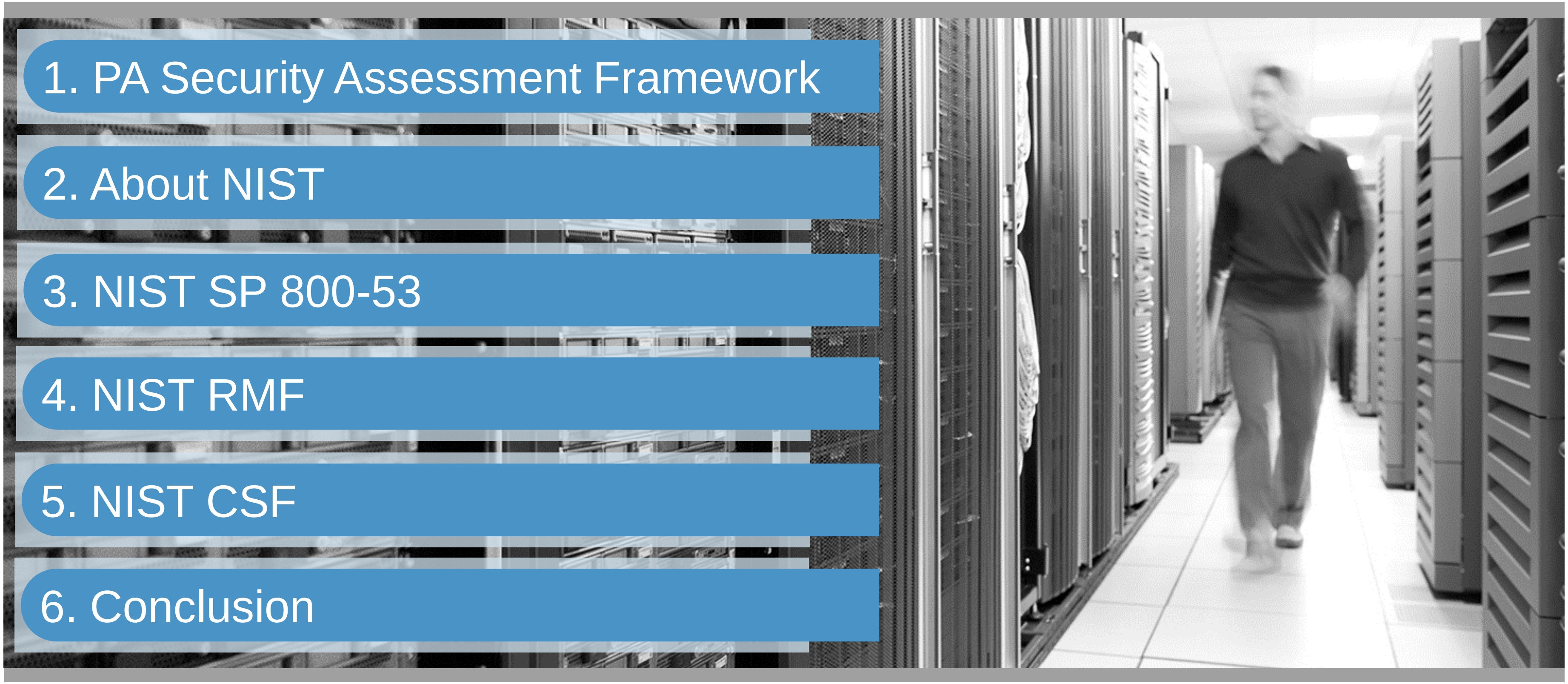
# NIST, No Mystery:

## Understanding NIST Cybersecurity Risk Management

**Peter Romness**
Cisco / US Public Sector Cybersecurity

# Agenda



1. PA Security Assessment Framework
2. About NIST
3. NIST SP 800-53
4. NIST RMF
5. NIST CSF
6. Conclusion

# PA Security Assessment Framework

- Baseline Security Best Practices Assessment
- Security Policy & Organization Review
- Physical and Environmental Security Assessment
- Internal Network Discovery & Vulnerability Scans
- External Network Discovery & Vulnerability Scan
- Wireless Security Analysis
- Account Management Procedure Analysis
- Server and Workstation Configuration Review
- Security Infrastructure Analysis
- Continuity Plan Review
- Human Resources Review
- Security Awareness and Training Programs Assessment

**Source**:http://www.portal.state.pa.us/portal/server.pt/community/security_awareness/494/security_assessment_framework/203339

# NIST References...

What's the difference?
How do these work?

## NIST Cybersecurity Framework (CSF)

## NIST Risk Management Framework (RMF)

## NIST Special Publication 800-53

# NIST

National Institute of Standards and Technology

## Information Technology publications, security standards, tools, and best practices

- Computer Security Resource Center (CSRC)
- Cybersecurity Framework (CSF)
- National Cybersecurity Center of Excellence (NCCoE)
- Information Technology Laboratory (ITL)
- National Strategy for Trusted Identities in Cyberspace (NSTIC)

## Breadth and depth across vast subject areas beyond Information Technology as well

- Telecommunications, nanotechnology, bioscience, energy, chemistry, math, physics, transportation, public safety -- and more

NIST

**Mission**

"To promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life"

**Source**: National Institute of Standards and Technology, http://www.nist.gov/

# NIST CSRC

Computer Security Resource Center

Federal Information Processing Standards (FIPS)

NIST Interagency or Internal Reports (NISTIRs)

Information Technology Laboratory (ITL) Bulletins

NIST Special Publications (SPs)

- **800-Series**: Computer Security
- **1800-Series**: Cybersecurity Practice Guides
- **500-Series**: Information Technology

**800-Series**: NIST's primary mode of publishing computer/cyber/information security guidelines, recommendations and reference materials.

**Source**: NIST CSRC Publications, http://csrc.nist.gov/publications/

# NIST Publications

## Key Standards and Guidelines

- **FIPS 199:** Standards for Security Categorization
- **FIPS 200:** Minimum Security Requirements

**NIST Risk Management Framework**

1. Categorize information system **(NIST SP 800-60)**
2. Select security controls **(NIST SP 800-53)**
3. Implement security controls **(NIST SP 800-160)**
4. Assess security controls **(NIST SP 800-53A)**
5. Authorize information system **(NIST SP 800-37)**
6. Monitor security controls **(NIST SP 800-137)**

**Source**: NIST CSRC, http://csrc.nist.gov/

# NIST Publications

## Key Standards and Guidelines

- **FIPS 199:** Standards for Security Categorization
- **FIPS 200:** Minimum Security Requirements

**NIST Risk Management Framework**

1. Categorize information system **(NIST SP 800-60)**
2. Select security controls **(NIST SP 800-53)**
3. Implement security controls **(NIST SP 800-160)**
4. Assess security controls **(NIST SP 800-53A)**
5. Authorize information system **(NIST SP 800-37)**
6. Monitor security controls **(NIST SP 800-137)**

**Focus Area**

**Source**: NIST CSRC, http://csrc.nist.gov/

# NIST SP 800-53

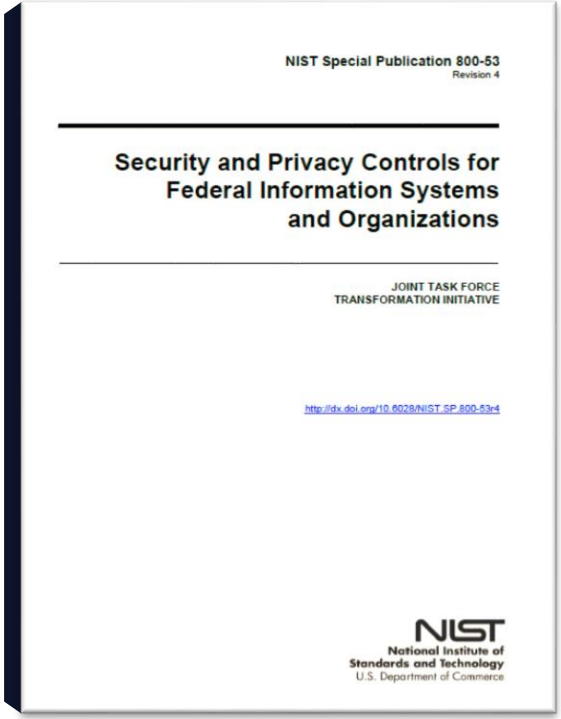
# NIST SP 800-53

Security and Privacy Controls for Federal Information Systems

## Security Control Catalog

- 18 security control families with hundreds of security controls
- Essential for FISMA and the NIST Risk Management Framework

> “Special Publication 800-53, Revision 4, provides a more **holistic approach** to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats.”
>
> “This ‘Build It Right’ strategy is coupled with a variety of security controls for **Continuous Monitoring** to give organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.”



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for
Federal Information Systems
and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

**Source**: NIST SP 800-53, Foreword, Page XV

# NIST SP 800-53

## Security Control Structure

### Security Control Families

- Each family contains security controls related to the general security topic of the family
- Security controls may involve aspects of policy, oversight, supervision, manual **processes**, actions by **individuals**, or automated mechanisms implemented by **information systems/devices**

A two-character ID uniquely identifies security control families

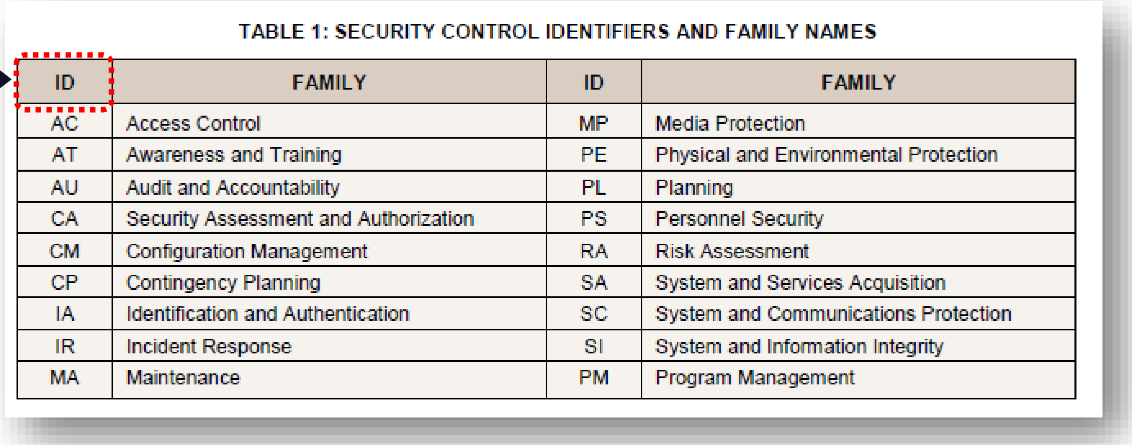
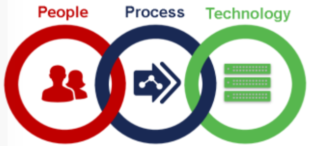


TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

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



# NIST SP 800-53

## Security Control Structure

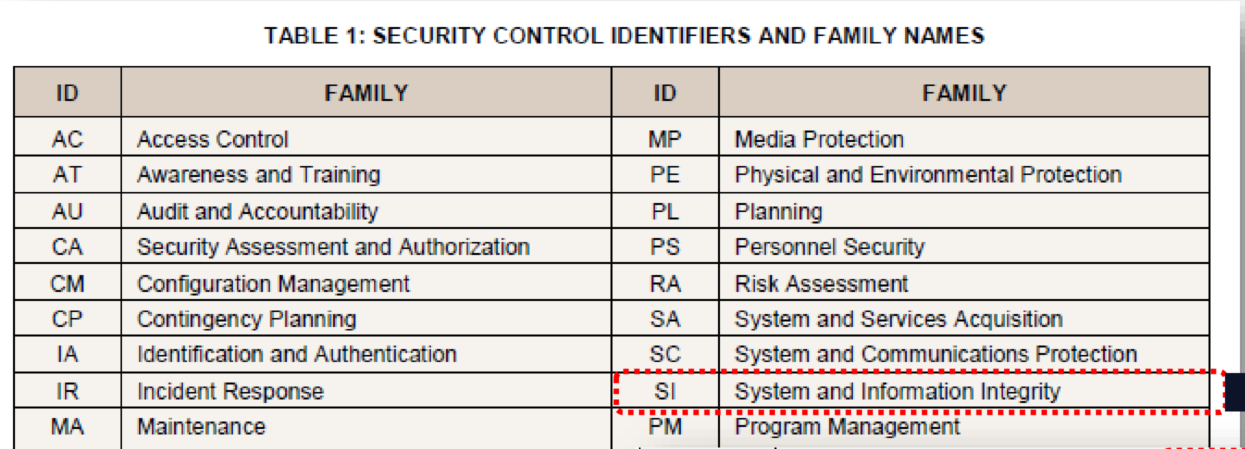
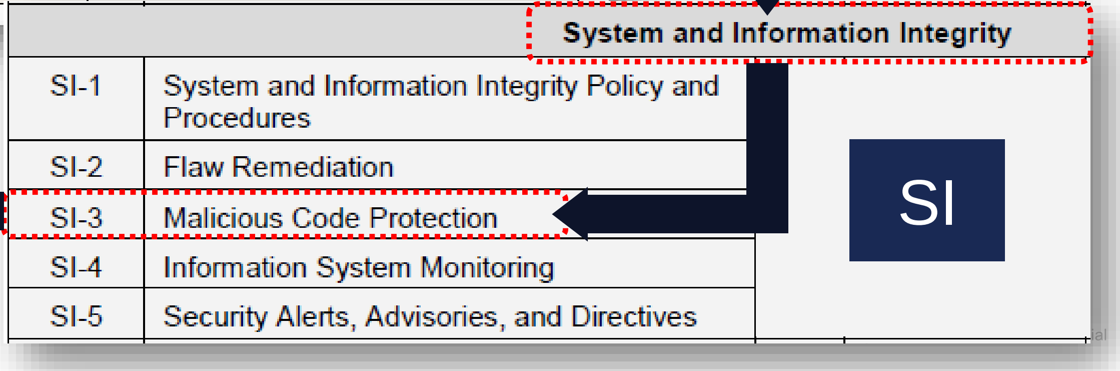


TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

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

Control families drill down into individual security controls



| | System and Information Integrity |
|---|---|
| SI-1 | System and Information Integrity Policy and Procedures |
| SI-2 | Flaw Remediation |
| SI-3 | Malicious Code Protection |
| SI-4 | Information System Monitoring |
| SI-5 | Security Alerts, Advisories, and Directives |

Next slide for security control sections

# NIST SP 800-53

## Security Control Structure

1 Control section

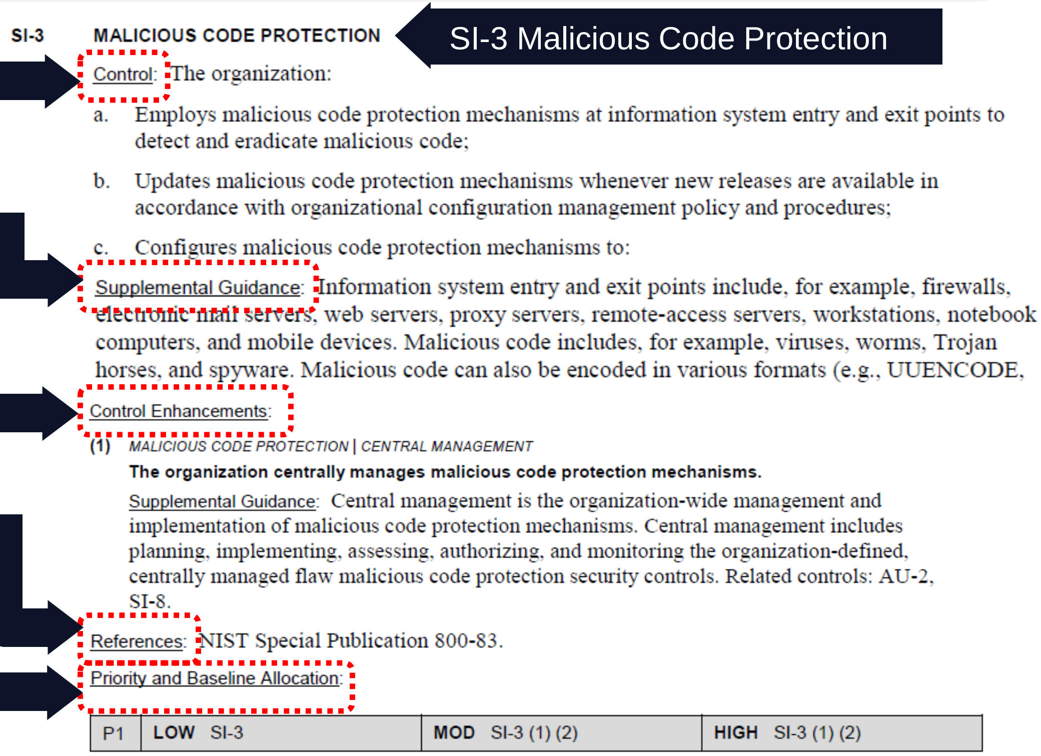
2 Supplemental Guidance section

3 Control Enhancements section

4 References section

5 Priority and Baseline Allocation section

SI-3 Malicious Code Protection



**SI-3 MALICIOUS CODE PROTECTION**

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE,

Control Enhancements:

(1) *MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*

**The organization centrally manages malicious code protection mechanisms.**

Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.

References: NIST Special Publication 800-83.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| P1 | **LOW** SI-3 | **MOD** SI-3 (1) (2) | **HIGH** SI-3 (1) (2) |

# NIST SP 800-53

## Cisco Solution Alignment Summary by Control Family

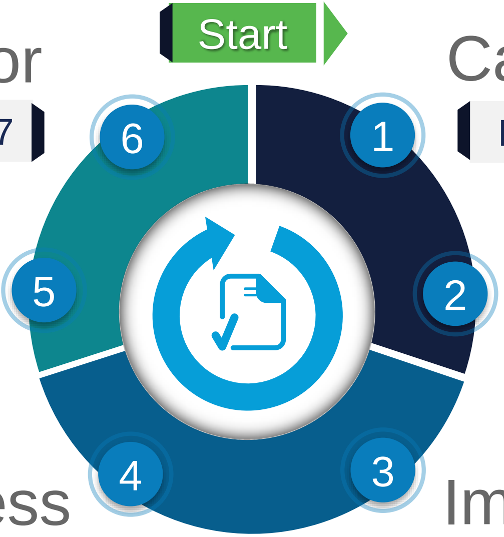
| | | AMP/Threat Grid | Lancope StealthWatch | Cloud Access Security (CAS) | Web/Email Security | Cognitive Threat Analytics (CTA) | OpenDNS | ASA/Firepower | Identity Services Engine (ISE) | TrustSec | AnyConnect |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AC | Access Control | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| AT | Awareness/Training | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ |
| AU | Audit/Accountability | ⬜ | 🟩 | ⬜ | ⬜ | 🟩 | 🟩 | 🟩 | 🟩 | ⬜ | 🟩 |
| CA | Security Assessment | ⬜ | 🟩 | ⬜ | ⬜ | 🟩 | 🟩 | ⬜ | 🟩 | ⬜ | ⬜ |
| CM | Configuration Mgmt | 🟩 | 🟩 | ⬜ | ⬜ | ⬜ | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| CP | Contingency Planning | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ |
| IA | Identification/AuthZ | ⬜ | 🟩 | ⬜ | ⬜ | ⬜ | ⬜ | 🟩 | 🟩 | 🟩 | 🟩 |
| IR | Incident Response | 🟩 | 🟩 | ⬜ | ⬜ | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | ⬜ |
| MA | Maintenance | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ |
| MP | Media Protection | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ |
| PE | Physical Environment | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ |
| PL | Planning | ⬜ | 🟩 | ⬜ | ⬜ | ⬜ | ⬜ | 🟩 | 🟩 | ⬜ | 🟩 |
| PS | Personnel Security | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ | ⬜ |
| RA | Risk Assessment | 🟩 | 🟩 | ⬜ | ⬜ | 🟩 | ⬜ | 🟩 | 🟩 | 🟩 | ⬜ |
| SA | System Acquisition | ⬜ | 🟩 | ⬜ | ⬜ | ⬜ | ⬜ | 🟩 | 🟩 | 🟩 | 🟩 |
| SC | Sys/Comm Protection | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| SI | Sys/Info Integrity | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| PM | Program Management | ⬜ | 🟩 | ⬜ | ⬜ | ⬜ | ⬜ | 🟩 | 🟩 | ⬜ | ⬜ |

