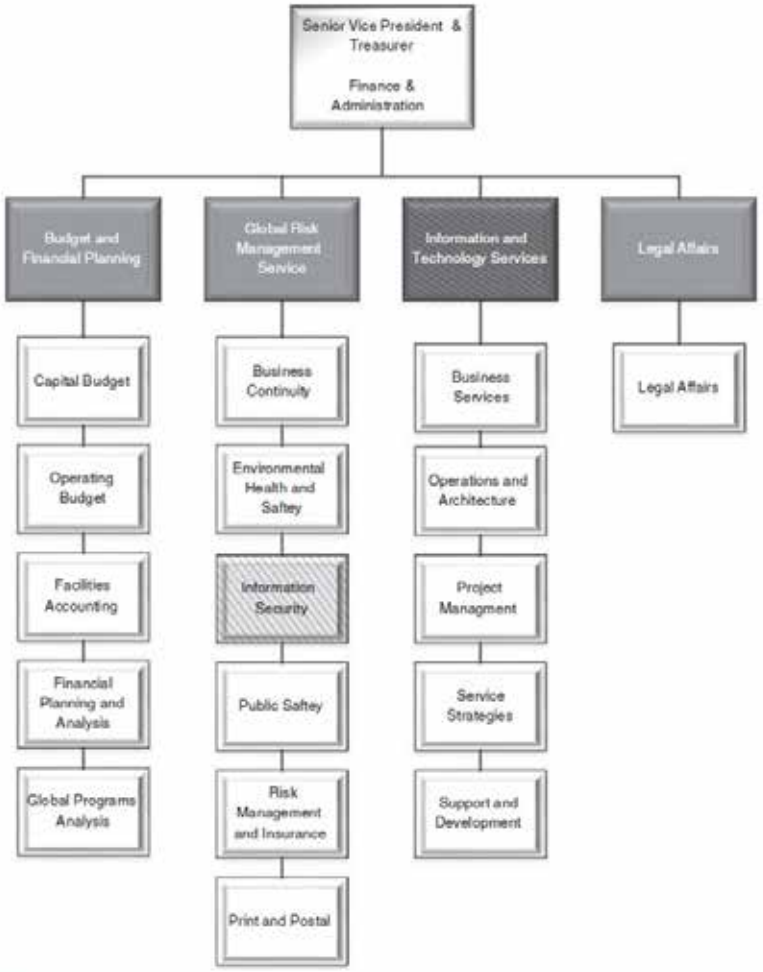


Figure C1 Partial RIT administrative organization chart.

Case Study Analysis: "Snowfall and a stolen laptop"

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?
2. What information security reporting or organizational governance relationship exists between ISO and the organization(s) Ballard and Francesco report into?
3. Is this a problem?
   - What kind of problem is it?

4. What evidence is the basis for Information Security Office (IS0) 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=1100ljkxAPpG

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.'

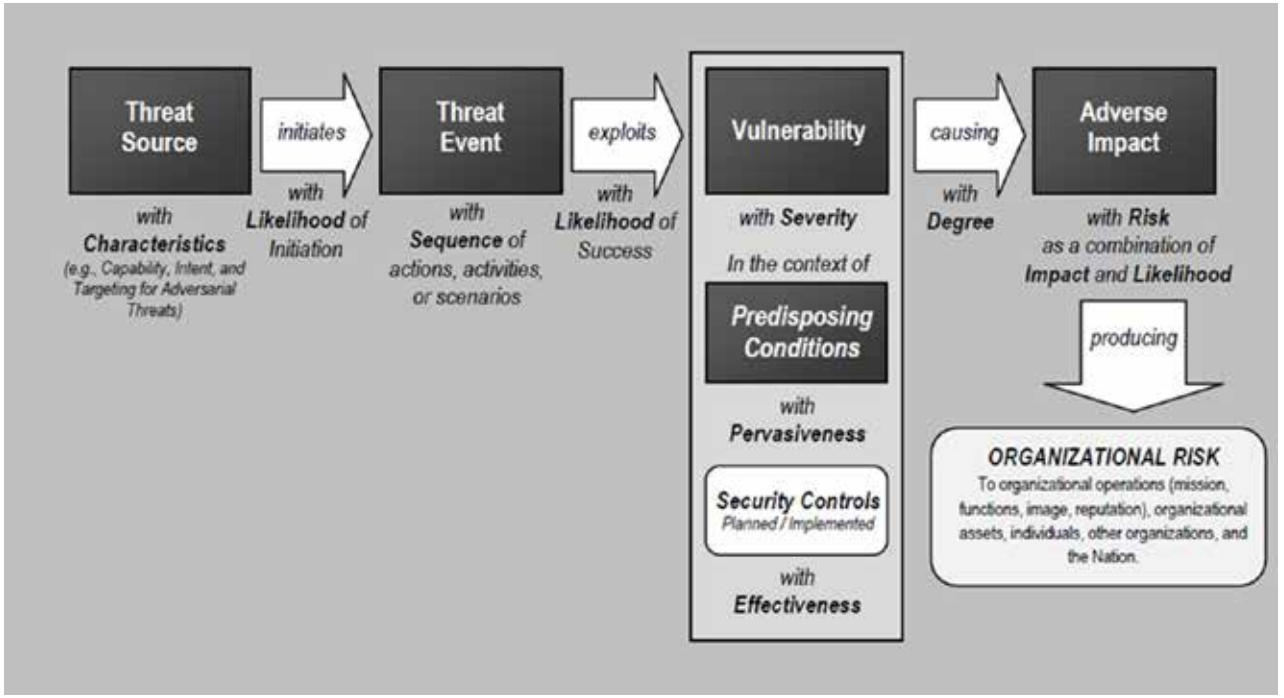
6. **Was Francesco correct or mistaken in his use of the term "proprietary" Saunders data" ?**

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

8. 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?***

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

What kind of <u>threat source</u> 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
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

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

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

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

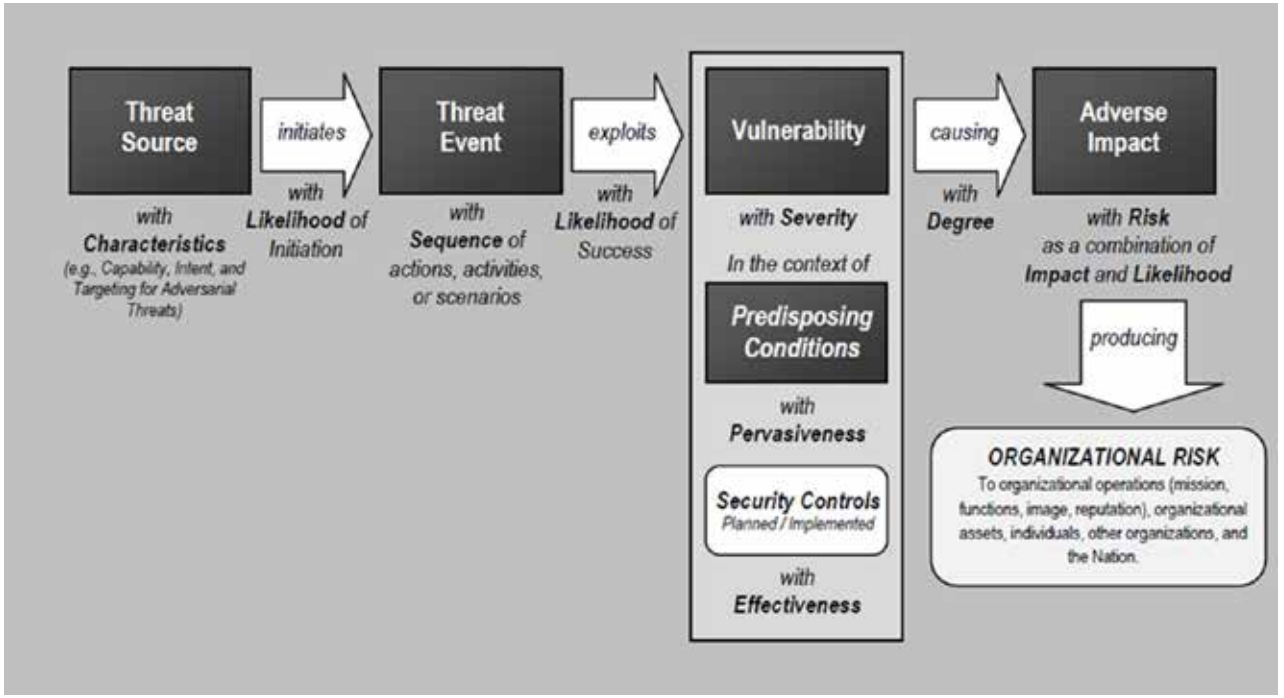
A. Threat source
- i. Capability
- ii. Intent
- iii. Targeting

