



Implementing a Framework

Utility Technology Association

2014

Greg Jackson
Cyber Security Analyst
Dynetics Inc.

Outline

- What is a Framework?
- Why is a Framework so Important?
- Risk Management Implementation
- Frameworks – Understanding the Difference
  - Risk Management Framework (RMF)
  - CyberSecurity Framework (CSF)
- How do I Implement a Framework
  - Business Impact Analysis
  - Risk Assessment
  - Categorization
- Specifically, How do I implement the Risk Management Framework
- Specifically, How do I implement the CyberSecurity Framework

Something to Think About

- How much security is enough?
- How do I prioritize decisions when it comes to security?
- How do I know what to protect?

What is a Framework?

- A framework is **not** a set of security controls.
- A framework is a structure or process that uses security controls to provide minimum security.
- A framework provides organizations with a structure to apply to today's multiple approaches to cybersecurity
  - There are a lot of valid approaches to cybersecurity but without a framework the approach lacks guidance, direction, and communication flow
- Enables organizations to apply the principles and best practices of risk management to improve the security and resilience of their enterprise

What is a Framework?

- **Frameworks require organizations to:**
  - **Understand the Business Impact if an information type were compromised**
    - **Business Impact Analysis**
  - **Understand the Cyber Threat Level**
    - **Risk Assessment**
      - **Identify threat sources**
        - **Who is targeting me?**
      - **Identify threat events**
        - **What can they do? (Physical damage, Theft of Data, etc)**
      - **Determine impact on the organization**
        - **If a vulnerability was executed successfully, what would be the impact to the Confidentiality, Integrity, or Availability of my data?**
  - **Understand the value of their data**
    - **Categorization**

What is a Framework?

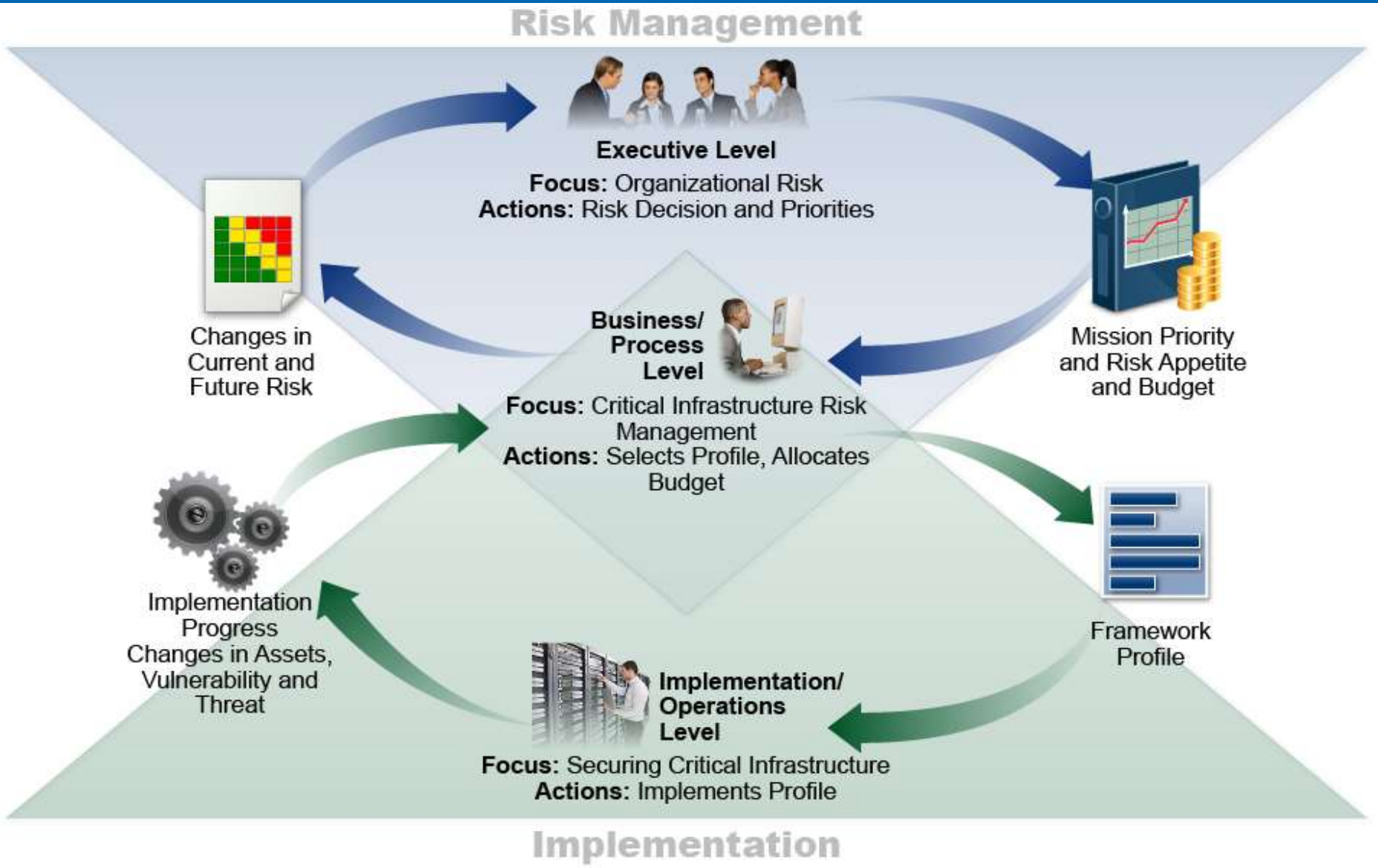
- **Frameworks require organizations to:**
  - **Document Policies and Procedures**
    - **Policies communicate the business priority, risk tolerance, and available resources from the executive level to the rest of the organization**
    - **Procedures ensure a continuity of operations**
  - **Assign Roles and Responsibilities**
    - **Eliminates ambiguity**
  - **Implement security**
    - **The act of implementing security features that align with the organizations categorization, business impact analysis, and risk assessment**
  - **Validate the effectiveness of their security**
    - **Cybersecurity Assessment**
    - **Security Controls Assessment**
    - **Penetration Testing**
  - **Continuously monitor**
    - **Ensure the implemented security is still providing an acceptable level of risk**