Cisco Safety and Security

# NIST RMF

# NIST RMF

Risk Management Framework



Categorize

FIPS 199 & NIST SP 800-60

Select

FIPS 200 & NIST SP 800-53

Implement

NIST SP 800-160

Assess

NIST SP 800-53A

Authorize

NIST SP 800-37

Monitor

NIST SP 800-137

**Source**: NIST RMF Overview, http://csrc.nist.gov/groups/SMA/fisma/framework.html

# Categorize

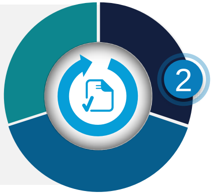
FIPS 199 and
NIST SP 800-60

| | | |
|---|---|---|
| System Impact Levels | High | The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals. |
| | Moderate | The loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. |
| | Low | The loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. |

**SC = {(**confidentiality, **impact), (**integrity, **impact), (**availability, **impact)}**

# Select

FIPS 200 and
NIST SP 800-53



## Select the Initial Control Baseline according to System Category (SC)

| CNTL NO. | CONTROL NAME | PRIORITY | INITIAL CONTROL BASELINES | | |
|---|---|---|---|---|---|
| | | | LOW | MOD | HIGH |
| ACCESS CONTROL | | | | | |
| AC-1 | Access Control Policy and Procedures | P1 | AC-1 | AC-1 | AC-1 |
| AC-4 | Separation of Duties | P1 | Not Selected | AC-4 | AC-4 |
| AC-6 | Least Privilege | P1 | Not Selected | AC-6(1)(2)(5)(9)(10) | AC-6(1)(2)(3)(5)(9)(10) |
| AC-7 | Unsuccessful Logon Attempts | P2 | AC-7 | AC-7 | AC-7 |
| AC-11 | Session Lock | P3 | Not Selected | AC-11(1) | AC-11(1) |

**Source**: NIST SP 800-53, Table D-2: Security Control Baselines

# Implement

NIST SP 800-160

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

| ID | PROCESS NAME | ID | PROCESS NAME |
|---|---|---|---|
| SR | Stakeholder Requirements Definition | TR | Transition |
| RA | Requirements Analysis | VA | Validation |
| AD | Architectural Design | OP | Operation |
| IP | Implementation | MA | Maintenance |
| IN | Integration | DS | Disposal |
| VE | Verification | | |

**Source**: NIST SP 800-60, Table 1: Process Names and Designators

# Assess

NIST SP 800-53A

4

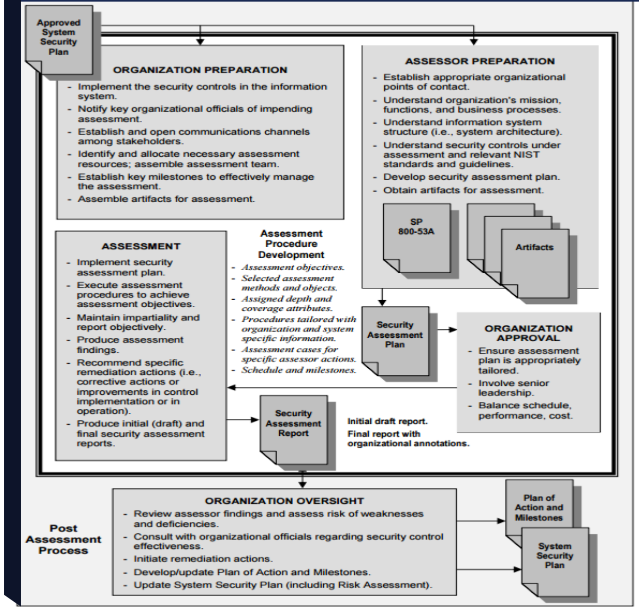
## Assess the implemented security controls to determine whether they are:

- Implemented correctly
- Operating as intended
- Producing the desired results

## Security control assessment goals:

- Consistent, comparable, and repeatable assessments of security controls with reproducible results
- More cost-effective assessments of security controls
- Better understanding of the risks to organizational operations, assets, individuals

## Security Control Assessment Process Overview



Approved System Security Plan

**ORGANIZATION PREPARATION**

- Implement the security controls in the information system.
- Notify key organizational officials of impending assessment.
- Establish and open communications channels among stakeholders.
- Identify and allocate necessary assessment resources; assemble assessment team.
- Establish key milestones to effectively manage the assessment.
- Assemble artifacts for assessment.

**ASSESSOR PREPARATION**

- Establish appropriate organizational points of contact.
- Understand organization's mission, functions, and business processes.
- Understand information system structure (i.e., system architecture).
- Understand security controls under assessment and relevant NIST standards and guidelines.
- Develop security assessment plan.
- Obtain artifacts for assessment.

SP 800-53A

Artifacts

**ASSESSMENT**

- Implement security assessment plan.
- Execute assessment procedures to achieve assessment objectives.
- Maintain impartiality and report objectively.
- Produce assessment findings.
- Recommend specific remediation actions (i.e., corrective actions or improvements in control implementation or in operation).
- Produce initial (draft) and final security assessment reports.

**Assessment Procedure Development**

- *Assessment objectives.*
- *Selected assessment methods and objects.*
- *Assigned depth and coverage attributes.*
- *Procedures tailored with organization and system specific information.*
- *Assessment cases for specific assessor actions.*
- *Schedule and milestones.*

Security Assessment Plan

**ORGANIZATION APPROVAL**

- Ensure assessment plan is appropriately tailored.
- Involve senior leadership.
- Balance schedule, performance, cost.

Security Assessment Report

Initial draft report.

Final report with organizational annotations.

**Post Assessment Process**

**ORGANIZATION OVERSIGHT**

- Review assessor findings and assess risk of weaknesses and deficiencies.
- Consult with organizational officials regarding security control effectiveness.
- Initiate remediation actions.
- Develop/update Plan of Action and Milestones.
- Update System Security Plan (including Risk Assessment).

Plan of Action and Milestones

System Security Plan

**Source**: NIST SP 800-53A, Figure 1: Security Control Assessment Process Overview

# Authorize

NIST SP 800-37

## 1 Plan of Action and Milestones

Prepare based on the findings and recommendations of the security assessment report excluding any remediation actions taken

## 2 Security Authorization Package

Assemble the security authorization package and submit the package to the authorizing official for adjudication

## 3 Risk Determination

Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, etc.

## 4 Risk Acceptance

Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable

**ATO**

"If the authorizing official, after reviewing the authorization package deems that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable, an **authorization to operate** is issued for the information system or for the common controls inherited by organizational information systems"

**Source**: NIST SP 800-37, Appendix F: Security Authorization

# Monitor

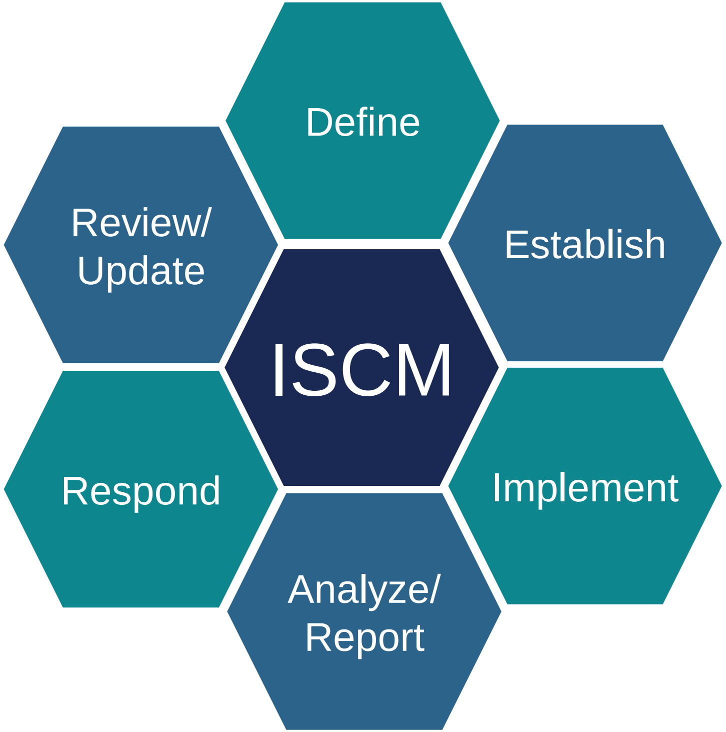
NIST SP 800-137

## Information Security Continuous Monitoring (ISCM)

- Provides security situational awareness
- Enables appropriate action as the situation changes
- Part of the larger strategy of enterprise risk management

## The role of automation in ISCM

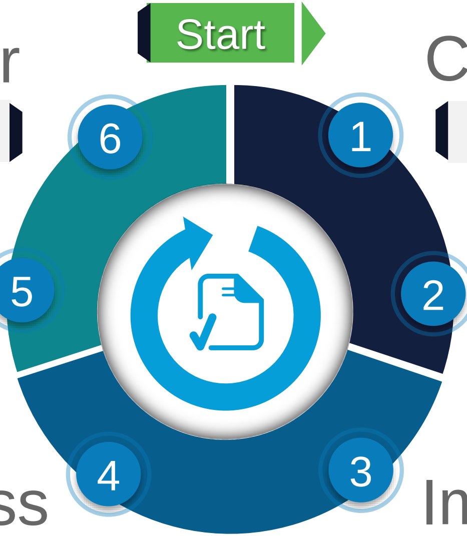
- Augments the security processes conducted by security professionals within an organization
- Reduces the amount of time a security professional must spend on doing redundant tasks
- Frees the security professional to spend time on tasks that do require human cognition