B. Threat event
- i. Attack type
- ii. Likelihood of attack initiation

C. Vulnerability
- i. Weakness type
- ii. Likelihood attack succeeds

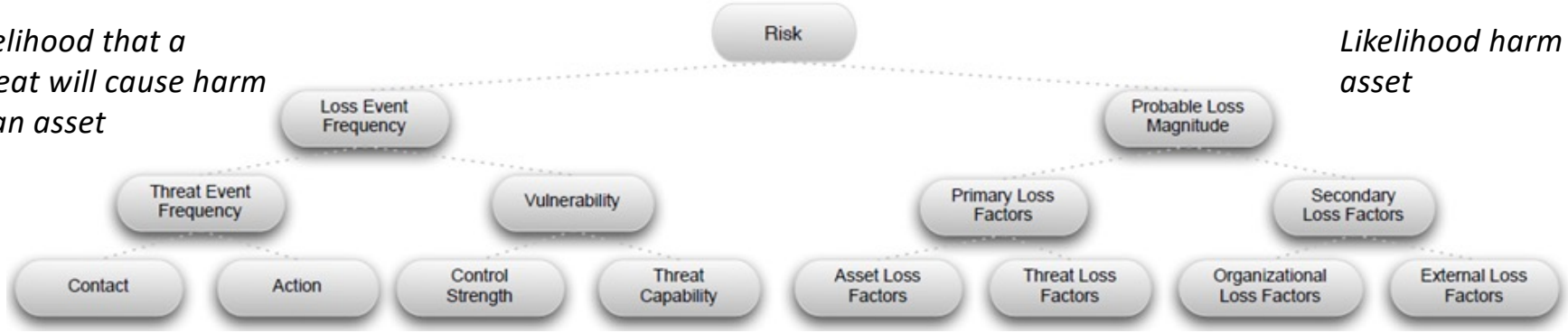
D. Impact
- i. Impact type
- ii. Severity of impact
- iii. Overall likelihood

E. Risk



10. How should we organize and present the risks?

Likelihood that a threat will cause harm to an asset



Likelihood harm to an asset

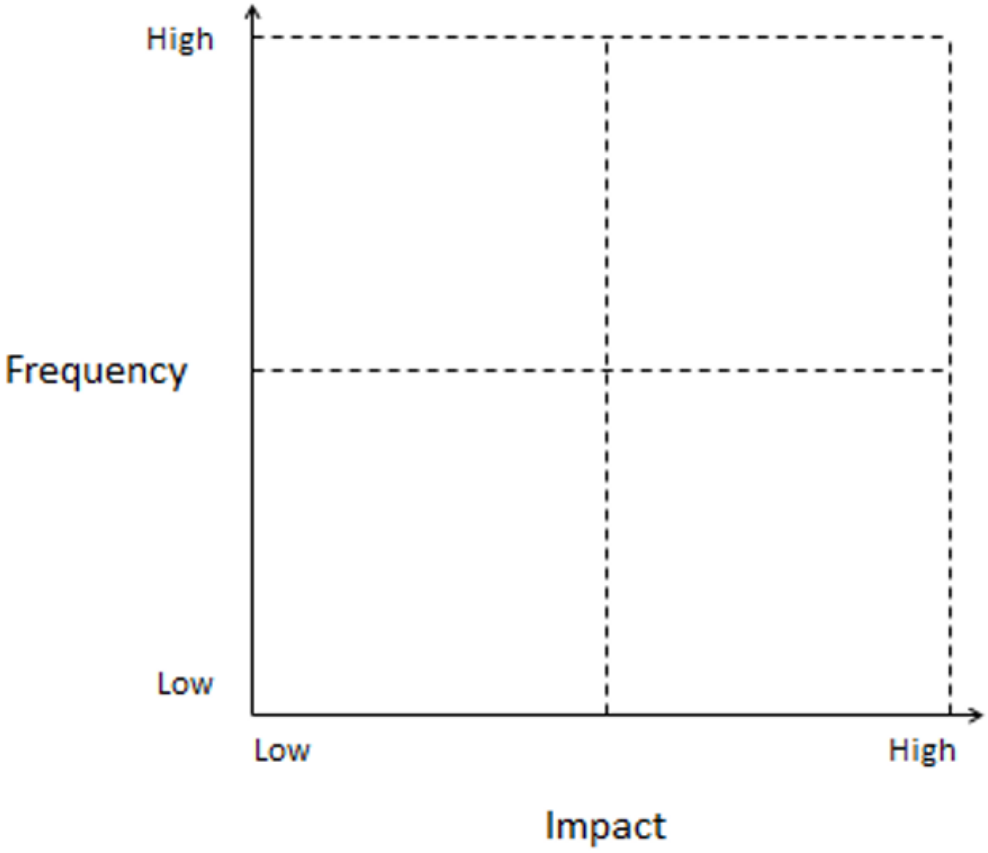
Factor Analysis of Information Risk (FAIR) framework

- 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?

https://www.fairinstitute.org/what-is-fair

10. How should we organize and present the risks?

Risk	Impact	Frequency



Case Study Analysis: “Snowfall and a stolen laptop”

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

Rochester Institute of Technology (RIT)