Why is a Framework so important?

- **Provides a context for implementing security**
- **Reduces the possibility of over or under securing your data**
- **Ensures continuity of solutions at all 3 levels of the organization**
  - **Executive Level**
  - **Operations Level**
  - **Implementation Level**

The framework will not eliminate the possibility of a breach. However, implementing the framework will give you a highly effective defensive posture that meets the criterion of “Due Diligence”

Risk Management Implementation



Frameworks

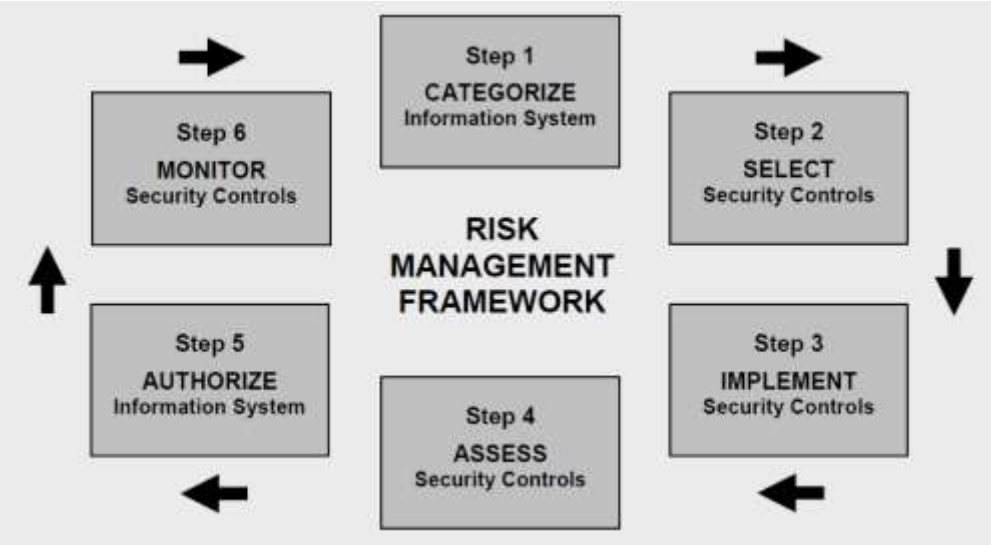
- **Examples of Frameworks include:**
  - **National Institute of Standards and Technology (NIST)**
    - **Risk Management Framework (RMF)**
      - **Developed for the Federal Government and its Contractors**
      - **Compulsory and Binding**
    - **CyberSecurity Framework (CSF)**
      - **Developed for Critical Infrastructure**
      - **Voluntary**

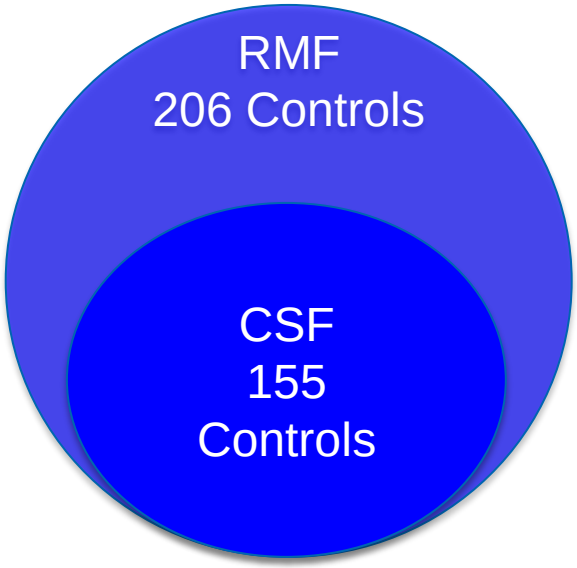
"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

- **Who can use these Frameworks?**
  - **Anyone!**
  - **Even if you have current "data-type specific" compliance requirements (HIPAA, PCI, SOX, …etc)**

RMF vs CSF?