**Source**: NIST SP 800-137, Chapter 2: The Fundamentals

# NIST RMF Summary

Risk Management Framework



Categorize

FIPS 199 & NIST SP 800-60

Select

FIPS 200 & NIST SP 800-53

Implement

NIST SP 800-160

Assess

NIST SP 800-53A

Authorize

NIST SP 800-37

Monitor

NIST SP 800-137

**Source**: NIST RMF Overview, http://csrc.nist.gov/groups/SMA/fisma/framework.html

# NIST CSF

# Improving Critical Infrastructure Cybersecurity

Executive Order 13636

February 2013

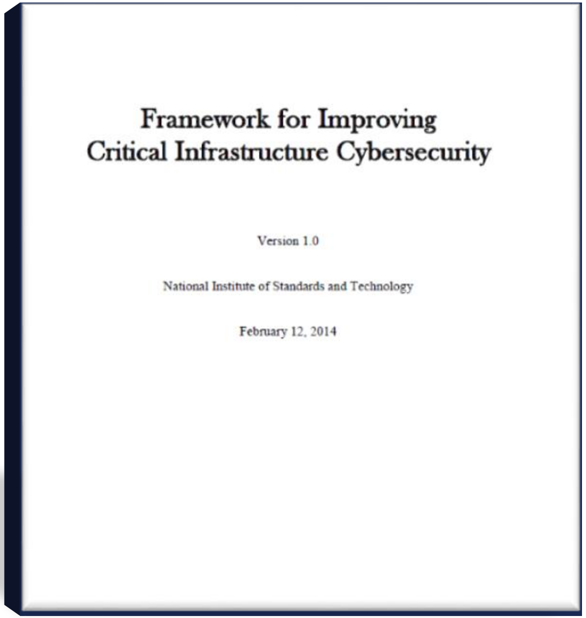
> “It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a **cyber environment** that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”

# NIST CSF

Cybersecurity Framework

Outcome of Executive Order 13636, and result of collaboration between public and private sectors

- Manages cybersecurity risks in a cost-effective way, while protecting privacy and civil liberties
- References the globally accepted standards (COBIT, ISO/IEC, ISA, NIST, CCS) that are working well today
- Intended for worldwide adoption -- not US only
- Uses common terminology to discuss cybersecurity risk
- Ensures business drivers guide cybersecurity activities
- Considers cybersecurity risks as part of organization’s overall risk management process



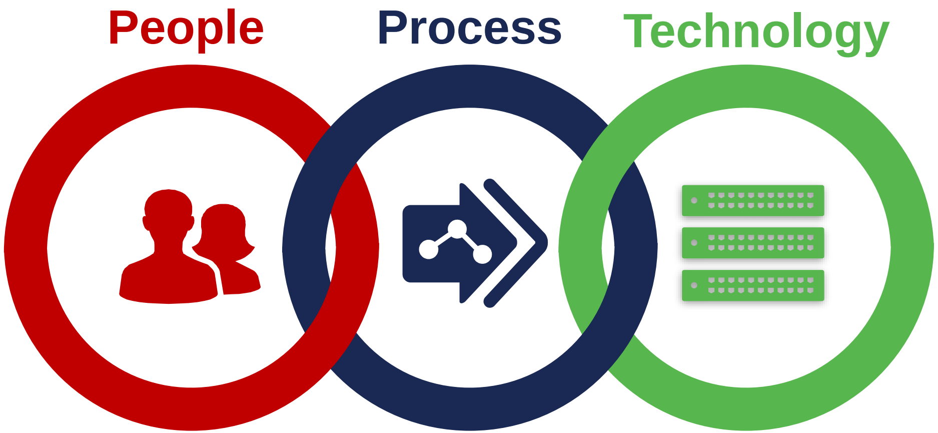
Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

# Best Practices



Framework covers all three

# Focused Action

People

## Framework helps organizations optimize their cybersecurity activities

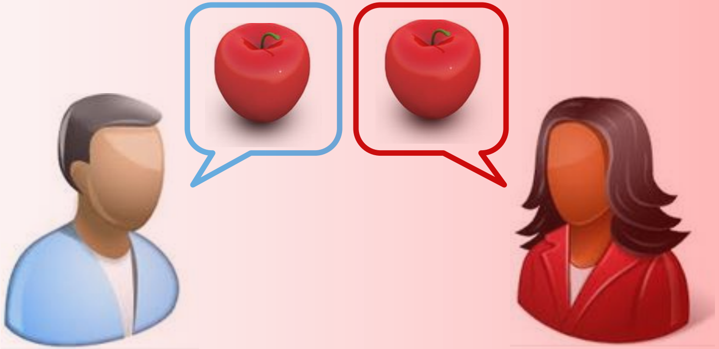
- Aligns cybersecurity activities with business risk
- Prioritizes activities that are most important for critical service delivery
- Maximizes the impact of cybersecurity spending

# Better Communication

People

## Framework uses a common language to discuss cybersecurity risk

- Improves communication among cybersecurity experts and senior leadership within an organization
- Improves communication with external vendors, partners, and contractors
- Aligns the Information Technology (IT) and Operations Technology (OT) teams



# Process Support

Process

## Framework works with existing risk management programs

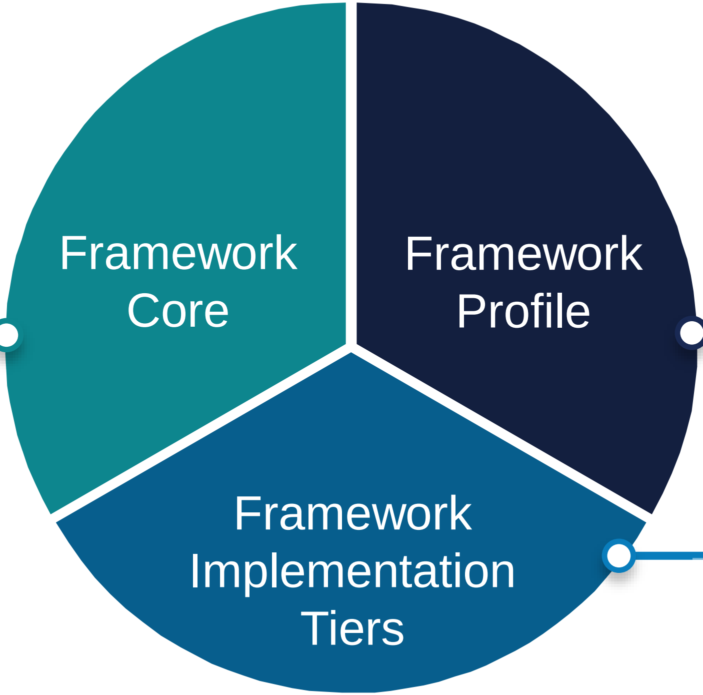
- ISO/IEC 27005, Information Security Risk Management
- ISO/IEC 31000, Risk Management
- NIST SP 800-39, Managing Information Security Risk
- Electricity Subsector Cybersecurity Risk Management Process (RMP)

# Broad Applicability

## Framework enables all organizations to improve security and resilience

- Any size or type of organization
- Both public and private sectors
- Any degree of cybersecurity risk
- Any level of cybersecurity sophistication
- Anywhere in the world

# CSF Components



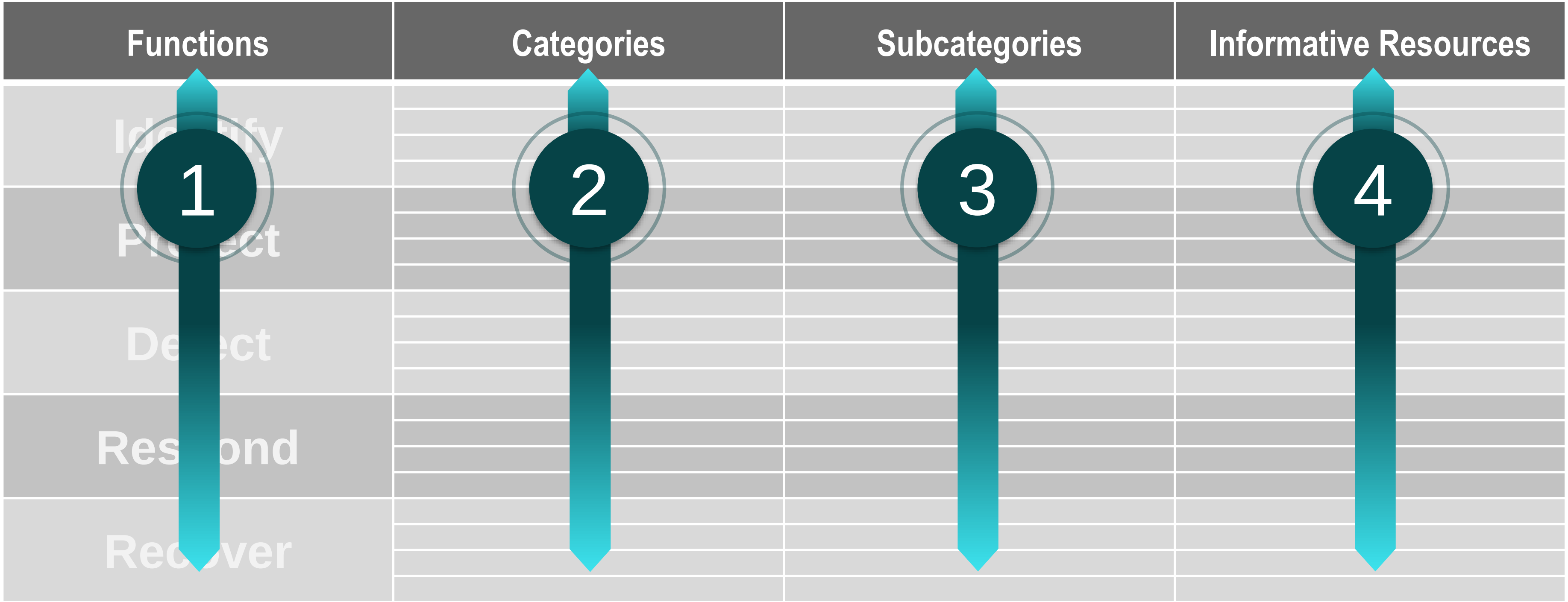
Set of activities, desired outcomes, and applicable references common across critical infrastructure sectors

Alignment of Framework Core structure with the specific business requirements of a particular organization

An organization’s view on how well it manages risk, ranging from Partial (Tier 1) to Adaptive (Tier 4)