Saunders College of Business

Ashok Rao

Janis Gogan • 3rd

Professor at Bentley U and President at Cases for Action

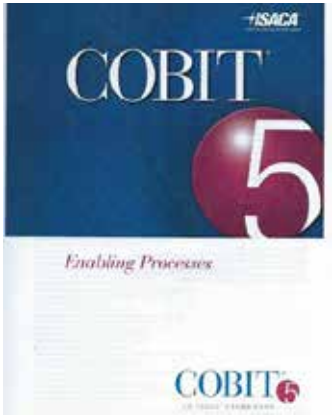
Bentley University • Harvard University

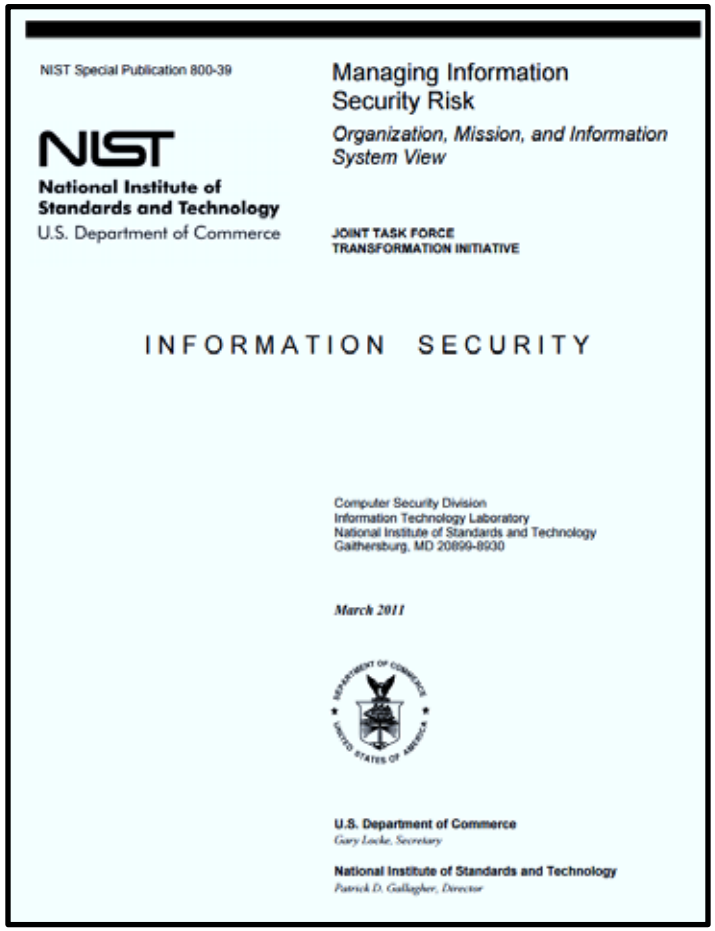
Greater Boston Area • 274

Frameworks for Protecting Information Assets…

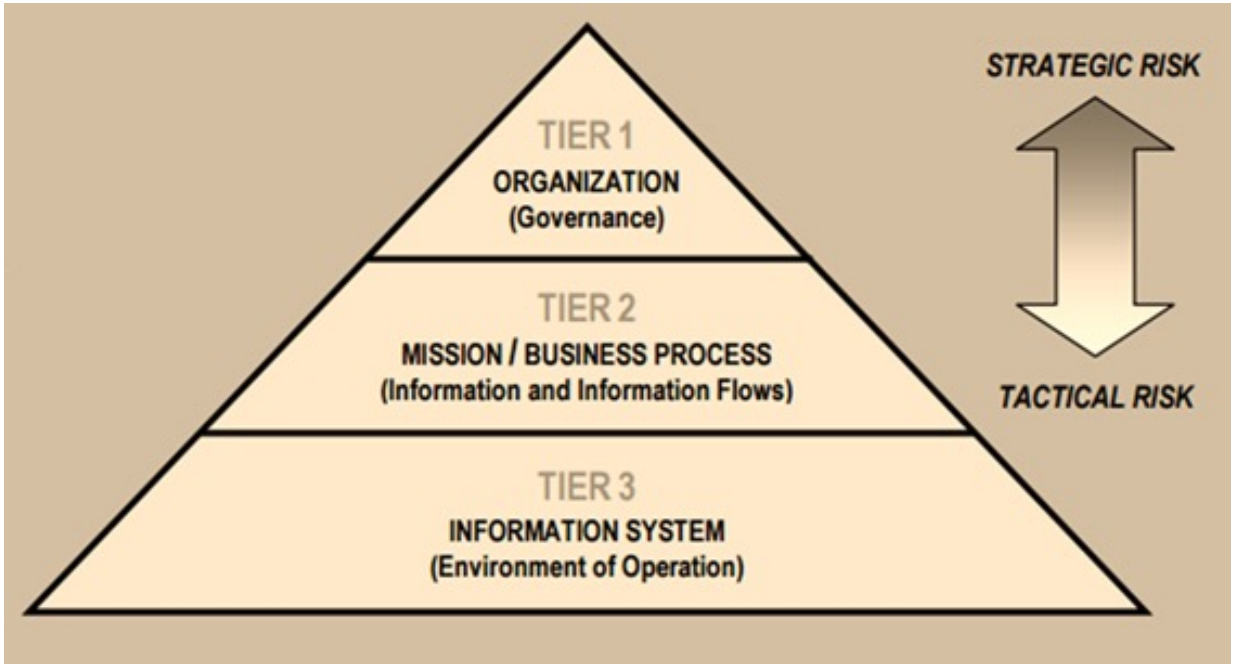
A leading example of information security risk management