- If you're not mandated to use a specific Framework, you can use either one.
- The primary difference between RMF and CSF is their approach
  - RMF – Implement based on the results of your categorization





  - CSF – Implement based on specific cybersecurity outcomes

How do I Implement a Framework?
Business Impact Analysis

- **Whether you implement RMF or CSF, the first priority is to understand your existing processes and the value of your data**
  - **Business Impact Analysis**
    - **Document your business processes and assets**
    - **Document how each process/asset interacts with the other processes within the organization**
    - **Document the different data types that exist within each process**
  - **Outcomes of a Business Impact Analysis**
    - **Identify network segmentation points**
    - **Predicts the consequences of disruption of a business function or process**
    - **Enables the development of recovery strategies**
    - **Provides the basis for investment in prevention and mitigation strategies**
- **Reference**
  - **NIST SP 800-34**

How do I Implement a Framework?
Risk Assessment

- **Identify Threats**
  - A threat is a possible action taken against you.
    - Threat Source – Who is likely to target me?
      - Non-Hostile (Reckless, Untrained employee, Vendor)
      - Hostile (Civil Activist, Data Miner, Disgruntled Employee, Nation-state or Government Cyber Warrior)
    - Threat Event – What action is a threat likely to take?
- **Identify Vulnerabilities**
  - A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
  - A cybersecurity assessment identifies weaknesses in your enterprise
    - Web Application Assessment
    - Network Architecture Review
    - Internal Cybersecurity Assessment
    - External Cybersecurity Assessment
    - Penetration Testing

How do I Implement a Framework?
Risk Assessment (cont.)

- **Web Application Assessment**
  - **Usually follows the OWASP methodology to detect vulnerabilities such as SQL injection, cross-site scripting (XXS), and session hijacking.**
  - **Using tools such as Cenzic Hailstorm, Burp suite Pro, and SQLmap**
- **Network Architecture Review (NAR)**
  - **Analysis of boundary devices for misconfigurations and default settings**
- **Internal/External Cybersecurity Assessment**
  - **Examine existing security mechanisms for effectiveness**
  - **Identify known vulnerabilities using tools such as Tenable's Nessus**
- **Penetration Testing**
- **Determine Likelihood and Impact**
- **Reference**
  - **NIST SP 800-30**

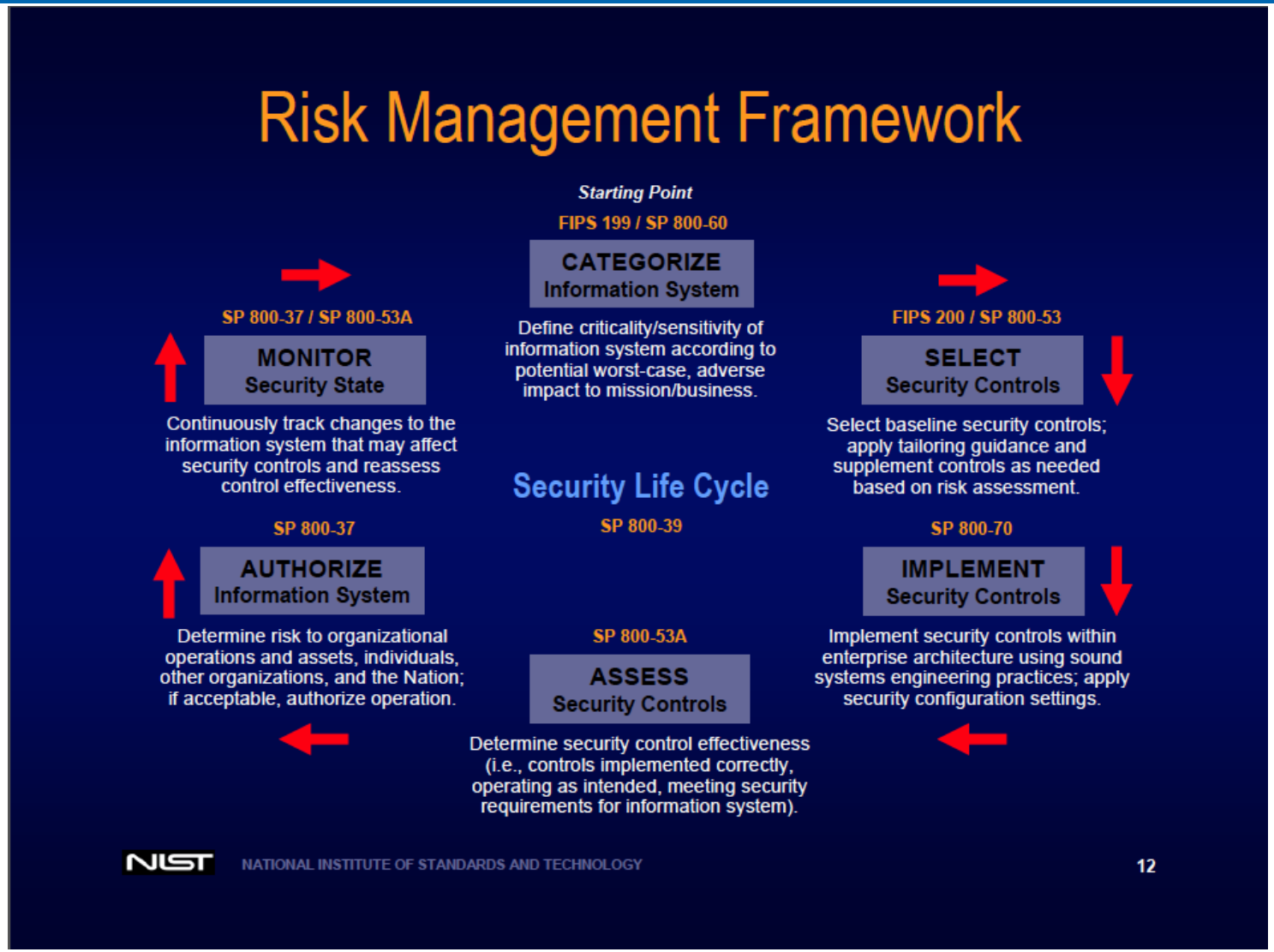
Risk is a function of the ***likelihood*** that a given ***threat*** can exploit an existing ***vulnerability*** that results in an adverse ***impact*** to the organization.