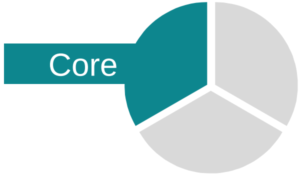
# CSF Core

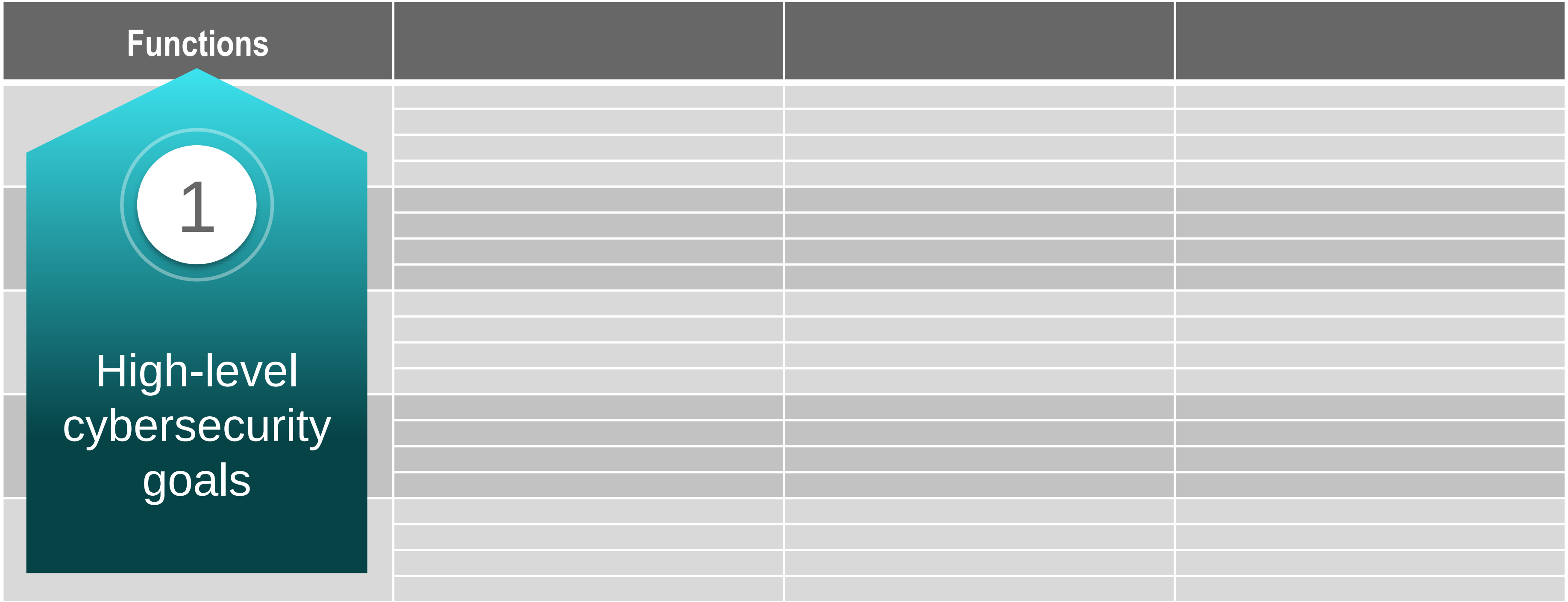
Core



| Functions | Categories | Subcategories | Informative Resources |
|---|---|---|---|
| Identify | | | |
| Protect | | | |
| Detect | | | |
| Respond | | | |
| Recover | | | |

# CSF Core





High-level cybersecurity goals

# CSF Core

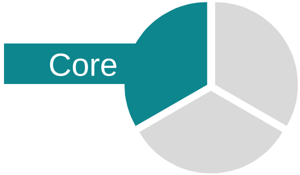
Core

|  | Categories |  |  |
|---|---|---|---|
| Identify |  |  |  |
| Protect |  |  |  |
| Detect |  |  |  |
| Respond |  |  |  |
| Recover |  |  |  |

2

Subdivide Functions into specific activities

# CSF Core

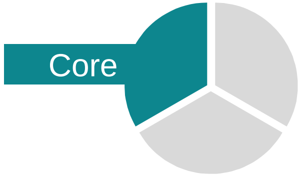


|  |  | Subcategories |  |
|---|---|---|---|
| Identify |  |  |  |
| Protect |  |  |  |
| Detect |  |  |  |
| Respond |  |  |  |
| Recover |  |  |  |

3

Subdivide Categories into desired outcomes

# CSF Core

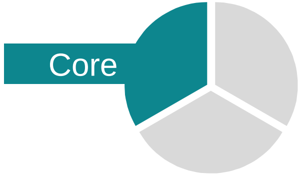


| | | | Informative Resources |
|---|---|---|---|
| Identify | | | |
| Protect | | | |
| Detect | | | |
| Respond | | | |
| Recover | | | |

4

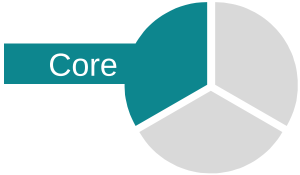
Standards references to achieve the outcomes

# Functions



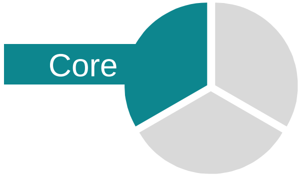
| Functions | | |
|---|---|---|
| ID | **Identify** | Develop the **organizational understanding** to manage cybersecurity risk to systems, assets, data, and capabilities |
| PR | **Protect** | Develop and implement the **appropriate safeguards** to ensure delivery of critical infrastructure services |
| DE | **Detect** | Develop and implement the appropriate activities to **identify the occurrence** of a cybersecurity event |
| RS | **Respond** | Develop and implement the appropriate activities to **take action** regarding a **detected** cybersecurity event |
| RC | **Recover** | Develop and implement the appropriate activities to **maintain plans for resilience** and to **restore any capabilities or services** that were impaired due to a cybersecurity event |

# Categories



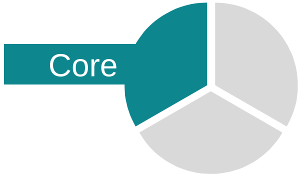
| Function | Categories | | |
|---|---|---|---|
| **Identify (ID)** | **ID.AM** | **Asset Management (AM)** | The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are **identified** and **managed** consistent with their **relative importance** to business objectives and the organization's risk strategy. |
| | **ID.BE** | **Business Environment (BE)** | The organization's **mission**, **objectives**, **stakeholders**, and **activities** are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. |
| | **ID.GV** | **Governance (GV)** | The **policies**, **procedures**, and **processes** to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber risk. |
| | **ID.RA** | **Risk Assessment (RA)** | The organization **understands the cybersecurity risk** to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. |
| | **ID.RM** | **Risk Management Strategy (RM)** | The organization's priorities, constraints, risk tolerances, and assumptions are established and used to **support operational risk decisions**. |

# Subcategories



| Function | Category | Subcategories | |
|---|---|---|---|
| **Identify (ID)** | **Asset Management (ID.AM)** | **ID.AM-1** | **Physical devices and systems** within the organization are **inventoried** |
| | | **ID.AM-2** | **Software platforms and applications** within the organization are **inventoried** |
| | | **ID.AM-3** | Organizational **communication** and **data flows** are **mapped** |
| | | **ID.AM-4** | **External information systems** are **catalogued** |
| | | **ID.AM-5** | **Resources** (hardware, devices, data, 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 (suppliers, customers, partners) are **established** |

# Informative Resources



| Function | Category | Subcategory | Informative Resources |
|---|---|---|---|
| Identify (ID) | Asset Management (ID.AM) | Physical device inventories (ID.AM-1) | • CCS CSC 1<br>• COBIT 5 BAI09.01, BAI09.02<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISA 62443-3-3:2013 SR 7.8<br>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2<br>• NIST SP 800-53 Rev. 4 CM-8 |

**International standards references**

- Council on CyberSecurity (CCS)
- Control Objectives for Information and Related Technology (COBIT)
- International Society of Automation (ISA)
- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)

# Informative Resources

| Function | Category | Subcategory | Informative Resources |
|---|---|---|---|
| Identify (ID) | Asset Management (ID.AM) | Physical device inventories (ID.AM-1) | • CCS CSC 1<br>• COBIT 5 BAI09.01, BAI09.02<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISA 62443-3-3:2013 SR 7.8<br>• **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2**<br>• NIST SP 800-53 Rev. 4 CM-8 |

| ISO/IEC 27001:2013 Annex A | |
|---|---|
| **A.8 Asset Management** | |
| **A.8.1.1** | Inventory of Assets |
| **A.8.1.2** | Ownership of Assets |

# Tiers

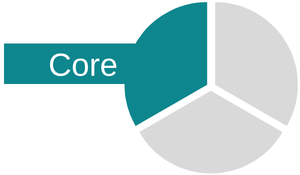
Reflect how an organization views cybersecurity risk and the processes in place to manage that risk

- Tier 4 **Adaptive**: Practices fully established and continuously improved
- Tier 3 **Repeatable**: Practices approved and established by organizational policy
- Tier 2 **Risk Informed**: Practices approved but not completely established by policy
- Tier 1 **Partial**: Informal, ad hoc, reactive responses

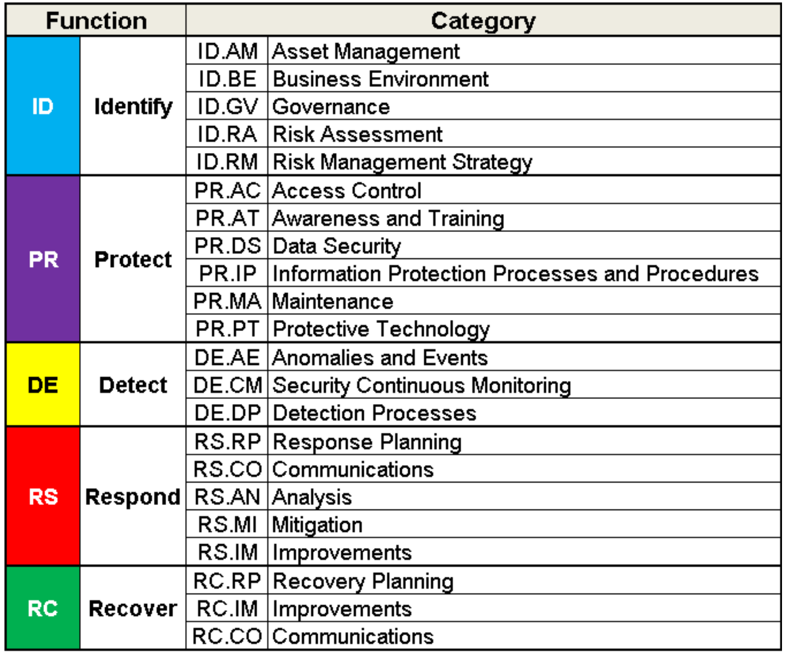
# Profiles

## The alignment of the Framework core with an organizations business requirements, risk tolerance, and resources

- Describes the current state and desired future state
- Reveals gaps that can flow into action plan development
- Facilities a roadmap for reducing cybersecurity risk



