

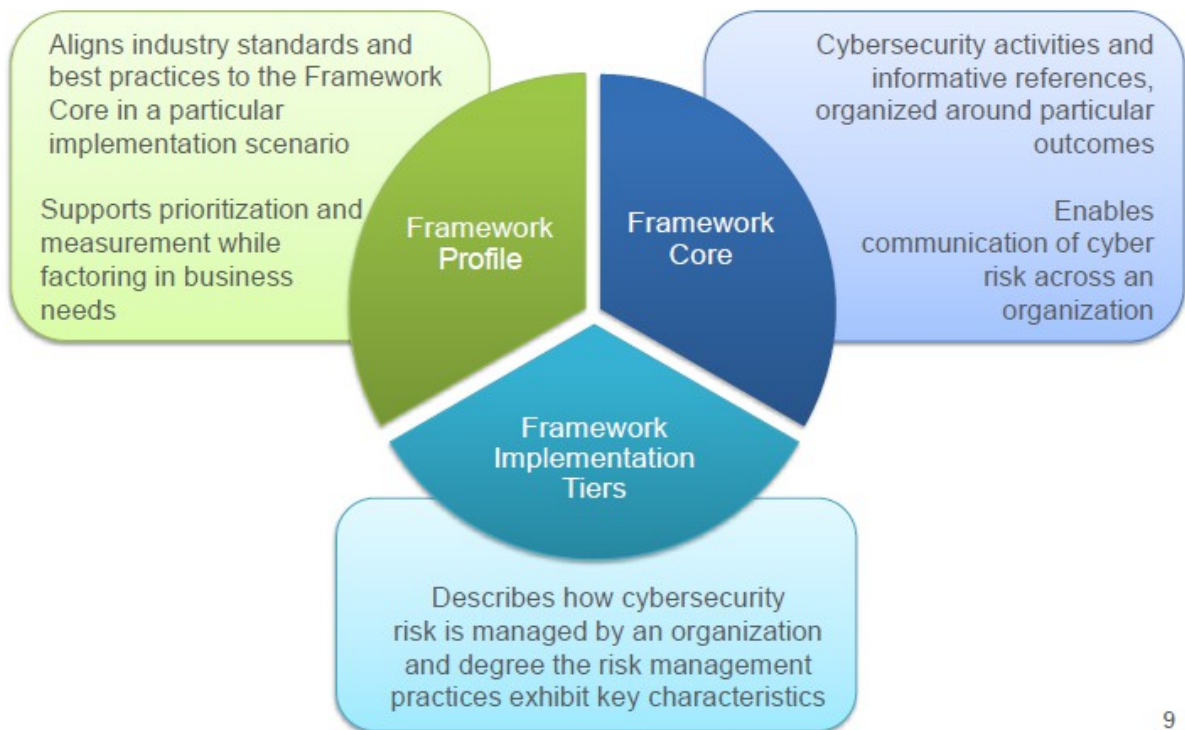
Cyber Security Framework

“The Threat Situation: Continuing serious cyber attacks on information systems, large and small; targeting key federal, state, local, and private sector operations and assets...”

- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated
 - Adversaries are nation states, terrorist groups, criminal hackers, and individuals or groups with intentions of compromising your information.
 - Effective deployment of malicious software causing significant exfiltration of sensitive information (including intellectual property) and potential for disruption of critical information system/services.”
- Dr. Ron Ross, NIST Computer Security Division, Information Technology Laboratory

NIST - 3 Parts

Framework Components



9

1. The Framework Core

- 1.1. Set of cybersecurity activities
 - (1) 5 concurrent and continues Functions
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 1: Framework Core Structure

- 1.2. Outcomes
- 1.3. Informative references – from following Frameworks:
 - (1) **CCS CSC**
 - (2) **COBIT5**
 - (3) **NIST SP 800-53**
 - (4) **HIPAA Security Rule 45 C.F.R.**
 - (5) **ISA 62443-2-1: 2009 & 62443-3-3: 2013**
 - (6) **ISO/IEC 27001:2013**
- 1.4. Detailed guidance to develop profile