How do I Implement a Framework? Categorization

- **Determine the "Data Types" that exist within the organization**
  - **Financial data**
  - **Contract data**
  - **SCADA data**
- **Determine the Impact of a successful attack**
  - **What is the impact to the organization if…**
    - **Confidentiality – …this data was released to the public?**
    - **Integrity - …the content of this data was maliciously changed?**
    - **Availability - …access to this data was denied?**
- **Reference**
    - **FIPS – 199**
    - **NIST 800-60 Volume 2**

This is where implementation of the two frameworks diverge.

How do I Implement a Framework?
Risk Management Framework (RMF)



- **RMF – Implement based on the results of your categorization**

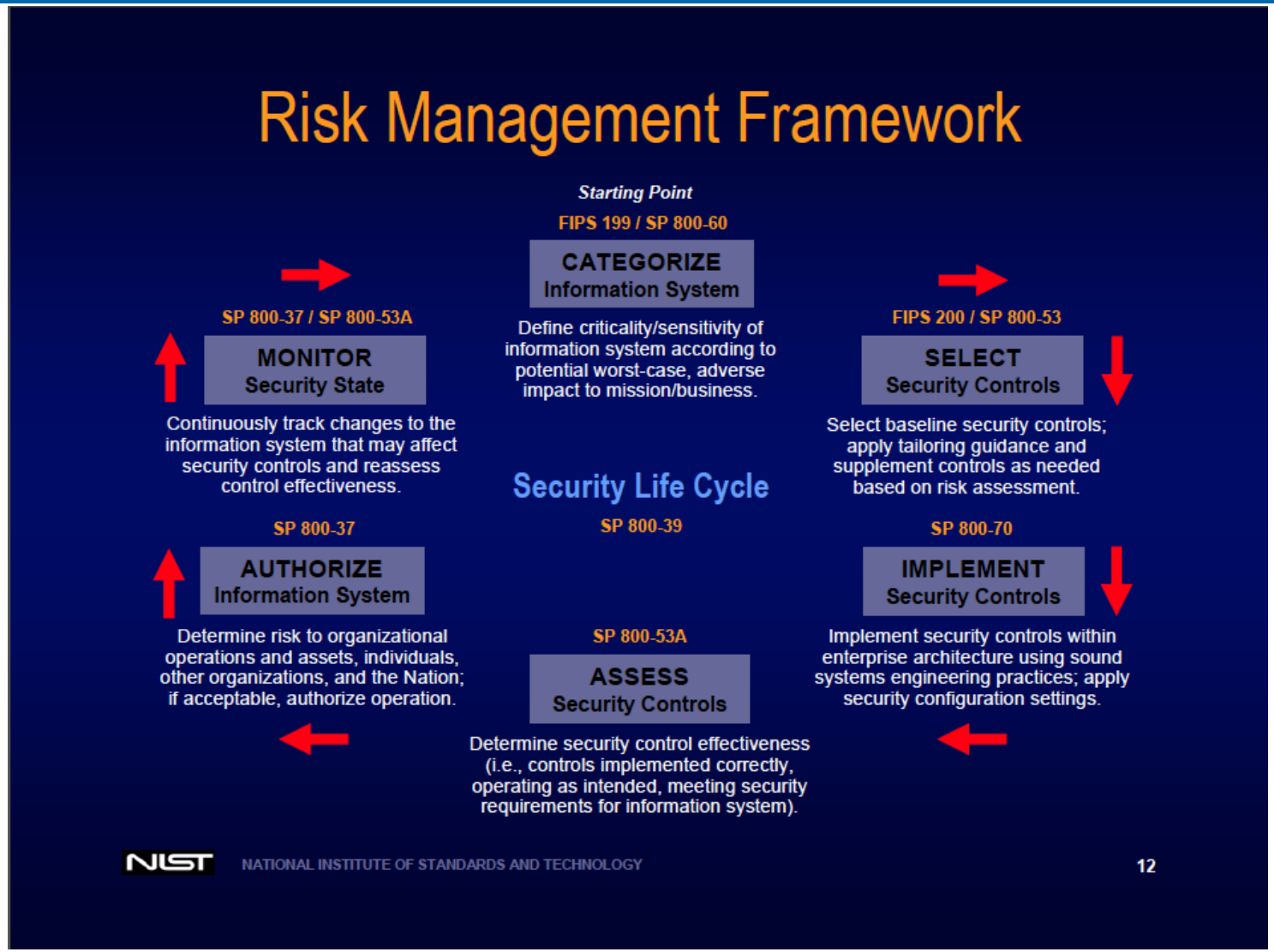
How do I Implement a Framework?
Risk Management Framework (RMF)

- Security Objectives - Consider Potential Impacts
  - Confidentiality – What if this data was released to the public?
  - Integrity – What if the content of the data was maliciously changed?
  - Availability – What if access to your data was denied?