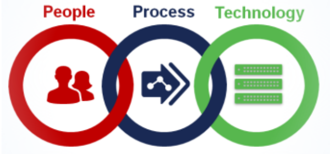
# High Level Core View

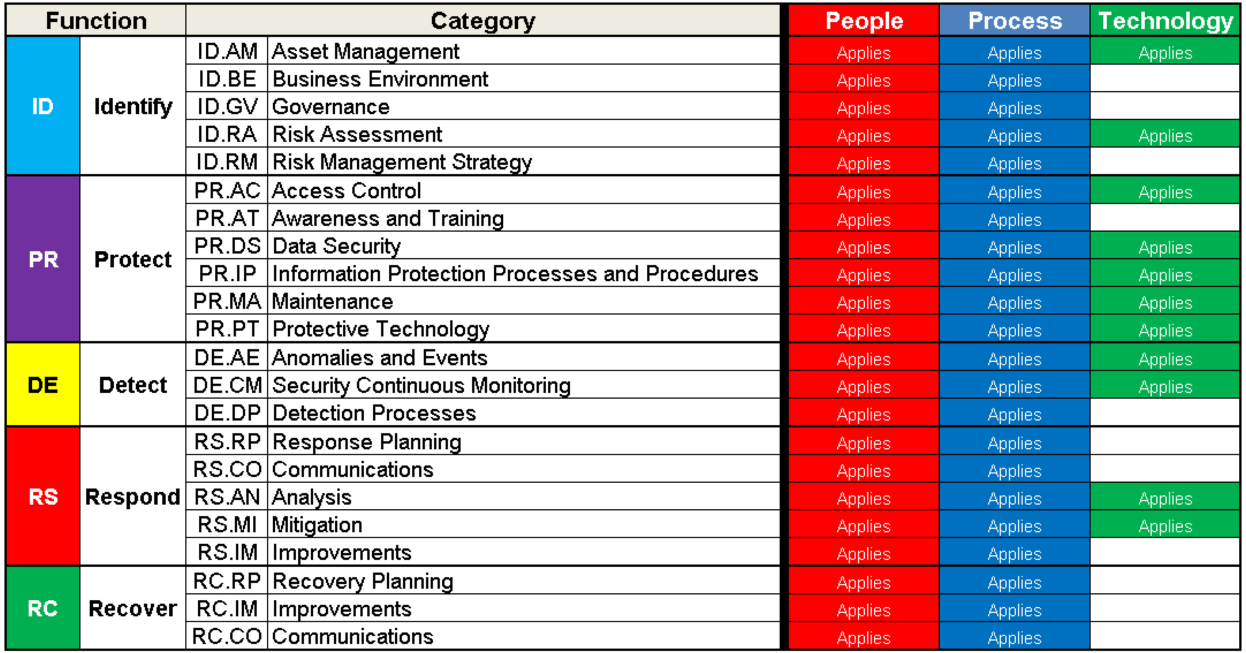


| Function | | Category | |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| 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 |

- Know what you have
- Secure what you have
- Spot threats quickly
- Take action immediately
- Restore operations

# Important Points





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

- **Only half** of the Framework's Categories are addressed by **technology**

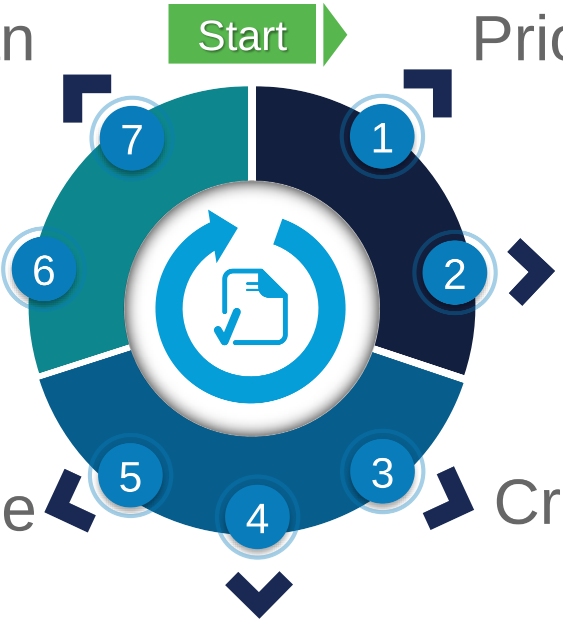
- Highlights the importance of both **people and process** in cybersecurity

# CSF Uses

| Basic Review of Cybersecurity Practices | Establishing or Improving a Cybersecurity Program | Communicating Cybersecurity Requirements with Stakeholders | Identifying Opportunities for Updated Informative References | Methodology to Protect Privacy and Civil Liberties |
|---|---|---|---|---|
| “How well are we doing today?” | “Can we assess and improve?” | “Can we speak the same language?” | “What else should we consider?” | “Can we protect data better?” |

Let’s focus here

# Improving a Program



Implement Action Plan

Prioritize and Scope

Analyze Gaps

Orient

Create Target Profile

Create Current Profile

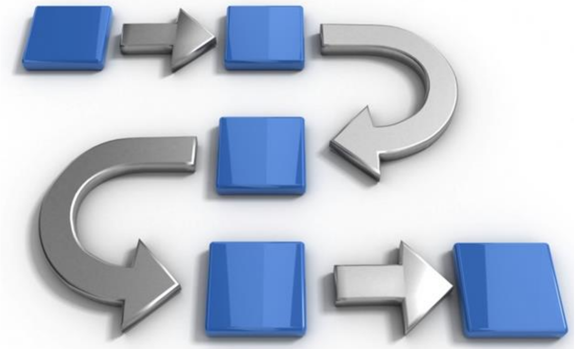
Conduct Risk Assessment

# Prioritize and Scope

1

## Identify business/mission objectives and high-level organizational priorities

- Make strategic decisions on cybersecurity
- Determine scope of systems and assets that support the mission
- Assess risk tolerance



# Orient

## Identify related systems, regulatory requirements, and overall risk approach

- Identify threats to systems and assets
- Identify vulnerabilities associated with systems and assets

# Current Profile

| Function | Category | Subcategory | Current Profile | |
|---|---|---|---|---|
| Identify (ID) | Asset Management (ID.AM) | Physical device inventories (ID.AM-1) | Tier 1 | Manual, spreadsheet-based system is insufficient and lacks network visibility. |
| | | Software inventories (ID.AM-2) | Tier 1 | Asset management system cannot detect new software applications being deployed. |
| | | Communication/data flow maps (ID.AM-3) | Tier 2 | Flow maps are documented and approved but needs to be formalized by policy. |
| | | External system catalogs (ID.AM-4) | Unused | Current business model does not require external system catalogs. |
| | | Resource prioritization (ID.AM-5) | Tier 4 | Prioritization system is working well for our needs today. |
| | | Roles/responsibilities clarification (ID.AM-6) | Tier 3 | New cybersecurity responsibilities need to be formalized by policy. |

# Risk Assessment

| Fxn. | Cat. | Sub. | Current Profile | Risk Assessment |
|---|---|---|---|---|
| ID | ID.AM | ID.AM-1 | Tier 1 | ✗ |
| | | ID.AM-2 | Tier 1 | ✗ |
| | | ID.AM-3 | Tier 2 | ✓ |
| | | ID.AM-4 | Unused | ✓ |
| | | ID.AM-5 | Tier 4 | ✓ |
| | | ID.AM-6 | Tier 3 | ✓ |

‹ Unacceptably high risks

‹ Acceptable risks at this time

# Target Profile

## This is where we want to be

- Physical device and software inventories at Tier 4, “Adaptive”
- Practices fully established, continuously improved, and built into our overall risk management program

| | Fxn. | Cat. | Sub. | Target Profile |
|---|---|---|---|---|
| ✓ | ID | ID.AM | ID.AM-1 | Tier 4 |
| ✓ | | | ID.AM-2 | Tier 4 |
| ✓ | | | ID.AM-3 | Tier 2 |
| ✓ | | | ID.AM-4 | Unused |
| ✓ | | | ID.AM-5 | Tier 4 |
| ✓ | | | ID.AM-6 | Tier 3 |

# Gap Analysis

6

| Fxn. | Cat. | Sub. | Current Profile |
|---|---|---|---|
| ID | ID.AM | ID.AM-1 | Tier 1 |
| | | ID.AM-2 | Tier 1 |
| | | ID.AM-3 | Tier 2 |
| | | ID.AM-4 | Unused |
| | | ID.AM-5 | Tier 4 |
| | | ID.AM-6 | Tier 3 |

Enables a **prioritized** action plan

| Fxn. | Cat. | Sub. | Target Profile |
|---|---|---|---|
| ID | ID.AM | ID.AM-1 | Tier 4 |
| | | ID.AM-2 | Tier 4 |
| | | ID.AM-3 | Tier 2 |
| | | ID.AM-4 | Unused |
| | | ID.AM-5 | Tier 4 |
| | | ID.AM-6 | Tier 3 |

# Action Plan

| Fxn. | Cat. | Sub. | Informative Resources |
|---|---|---|---|
| ID | ID.AM | ID.AM-1 | • CCS CSC 1<br>• COBIT 5 BAI09.01, BAI09.02<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISA 62443-3-3:2013 SR 7.8<br>• ISO/IEC 27001:2013 A.8.1.1, A.8.1<br>• **NIST SP 800-53 Rev. 4 CM-8** |
| | | ID.AM-2 | • CCS CSC 2<br>• COBIT 5 BAI09.01, BAI09.02, BAI 05<br>• ISA 62443-2-1:2009 4.2.3.4<br>• ISA 62443-3-3:2013 SR 7.8<br>• ISO/IEC 27001:2013 A.8.1.1, A.8.1<br>• **NIST SP 800-53 Rev. 4 CM-8** |

## NIST SP 800-53 Revision 4

**CM-8 / Information System Component Inventory**

Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]

# Develop Action Plan

Device Inventory

We need an accurate device inventory...