- 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

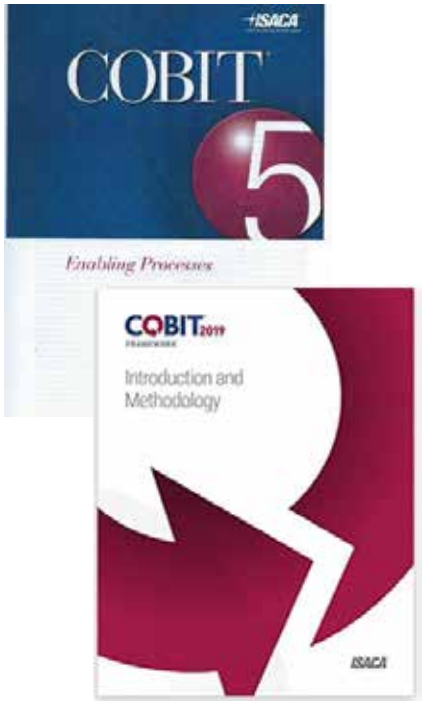


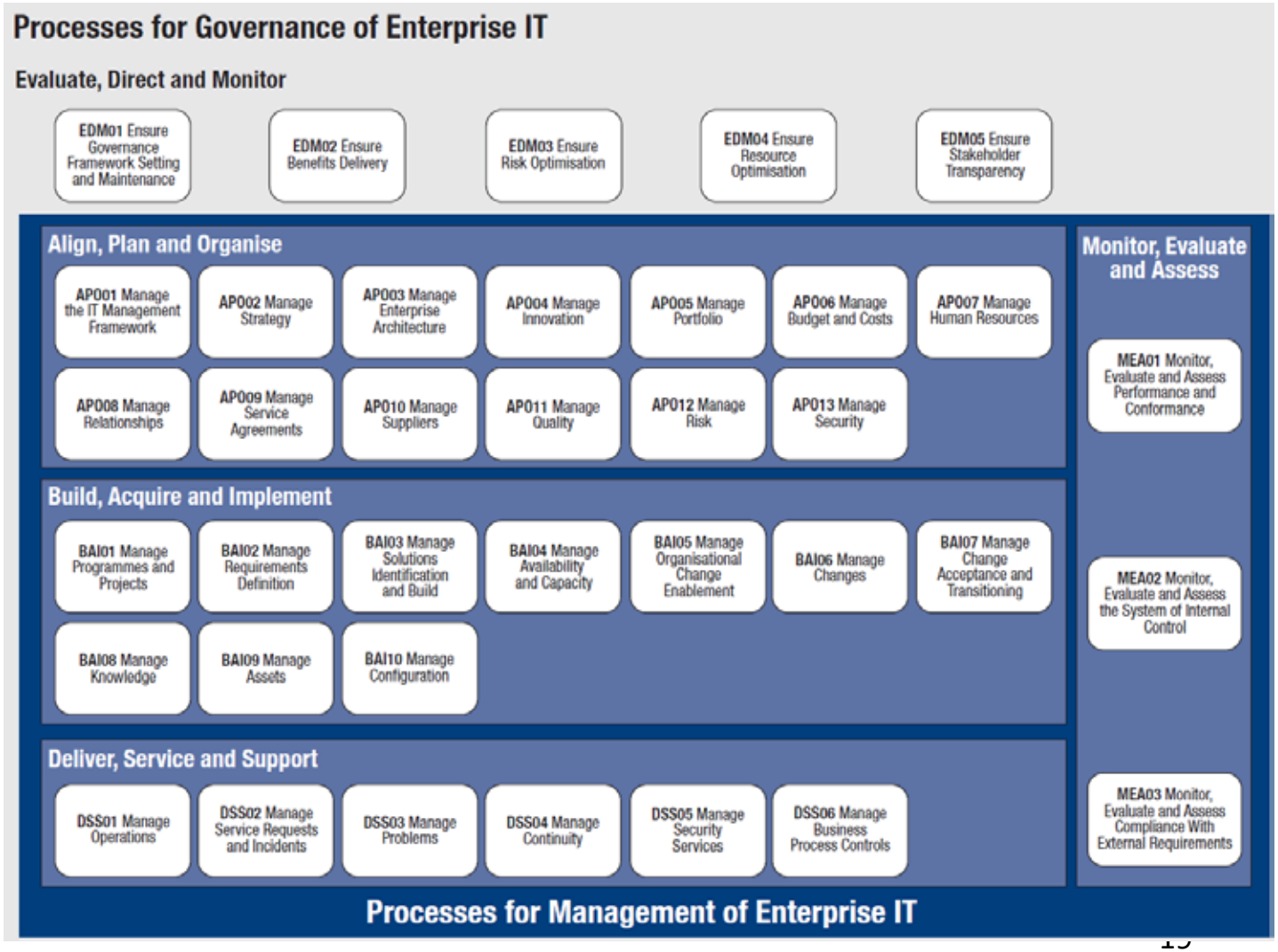


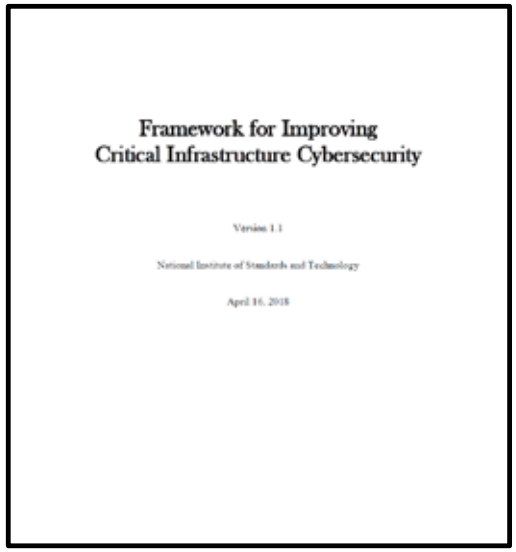
An Overview of Frameworks for Protecting Information Assets




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


ISACA
COBIT 5
Enabling Processes
COBIT 2019
Introduction and Methodology
ISACA

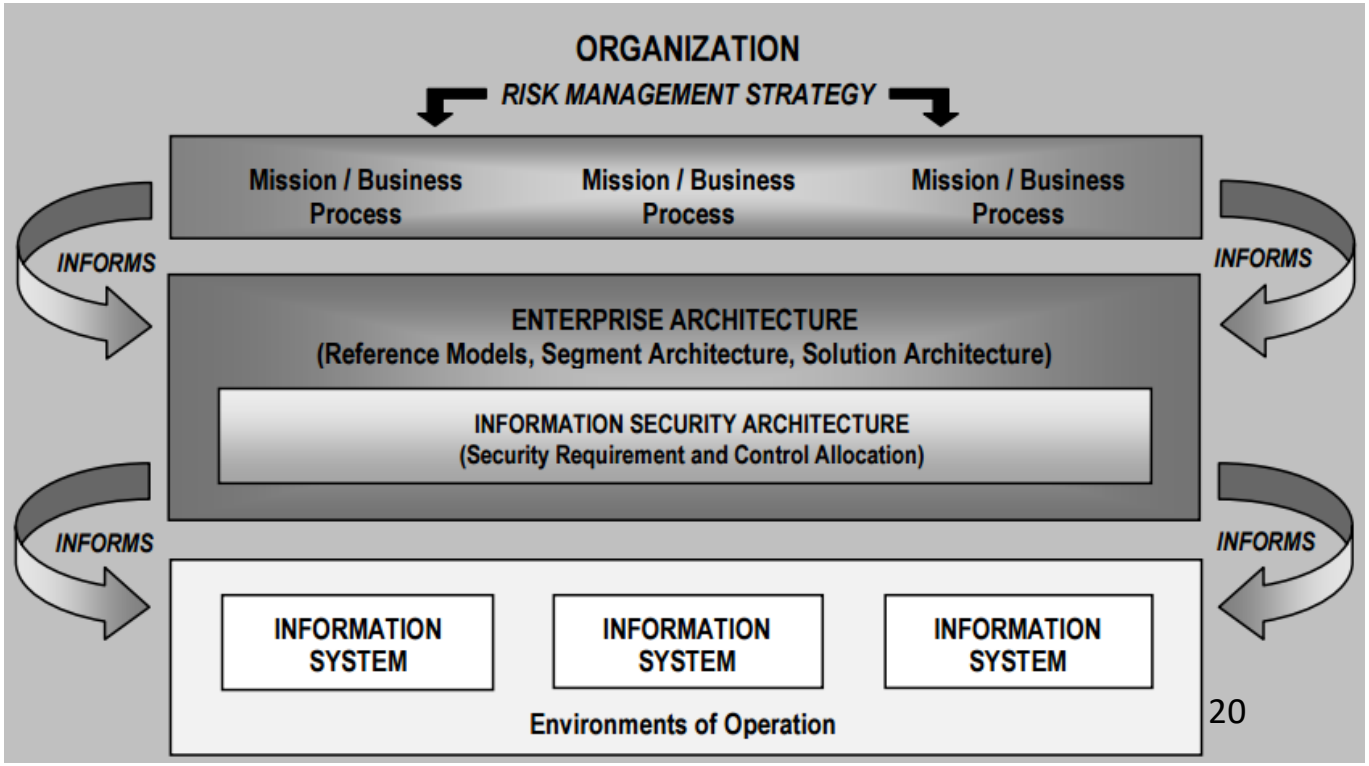

Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
AP001 Manage 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