Information Type	Confidentiality	Integrity	Availability
Public	N/A	Low	Moderate
Investigative	High	Moderate	Moderate
Contractual	Moderate	Moderate	Low
Sensor Data	N/A	High	High
SCADA	Moderate	High	High

Goal – Determine the “High Water Mark”

How do I Implement a Framework?
Risk Management Framework (RMF)



- **RMF – Implement based on the results of your categorization**

How do I Implement a Framework?
IA Security Control (NIST 800-53)

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AC-1	**MOD** AC-1	**HIGH** AC-1

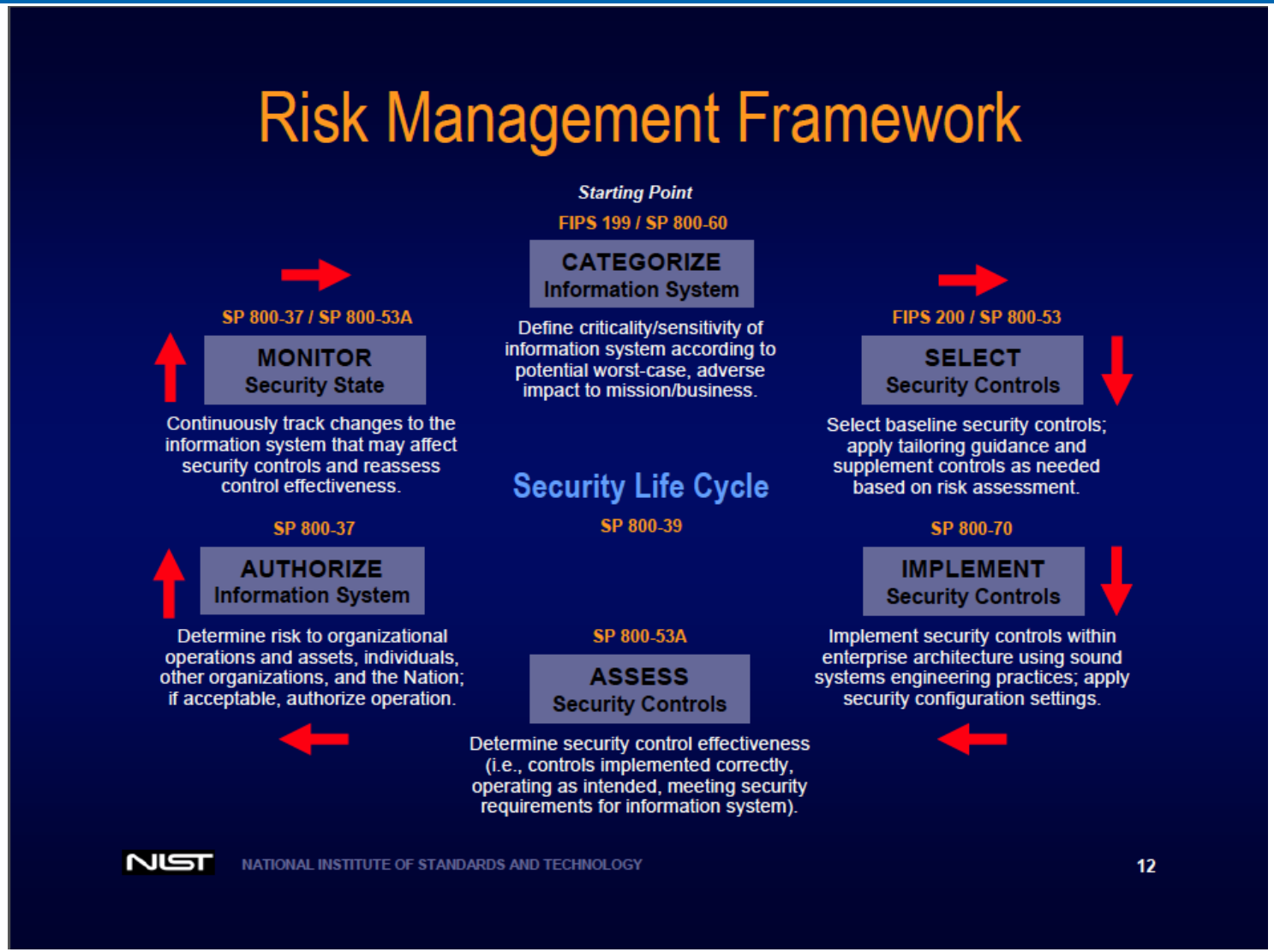
How do I Implement a Framework?
IA Security Control (NIST 800-53)