...but how can we know what’s actually on our network?

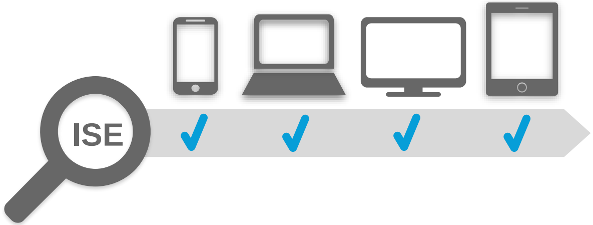
# Implement Action Plan

Device Discovery and Profiling

7

## Cisco Identity Services Engine (ISE)

- Discovers and accurately identifies devices connected to wired, wireless, and virtual private networks



### NIST SP 800-53 Revision 4

**CM-8 / Information System Component Inventory**

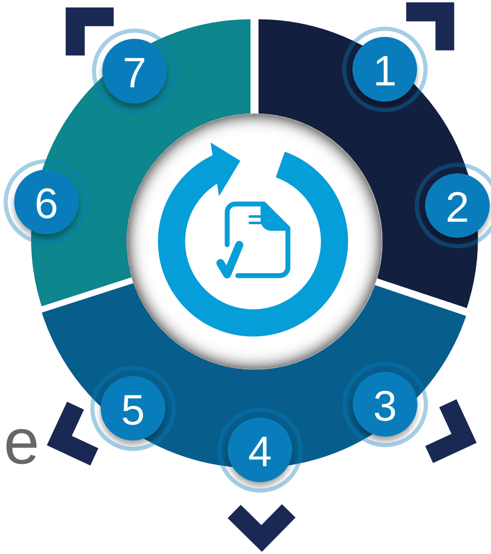
Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]

# Continuous Improvement

Not once and done!



Prioritize and Scope

Orient

Create Current Profile

Conduct Risk Assessment

Create Target Profile

Analyze Gaps

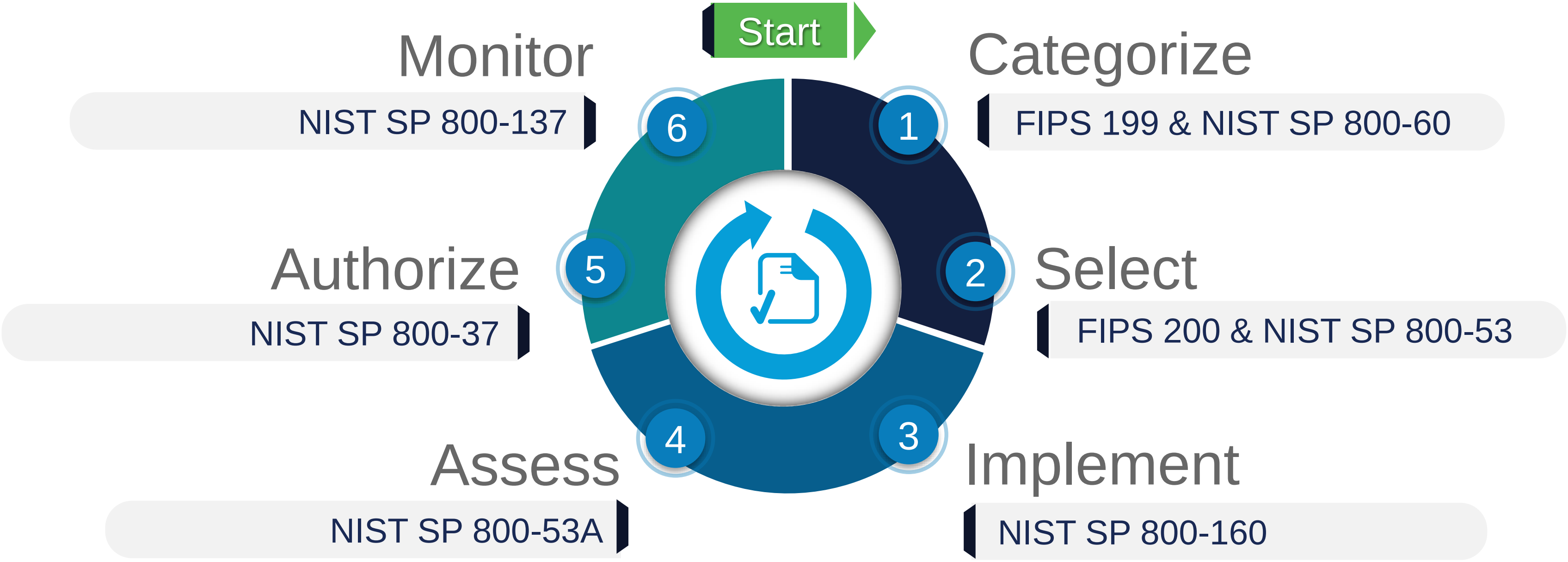
Implement Action Plan

# NIST RMF vs. NIST CSF

What's the difference?

# NIST RMF Overview

Risk Management Framework



Start

1 Categorize

FIPS 199 & NIST SP 800-60

2 Select

FIPS 200 & NIST SP 800-53

3 Implement

NIST SP 800-160

4 Assess

NIST SP 800-53A

5 Authorize

NIST SP 800-37

6 Monitor

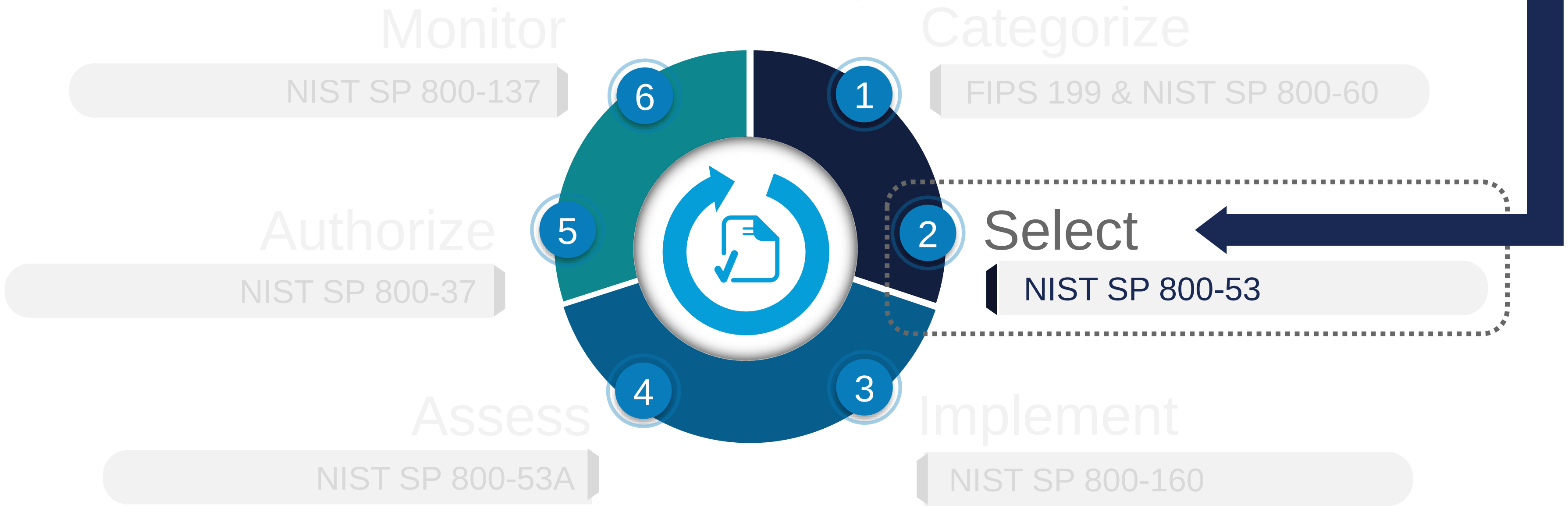
NIST SP 800-137

**Source**: NIST RMF Overview, http://csrc.nist.gov/groups/SMA/fisma/framework.html

# NIST RMF vs. NIST CSF

Security Control Selection

**NIST CSF guides organizations to risk-based Selection of effective security controls for inclusion in existing risk-management process**



# NIST RMF vs. NIST CSF

Other Important Differences

## NIST CSF can be used with the NIST RMF but does not require it

- Organizations may choose to follow the NIST RMF, but are also free choose to use the NIST CSF with ISO/IEC 27005 -- or any other enterprise risk management process

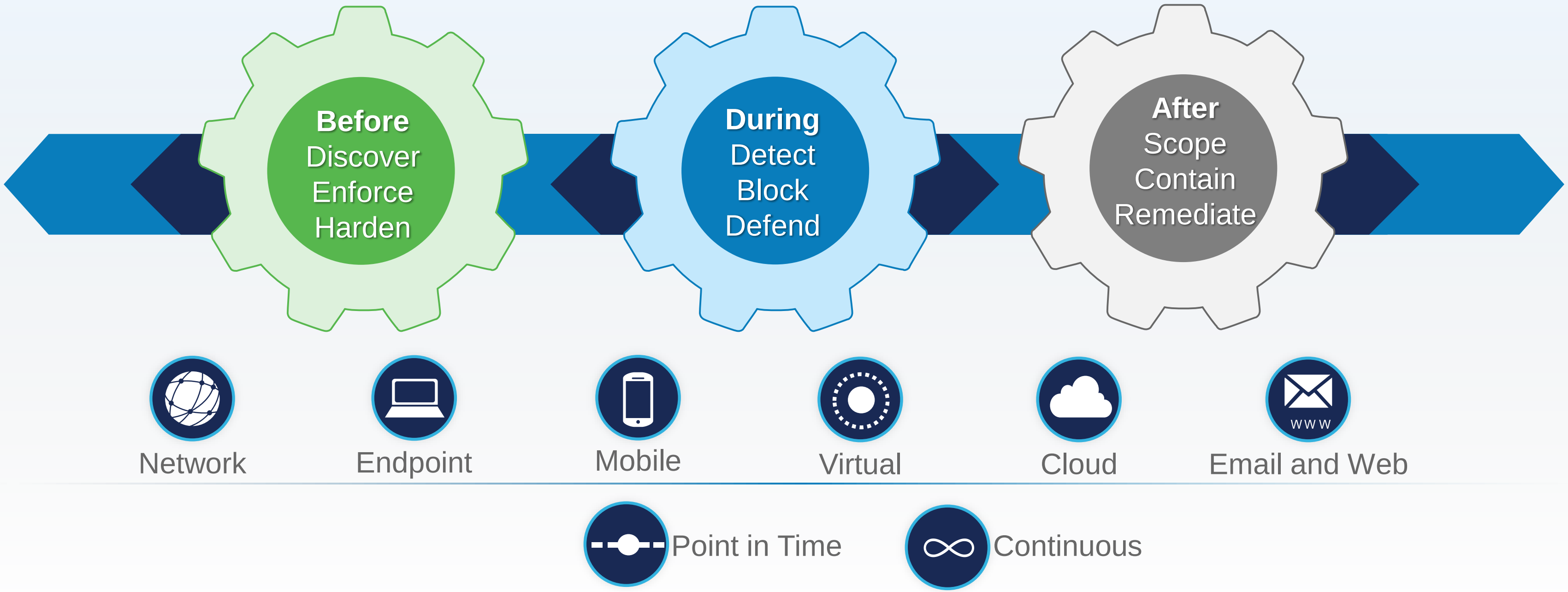
## NIST CSF references the NIST SP 800-53 security control catalog but does not require it