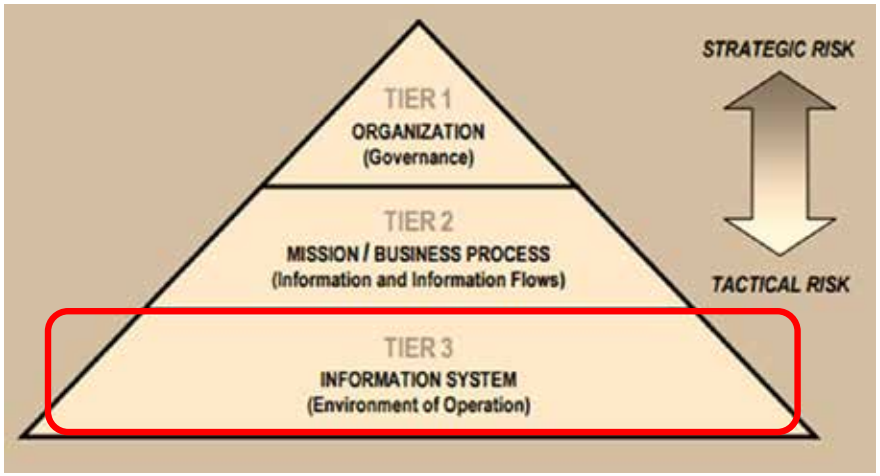

Framework for Improving
Critical Infrastructure Cybersecurity

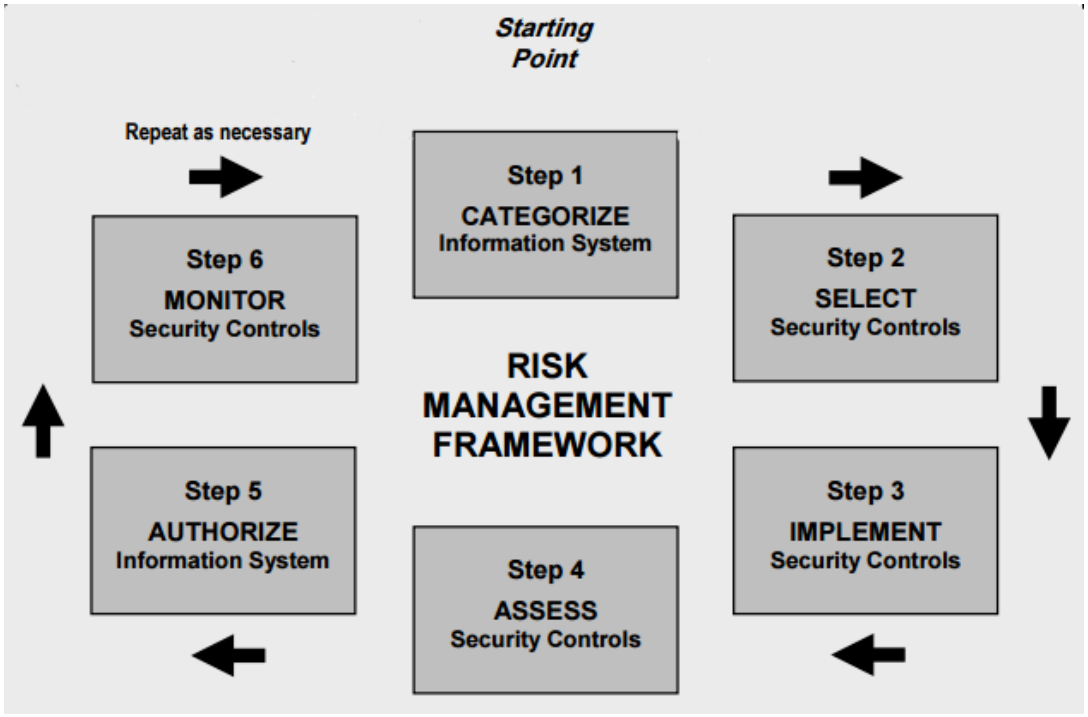
Version 1.1

National Institute of Standards and Technology

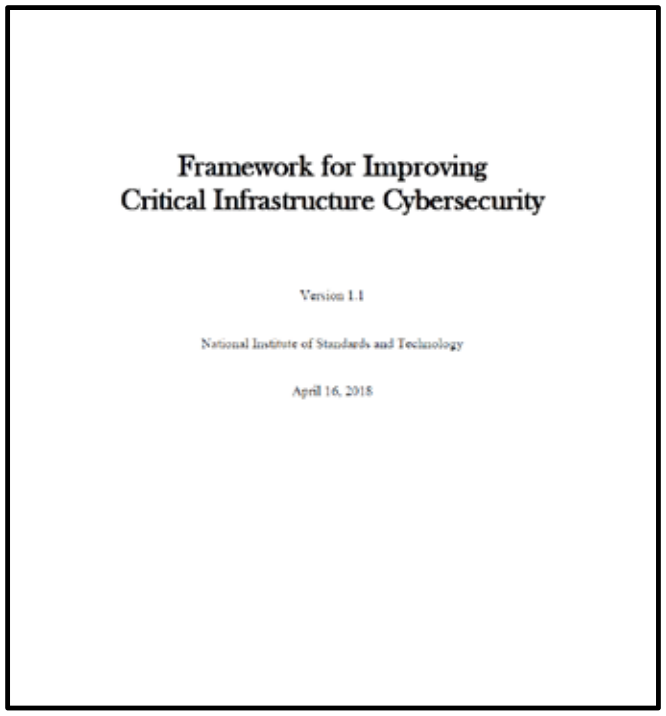
April 16, 2018




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


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

NIST Cybersecurity Framework


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

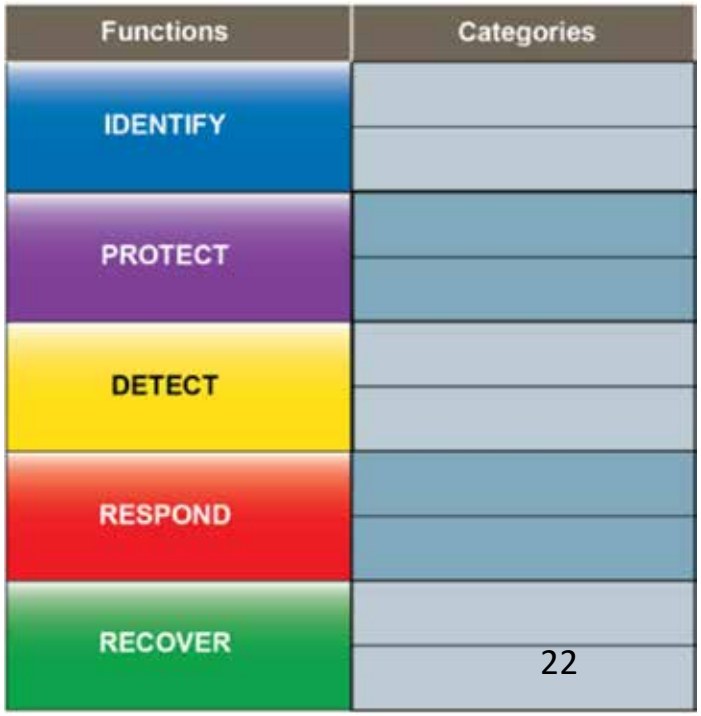
April 16, 2018

Refers to and builds on many principles of ISO/IEC 27001 standard

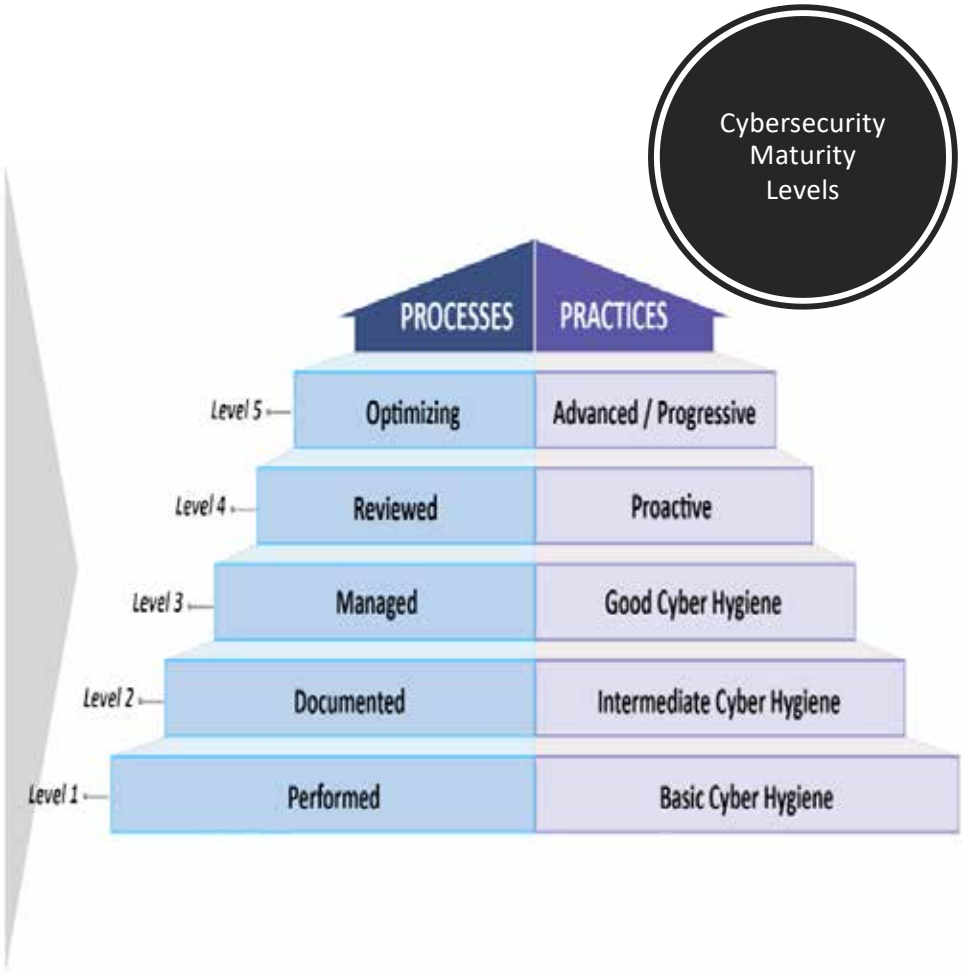
Goes way beyond IT and physical security environment

…by also including:

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



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)

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

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 Category of cybersecurity activities is further broken down into subcategories

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

The NIST SP 800 information references pertain to specific information security controls

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
DE	Detect		
RS	Respond		
		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 R 7.8 A.8.1.1, A.8.1.2, A.12.5.1 **4** CM-8, PM-5
			2.3.4 A.13.2.1, A.13.2.2 **4** AC-4, CA-3, CA-9, PL-8
			APO10.04, DSS01.02 A.11.2.6 **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