206 Total Security Controls

Low	Moderate	High
123	170	178

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** AC-10
P3	**LOW** Not Selected	**MOD** AC-11	**HIGH** AC-11
P1	**LOW** AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (2) (4) (5)
P1	**LOW** AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)
P1	**LOW** Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)
P2	**LOW** Not Selected	**MOD** IR-3	**HIGH** IR-3 (1)
P1	**LOW** Not Selected	**MOD** MA-6	**HIGH** MA-6

How do I Implement a Framework?
Risk Management Framework (RMF)



How do I Implement a Framework?
Risk Management Framework (RMF)

- **Implement the Security Controls**
  - Document the design, development, and implementation details for each control
- **Assess the Security Controls**
  - Determine the extent to which
    - Controls are implemented correctly
    - Operating as intended
    - Producing the desired outcome with respect to meeting the security requirements for the system
- **Authorize the Information System**
  - Based on risk to the organization is acceptable
- **Continuous Monitoring**
  - Performed on an ongoing periodic basis
  - Use Cybersecurity Assessments to
    - Determine control effectiveness
    - Determine continued compliance

How do I Implement a Framework?
CyberSecurity Framework (CSF)

- What assets need protection?
- Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management

- CSF – Implement based on specific cybersecurity outcomes

How do I Implement a Framework?
CyberSecurity Framework (CSF)

- **What safeguards are available?**
- **Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.**
- **Supports the ability to limit or contain the impact of a potential cybersecurity event.**

- **CSF – Implement based on specific cybersecurity outcomes**

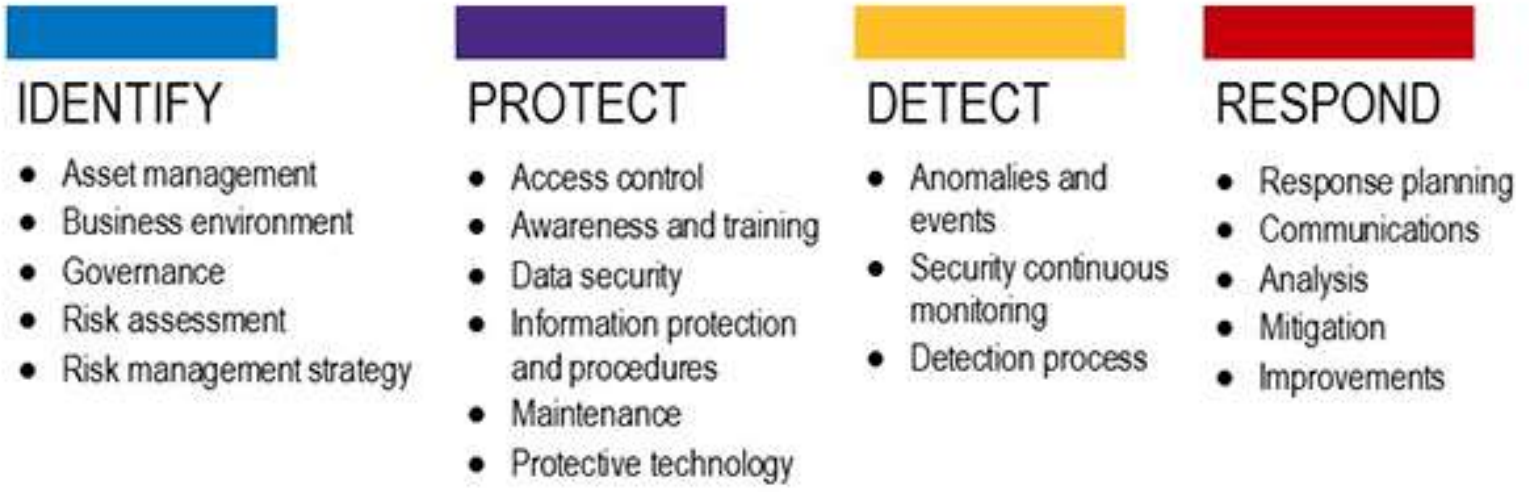
How do I Implement a Framework?
CyberSecurity Framework (CSF)

- What techniques can detect incidents?
- Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Enables timely discovery of cybersecurity events

- CSF – Implement based on specific cybersecurity outcomes

How do I Implement a Framework?
CyberSecurity Framework (CSF)