2. The Framework Profile

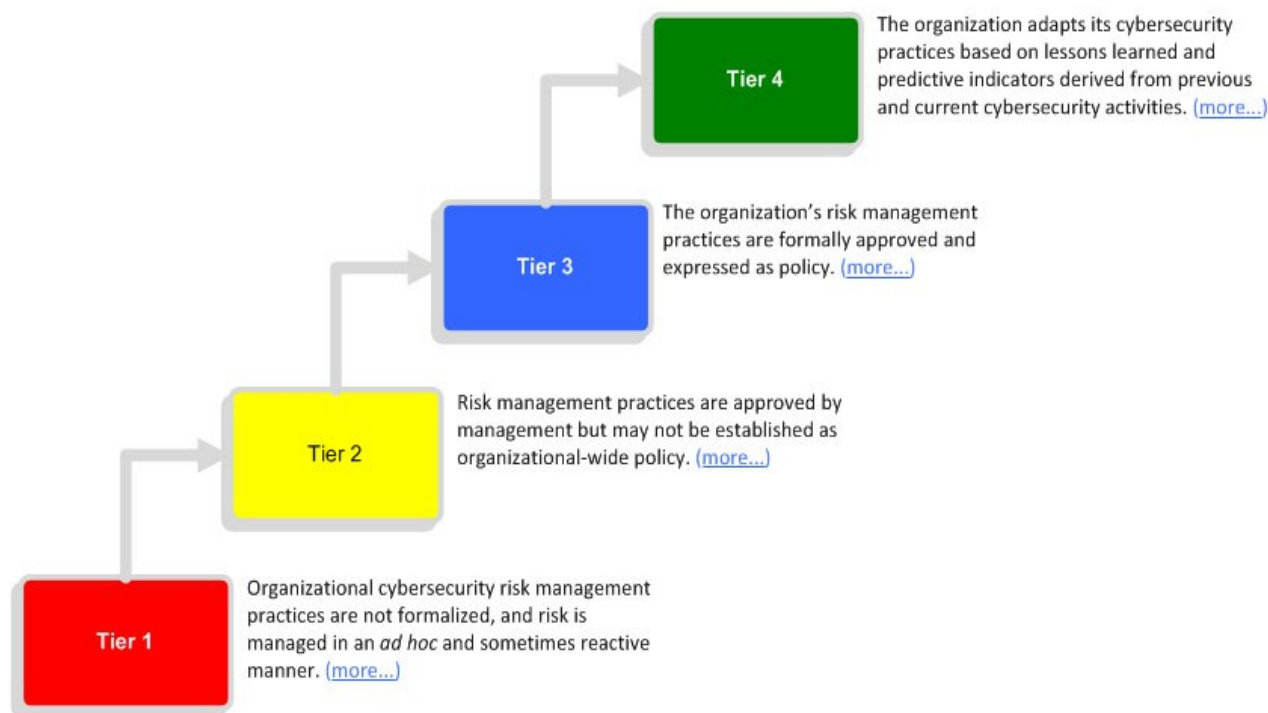
- 2.1. Represents outcomes based on business needs that an organization selected from the Framework Categories and Subcategories
- 2.2. Alignment of standards, guidelines and practices to the Framework
- 2.3. Opportunity of improvements comparing “Current Profile” With “Target “Profile
- 2.4. Helps organizations align its cybersecurity activities with biz requirements, risk tolerance, resources.

PROFILE



3. The Framework Implementation Tiers

- 3.1. Provide a mechanism for organizations to view and understand characteristics of their approach to managing cybersecurity risk
- 3.2. Describe the degree to which an organization cybersecurity risk management practices exhibit the characteristic defined in the Framework.
 - (1) Risk
 - (2) Threat awareness
 - (3) repeatable
 - (4) adaptive



3.3. Tier 1 Partial

- (1) • *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- (2) • *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- (3) • *External Participation* – An organization may not have the processes in place to participate in coordination or collaboration with other entities.

3.4. Tier 2 Risk Informed

- (1) • *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- (2) • *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.
- (3) • *External Participation* – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

3.5. Tier 3 Repeatable

- (1) • *Risk Management Process* – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- (2) • *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to

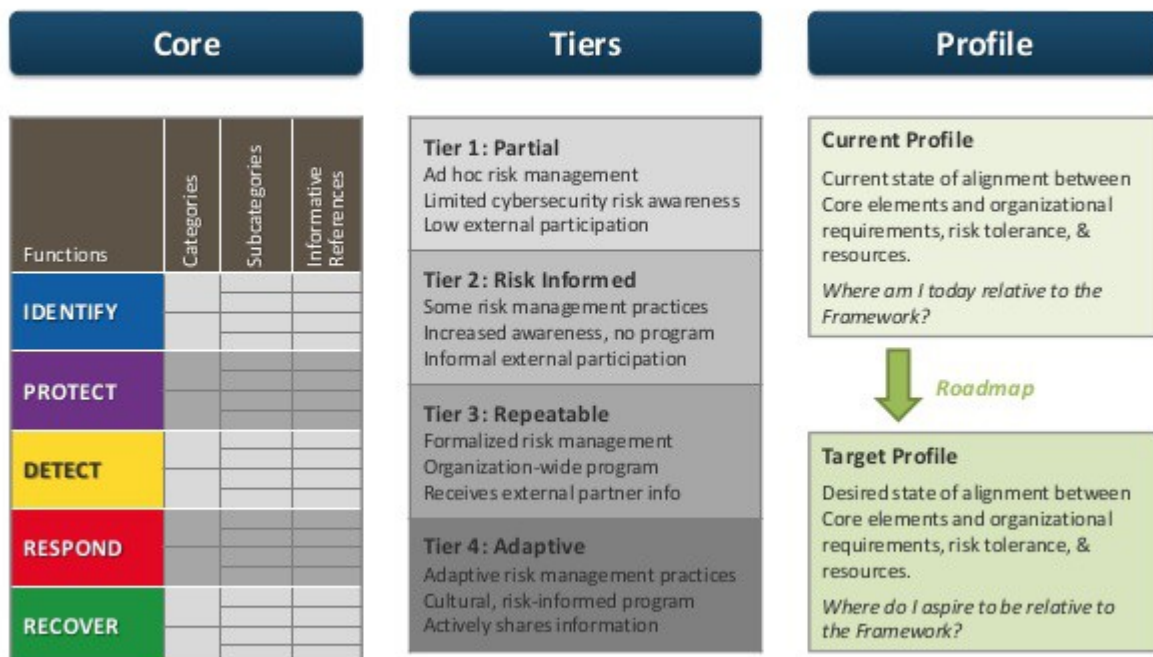
changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.

- (3) • *External Participation* – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

3.6. Tier 4 Adaptive

- (1) • *Risk Management Process* – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- (2) • *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- (3) • *External Participation* – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

NIST Cybersecurity Framework



3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.