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

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

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	• 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	• 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.	• Percent of used licences against paid-for licences
2. Assets are maintained at optimal levels.	• 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			C			C												I	C	C	A	R	C			
BAI																									C	
BAI																										
BAI																										
BAI																										

Manage licences.

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

BAI09 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	**Description**	**Description**	**To**
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.	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	
	From	**Description**	**Description**	**To**
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.			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.				

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
DE	Detect		
RS	Respond		
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

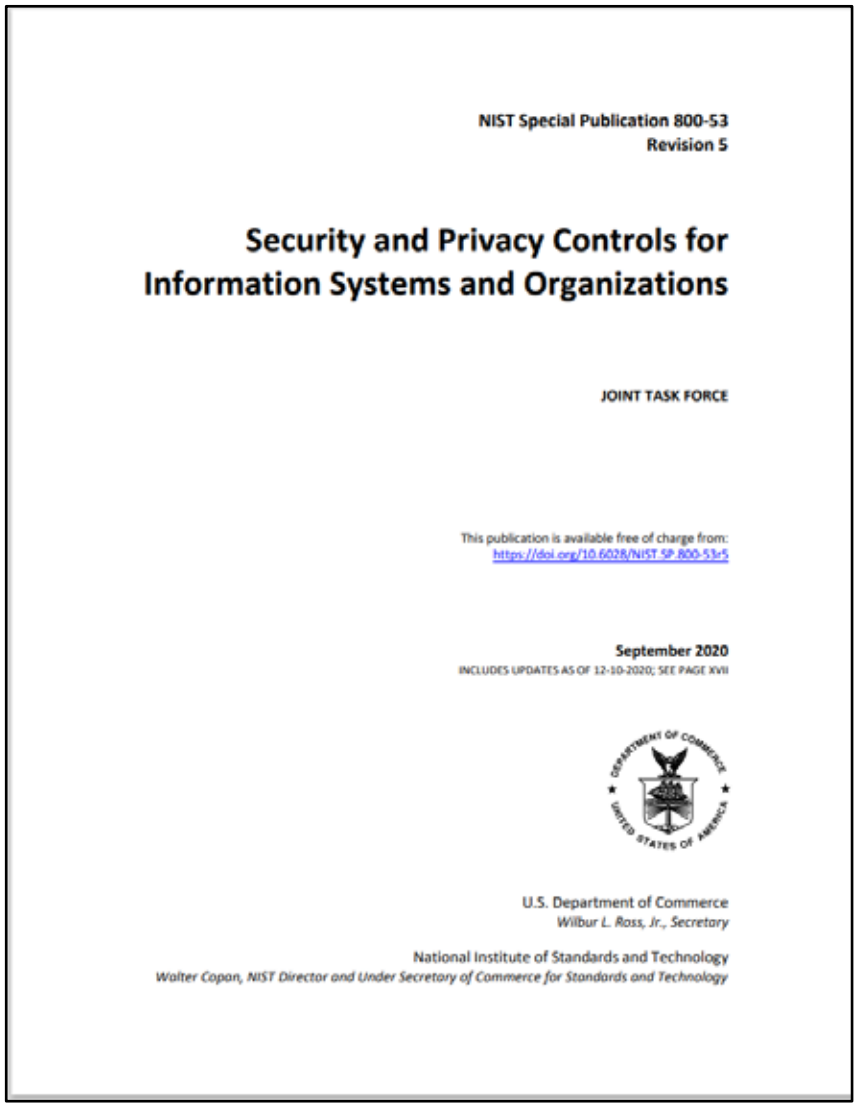
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives 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 R 7.8 A.8.1.1, A.8.1.2, A.12.5.1 4 CM-8, PM-5
			2.3.4 A.13.2.1, A.13.2.2 4 AC-4, CA-3, CA-9, PL-8
			APO10.04, DSS01.02 A.11.2.6 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