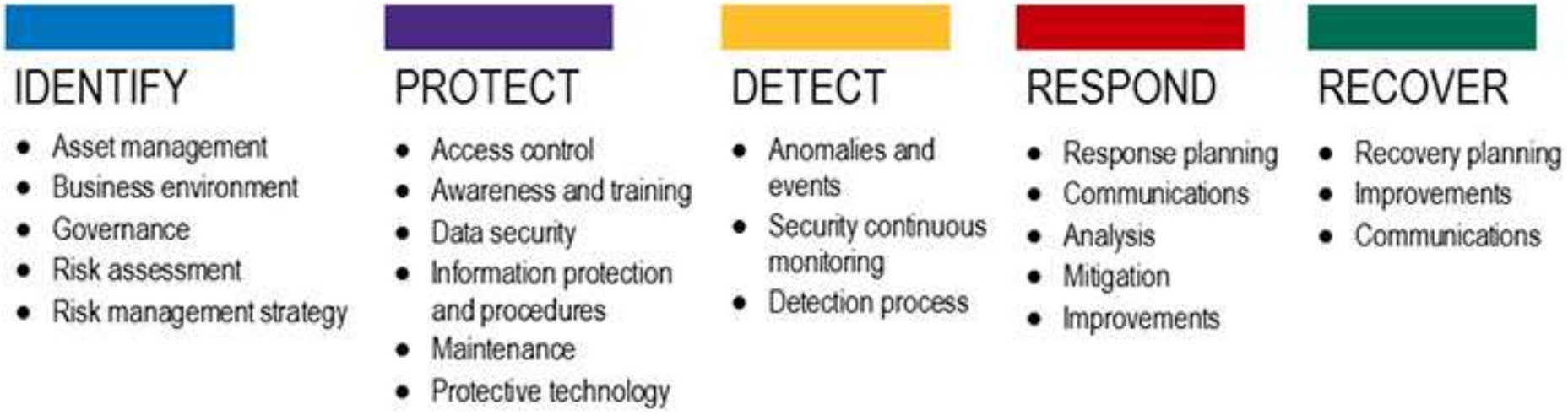
- What techniques can contain impacts of incidents?
- Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Supports the ability to contain the impact of a potential cybersecurity event



- CSF – Implement based on specific cybersecurity outcomes

How do I Implement a Framework?
CyberSecurity Framework (CSF)

- What techniques can restore capabilities?
- 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.
- Supports timely recovery to normal operations to reduce the impact from a cybersecurity event



- CSF – Implement based on specific cybersecurity outcomes

How do I Implement a Framework?
Create a Current Profile (CSF)

- **Identify which Category & Subcategory outcomes are currently being achieved**
  - **Identify**
    - **Do we have an organizational understanding that's detailed enough to successfully manage cybersecurity risk to systems, assets, data, and capabilities?**
  - **Protect**
    - **How effective are we in our ability to limit or contain the impact of a potential cybersecurity event?**
  - **Detect**
    - **How effective are we at developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event?**
  - **Respond**
    - **Do we have the ability to contain the impact of a potential cybersecurity event?**
  - **Recover**
    - **Have we implemented the appropriate activities necessary to support a timely recovery to normal operations to reduce the impact of a cybersecurity event?**

How do I Implement a Framework?
Create a Target Profile (CSF)

- **Examine each Category & Subcategory to determine the desired outcome**

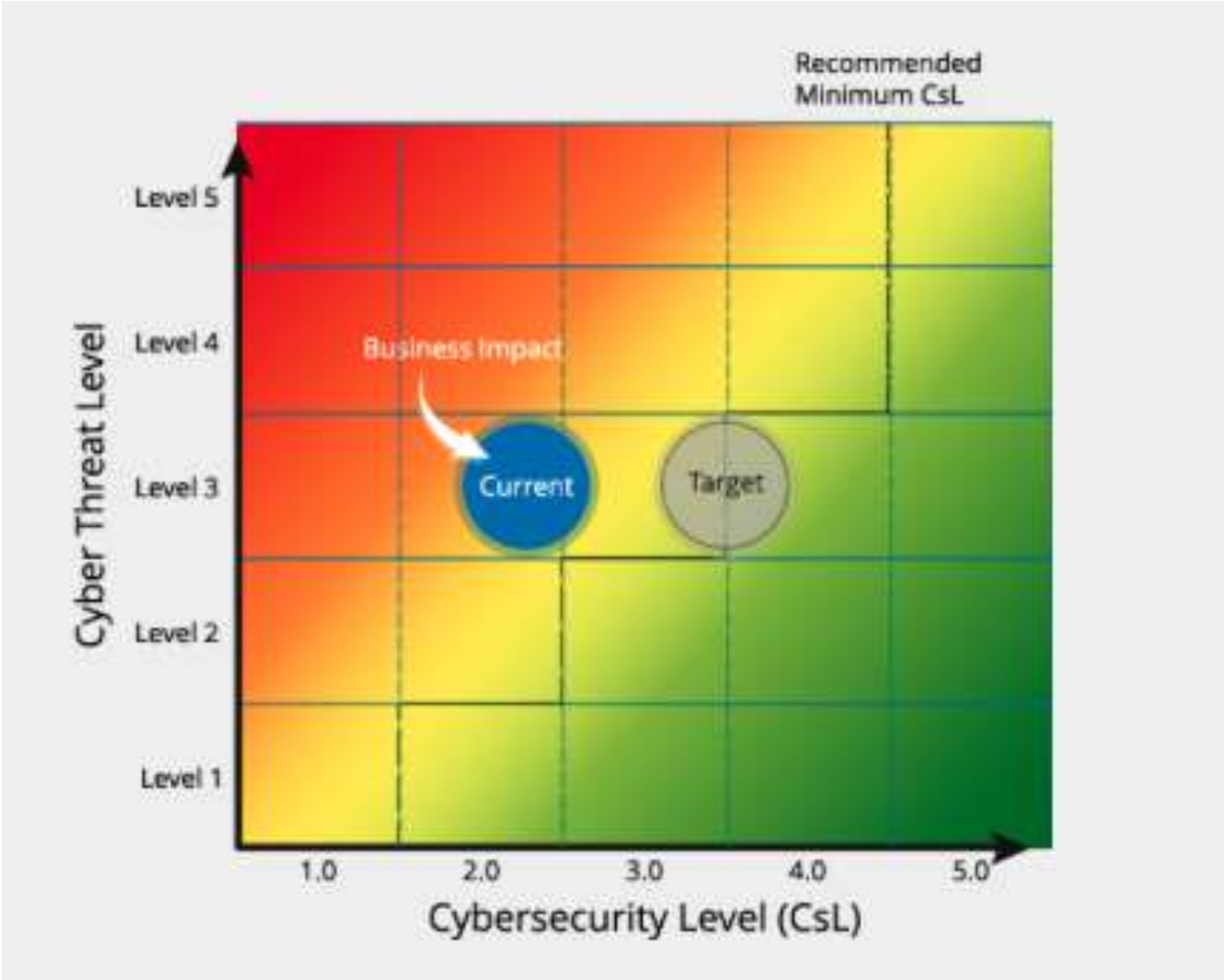
How do I Implement a Framework? Create a Target Profile (CSF)