- Organizations may choose to select security controls from NIST SP 800-53, but are also free to select from ISACA COBIT 5, ISO/IEC 27001/27002, or other security control catalogs
- NIST CSF Informative Resources refer to certain controls from NIST SP 800-53, but the CSF does not reference the complete set of NIST SP 800-53 controls
- NIST CSF describes its own cybersecurity improvement process that leverages CSF Profiles and Implementation Tiers, but without the rigor of the NIST RMF (e.g., no FIPS 199 System Categorization)

# Cisco Security Strategy

The Threat-Centric Security Model

## Attack Continuum



**Before**
Discover
Enforce
Harden

**During**
Detect
Block
Defend

**After**
Scope
Contain
Remediate

Network

Endpoint

Mobile

Virtual

Cloud

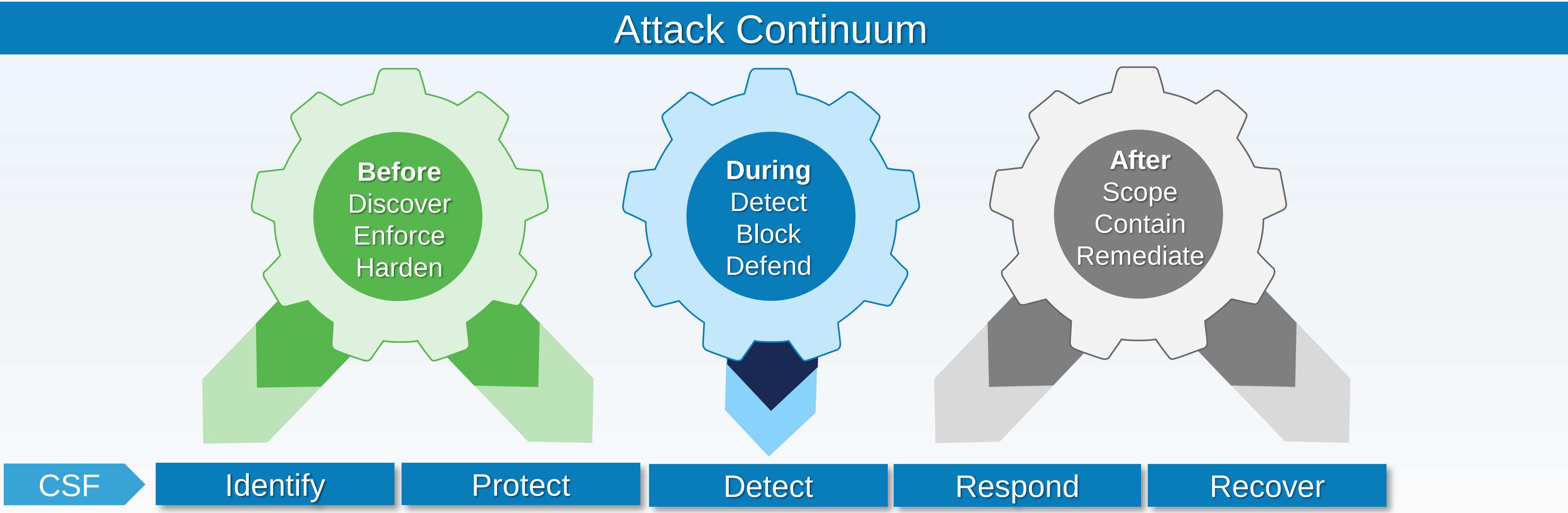
Email and Web

Point in Time

Continuous

# Cisco Security Strategy

NIST CSF Alignment



# Cisco Security Products

NIST CSF Alignment

Technology

| Function | Category | AMP/Threat Grid | Lancope StealthWatch | Cloud Access Security (CAS) | Web/Email Security | Cognitive Threat Analytics (CTA) | OpenDNS | Firepower | Identity Services Engine (ISE) | TrustSec | AnyConnect |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ID | Asset Management | | 🟩 | 🟩 | | | | 🟩 | 🟩 | | |
| | Business Environment | Non-technical control area | | | | | | | | | |
| | Governance | Non-technical control area | | | | | | | | | |
| | Risk Assessment | | | | | 🟩 | | 🟩 | | | |
| | Risk Mgmt. Strategy | Non-technical control area | | | | | | | | | |
| PR | Access Control | | | 🟩 | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| | Awareness/Training | Non-technical control area | | | | | | | | | |
| | Data Security | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| | Info Protection Process | Non-technical control area | | | | | | | | | |
| | Maintenance | | | | | | | | | | 🟩 |
| | Protective Technology | 🟩 | | | | | | 🟩 | 🟩 | 🟩 | 🟩 |
| DE | Anomalies and Events | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | |
| | Continuous Monitoring | 🟩 | 🟩 | | 🟩 | 🟩 | | 🟩 | | | |
| | Detection Processes | Non-technical control area | | | | | | | | | |
| RS | Response Planning | Non-technical control area | | | | | | | | | |
| | Communications | Non-technical control area | | | | | | | | | |
| | Analysis | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | |
| | Mitigation | 🟩 | 🟩 | 🟩 | 🟩 | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| | Improvements | Non-technical control area | | | | | | | | | |
| RC | Recovery Planning | Non-technical control area | | | | | | | | | |
| | Improvements | Non-technical control area | | | | | | | | | |
| | Communications | Non-technical control area | | | | | | | | | |

B

D

A

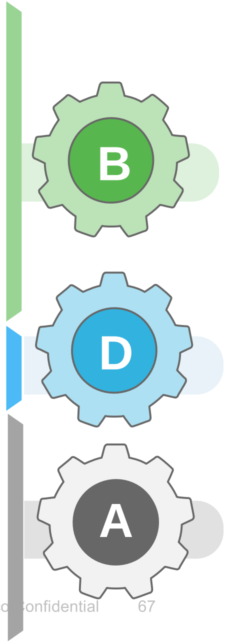
# Cisco Security Services

## NIST CSF Alignment

People Process

cisco

| | | Advisory | Integration | Managed |
|---|---|---|---|---|
| ID | Asset Management | 🟩 | 🟩 | 🟩 |
| | Business Environment | 🟩 | | |
| | Governance | 🟩 | | |
| | Risk Assessment | 🟩 | 🟩 | 🟩 |
| | Risk Mgmt. Strategy | 🟩 | 🟩 | |
| PR | Access Control | 🟩 | 🟩 | 🟩 |
| | Awareness/Training | 🟩 | | 🟩 |
| | Data Security | 🟩 | | 🟩 |
| | Info Protection Process | 🟩 | | 🟩 |
| | Maintenance | 🟩 | | 🟩 |
| | Protective Technology | 🟩 | 🟩 | 🟩 |
| DE | Anomalies and Events | 🟩 | 🟩 | 🟩 |
| | Continuous Monitoring | 🟩 | 🟩 | 🟩 |
| | Detection Processes | 🟩 | | 🟩 |
| RS | Response Planning | 🟩 | | 🟩 |
| | Communications | 🟩 | | 🟩 |
| | Analysis | 🟩 | 🟩 | 🟩 |
| | Mitigation | 🟩 | 🟩 | 🟩 |
| | Improvements | 🟩 | | 🟩 |
| RC | Recovery Planning | 🟩 | | 🟩 |
| | Improvements | 🟩 | | 🟩 |
| | Communications | 🟩 | | 🟩 |



# Cisco

## Our Advantages

Cisco has the people, services, products, partners, corporate commitment and financial strength to ensure your success

- Our **worldwide security team**, including threat intelligence, research, supply chain, and customer support professionals, is focused on your success.
- Our **services professionals** can guide you as you plan, implement and manage your security, deliver security as a service, or help you during an attack.
- Our family of **best in class products** work together to stop threats quickly while reducing complexity and cost.
- Because of our open platform and industry leadership, we team with comprehensive list of solutions providers and delivery **partners**.
- Cisco is **committed to your success** with the financial strength to invest in research, develop new products, and support your success

Securely digitizing you enterprise allows you to secure your reputation, accelerate your mission, and save money.

# Conclusion

# Summary

Did we accomplish our mission?

| | |
|---|---|
| 1. PA Cybersecurity | ✓ Reviewed Assessment Framework |
| 2. About NIST | ✓ Discussed who they are and what they do |
| 3. NIST SP 800-53 | ✓ Explained how the control catalog works |
| 4.NIST RMF | ✓ Connected with the Strategic Plan |
| 5. NIST CSF | ✓ Recommended it for cyber risk management |

# Call to Action

1 **Learn more about Pennsylvania IT Governance**
http://www.portal.state.pa.us/portal/server.pt/community/security_awareness/494/security_assessment_framework/203339

2 **Learn more about NIST cybersecurity best practices:**
http://csrc.nist.gov

3 **Learn more about Cisco's threat-centric security:**
http://www.cisco.com/go/security

**Thanks for your time today!**

CISCO

*TOMORROW starts here.*