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

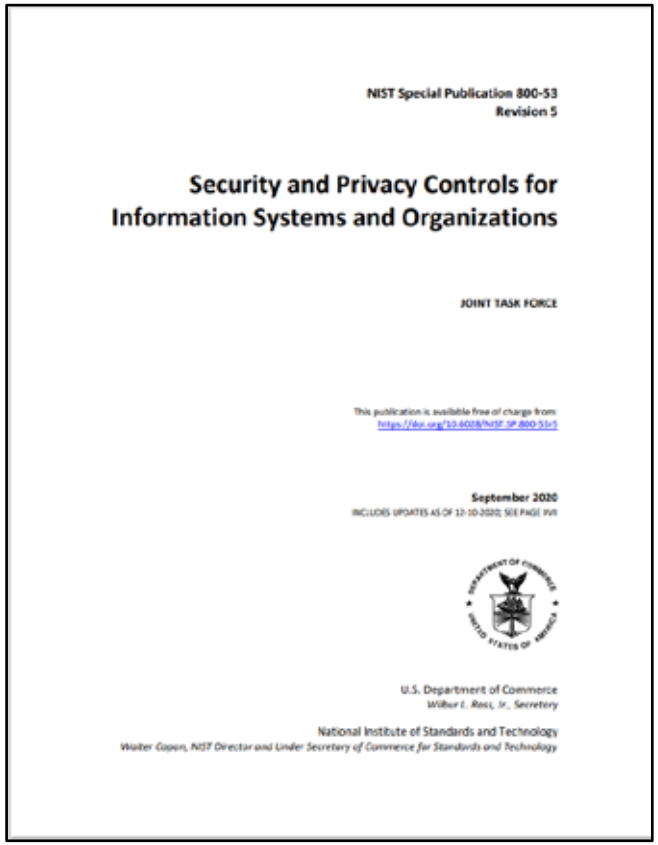
Each subcategory or activity is associated or cross-referenced to information references

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



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



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

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
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

Table of Contents

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:

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;
2. Includes all components within the system;
3. Does not include duplicate accounting of components or components assigned to any other system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability: [*Assignment: organization-defined information deemed necessary to achieve effective system component accountability*]; and

b. Review and update the system component inventory [*Assignment: organization-defined frequency*].

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

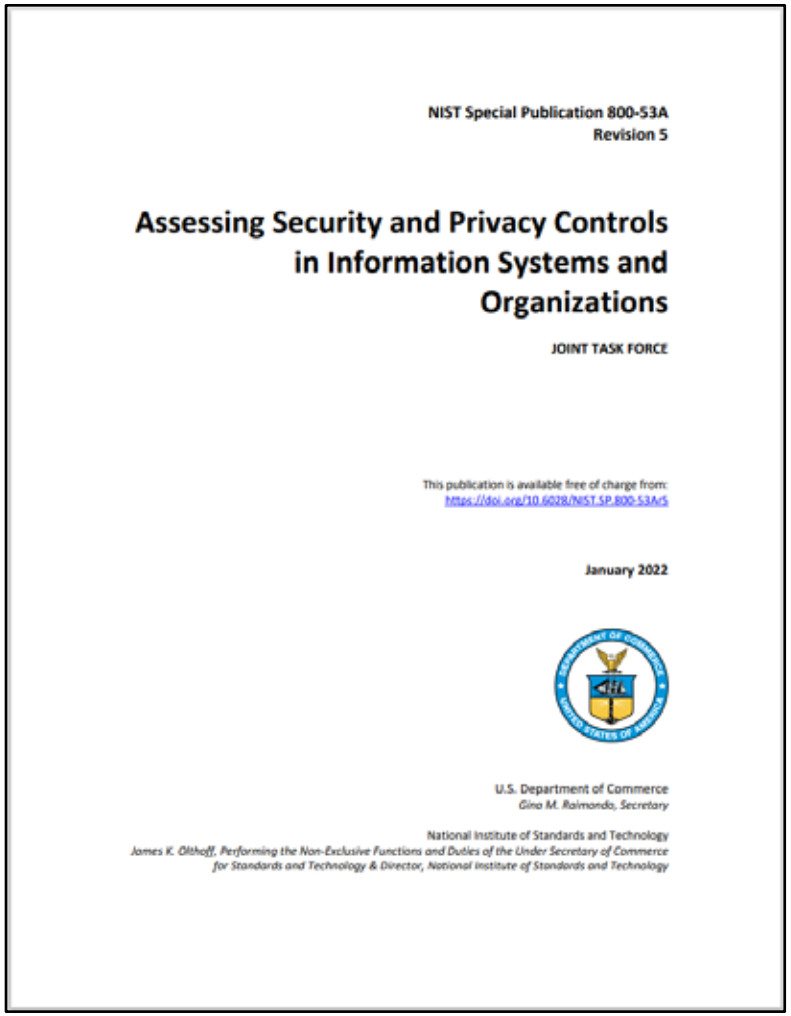


Table of Contents

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

CM-8	INFORMATION SYSTEM COMPONENT INVENTORY		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	CM-8(a)	**CM-8(a)(1)**	*develops and documents an inventory of information system components that accurately reflects the current information system;*
		CM-8(a)(2)	*develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system;*
		CM-8(a)(3)	*develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting;*
		CM-8(a)(4)	**CM-8(a)(4)[1]** *defines the information deemed necessary to achieve effective information system component accountability;*
			CM-8(a)(4)[2] *develops and documents an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability;*
	CM-8(b)	**CM-8(b)[1]**	*defines the frequency to review and update the information system component inventory; and*
		CM-8(b)[2]	*reviews and updates the information system component inventory with the organization-defined frequency.*
	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].		

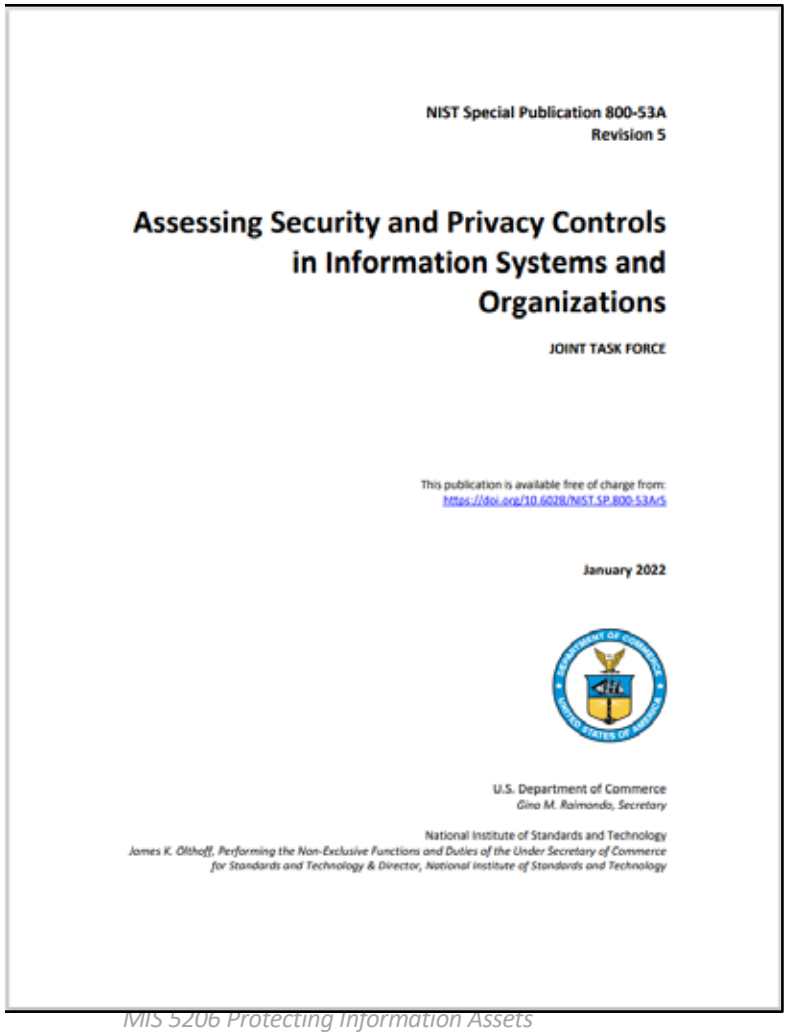
Which Asset Management Subcategories of activities relate to a Risk Assessment (RA) of impacts resulting from a breach in data confidentiality, integrity and/or availability?