- **Examine each Category & Subcategory to determine the desired outcome**

Function	Category	Subcategory
Detect	Security Continuous Monitoring - The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	The network is monitored to detect potential cybersecurity events
		The physical environment is monitored to detect potential cybersecurity events
		Personnel activity is monitored to detect potential cybersecurity events
		Malicious code is detected
		Unauthorized mobile code is detected
		External service provider activity is monitored to detect potential cybersecurity events
		Monitoring for unauthorized personnel, connections, devices, and software is performed
		Vulnerability scans are performed

Cyber Risk Profile

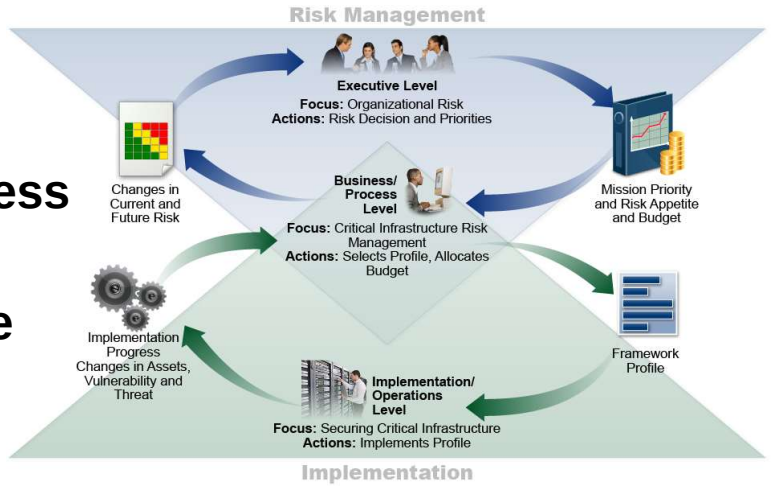
- **Business Impact**
- **Cyber Threat Level**
- **Cybersecurity Level**



http://www.dynetics.com/riskscope/

How do I Implement a Framework?
Implement a Plan of Action and Milestones (CSF)

- **Determine, Analyze, and Prioritize Gaps**
  - Compare the current profile to the target profile to determine gaps
  - Create a prioritized action plan to address the gaps based upon:
    - Business Impact
    - Cyber Threat Level
    - Cybersecurity level
  - Determine resources necessary to address the gaps
  - Flow this information up the chain to the Executive Level



- **Outcome**
  - Enables the organization to make informed decisions about cybersecurity activities
  - Supports Risk Management
  - Enables the organization to perform cost-effective, targeted improvements

Summary – How Do You Implement a Framework

- **Understand your System**
  - **Business Impact Analysis**
  - **Cyber Threat Assessment**
  - **Categorization**
- **Identify the Framework You Want to Implement**
  - **Based on Categorization**
  - **Based on Outcomes**
- **Risk Management Framework**
  - **Categorization, Select Controls, Implement Controls, Assess Controls, Authorize the System, Continuously Monitor**
- **CyberSecurity Framework**
  - **Develop Current Profile, Determine Target Profile, Develop a POA&M based on Gaps using the References as a guide**

Questions?

- **How much security is enough?**
- **How do I prioritize decisions when it comes to security?**
- **How do I know what to protect?**

Dynetics

PO Box 5500 • Huntsville, AL 35814
www.dynetics.com

Greg Jackson
Sr. Cyber Security Analyst

1004 Explorer Blvd
Huntsville, AL 35806

Office: 256 964-4692
Mobile: 256 683-6296
greg.jackson@dynetics.com

Dynetics is an employee-owned company.

Contact Information

Dynetics

PO Box 5500 • Huntsville, AL 35814
www.dynetics.com

Greg Jackson
Sr. Cyber Security Analyst

1004 Explorer Blvd
Huntsville, AL 35806

Office: 256 964-4692
Mobile: 256 683-6296
greg.jackson@dynetics.com

Dynetics is an employee-owned company.