Function Unique Identifier	Function	Category Unique Identifier	Category
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
DE			
RS			
		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	**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
			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
			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

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



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: *Determine if:*	
	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
RC	Recover		

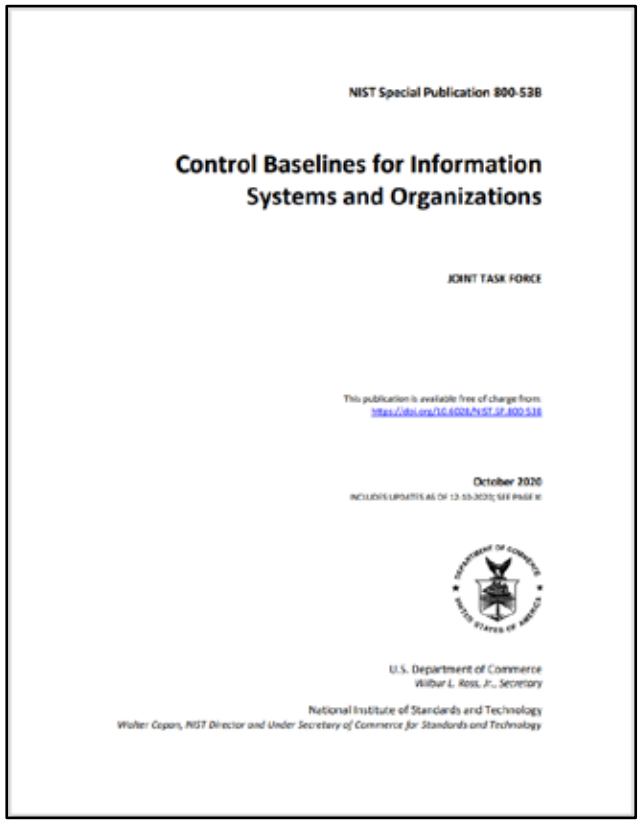
SP 800-53

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN
RA-1	**Risk Assessment Policy and Procedures**	
RA-2	**Security Categorization**	
RA-3	**Risk Assessment**	
RA-4	**Risk Assessment Update**	X
RA-5	**Vulnerability Scanning**	

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



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

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

October 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE iii

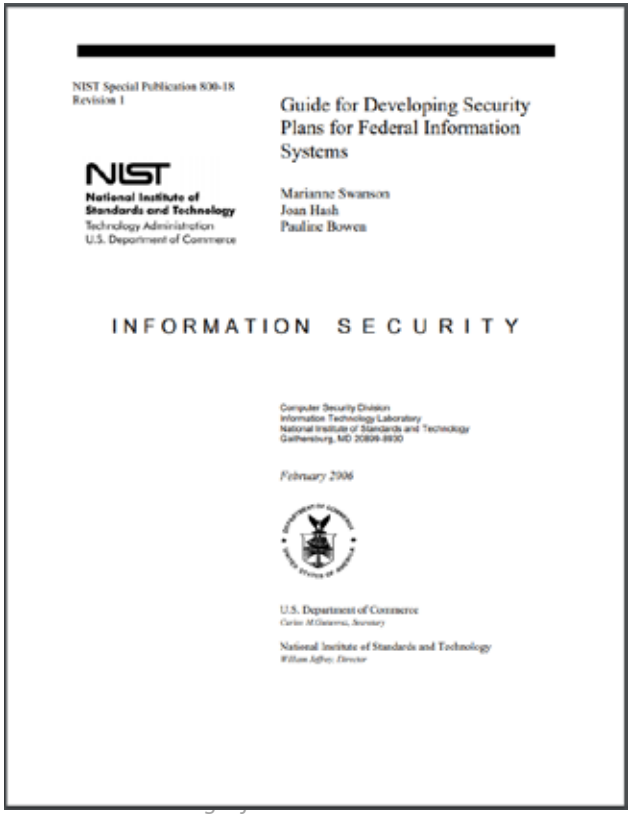
U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

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

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…



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

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

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

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

February 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

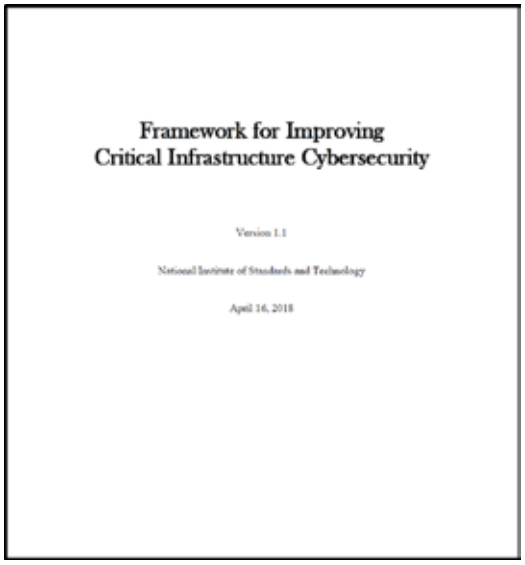
TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

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


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

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

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

Test Taking Tip

- Read the answers first -

This contradicts many people's test taking recommendations…

…but, it works. Here's why:

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

Test Taking Tip

Example:

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

Test Taking Tip

Example:

Which of the following represents the GREATEST potential risk in an Electronic Data Interchange (EDI) environment?

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

Test Taking Tip

Example:

Which of the following represents the GREATEST potential risk in an Electronic Data Interchange (EDI) environment?

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

Answer: A

Quiz

1. Which of the choices below is the most often used criteria to determine the classification of a business object?

   a. Value
   b. Useful life
   c. Age
   d. Personal association

Quiz – Unit #2

1. Which of the choices below is the most often used criteria to determine the classification of a business object?

   a. Value
   b. Useful life
   c. Age
   d. Personal association

Quiz

2. Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited
b. A company resource that is lost due to an incident
c. The minimum loss associated with an incident
d. A potential incident that could cause harm

Quiz

2. Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited
b. A company resource that is lost due to an incident
c. The minimum loss associated with an incident
d. A potential incident that could cause harm

Quiz

3. Which statement below best describes the purpose of risk analysis?

a. To develop a clear cost-to-value ratio for implementing security controls
b. To influence the system design process
c. To influence site selection decisions
d. To quantify the impact of potential threats

Quiz

3. Which statement below best describes the purpose of risk analysis?

a. To develop a clear cost-to-value ration for implementing security controls
b. To influence the system design process
c. To influence site selection decisions
d. To quantify the impact of potential threats

Quiz

4. What is an ARO?

a. A dollar figure assigned to a single event
b. The annual expected financial loss to an organization from a threat
c. A number that represents the estimated frequency of an expected event
d. The percentage of loss that would be realized for a specific asset if a threat occurred

Quiz

4. What is an ARO?

a. A dollar figure assigned to a single event
b. The annual expected financial loss to an organization from a threat
c. A number that represents the estimated frequency of an expected event
d. The percentage of loss that would be realized for a specific asset if a threat occurred

Quiz

5. Which group represents the most likely source of an asset loss through in appropriate computer use?

a. Crackers
b. Hackers
c. Employees
d. Saboteurs

Quiz

5. Which group represents the most likely source of an asset loss through in appropriate computer use?

a. Crackers
b. Hackers
c. Employees
d. Saboteurs

Agenda

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