2.2 Framework Profile

A Framework Profile ("Profile") is a tool to enable organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organization and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. A Framework Profile can be used to describe both the current state and the desired target state of specific cybersecurity activities, thus revealing gaps that can be addressed to meet cybersecurity risk management objectives. **Figure 2** shows the two types of Profiles: Current and Target. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. The Target Profile is built to support critical infrastructure requirements and aid in the communication of risk within and between organizations.

The Profile is the alignment of the Functions, Categories, Subcategories and industry standards with the business requirements, risk tolerance, and resources of the organization. The prioritization of the gaps is driven by the selection of the Framework Tier and organization's Risk Management Processes which can serve as an essential part for resource and time estimates needed that are critical to prioritization decisions.

Figure 2: Profile Comparisons

1/1/01 12:00 AM
Deleted: should

1/1/01 12:00 AM
Deleted: business/mission

1/1/01 12:00 AM
Comment [1]: This same thought is said in paragraph above.

1/1/01 12:00 AM
Deleted: and best practices

1/1/01 12:00 AM
Deleted: Identifying the gaps between the Current Profile and the Target Profile allows the creation of a prioritized roadmap that organizations will implement to reduce cybersecurity risk.

1/1/01 12:00 AM
Deleted: and

1/1/01 12:00 AM
Comment [2]: Add a footnote that says: "The process for selecting the appropriate Tier and performing an assessment to the Framework Functions is intentionally not identified within the Framework. This activity is left to the Sector Specific Agency and critical infrastructure organization to determine through their voluntary participation in the Framework."

This allows our sector to utilize our own documents such as the C2M2 and RMP.

1/1/01 12:00 AM
Formatted: File Stamp

1/1/01 12:00 AM
Formatted: File Stamp Character

The Framework provides a mechanism for critical infrastructure organizations, sectors, and other entities to create their own Target Profiles. It does not provide Target Profile templates; rather, sectors and organizations should identify existing Target Profiles based on their risk determinations and needs.

2.3 Coordination of Framework Implementation

2.4 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") describe how an organization manages its implementation of the Framework Functions and critical infrastructure cybersecurity risk management practices. The Tiers range from Not Initiated (Tier 0) to Adaptive (Tier 4) and describe an increasing degree of rigor and institutionalization of cybersecurity risk management practices and the extent to which cybersecurity risk management is integrated into an organization's overall risk management practices. The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, critical infrastructure business/mission objectives, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected levels meet the organizational goals, reduce cybersecurity risk to critical infrastructure, and are feasible and cost-effective to implement. The Tier definitions are as follows:

- Tier 0: Not Initiated
  - Risk Management Process – The Framework Functions and critical infrastructure cybersecurity risk management practices do not exist.
  - Integrated Program – There is no approach to managing cybersecurity risk in the organization.
  - Information Sharing – The organization has not established internal or external cybersecurity information sharing.
- **Tier 1: Initiated**
  - Risk Management Process – The Framework Functions and critical infrastructure cybersecurity risk management practices are not formalized and risk is managed in an ad hoc, irregular and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements essential for critical infrastructure.
  - Integrated Program – There is a limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or inadequate resources.
  - Information Sharing – The organization may not have processes that enable cybersecurity information to be shared within the organization. An organization may not have the processes in place to participate in coordination or collaboration with other entities.

1/1/01 12:00 AM
Deleted: that could be customized

1/1/01 12:00 AM
Deleted: for their purposes

1/1/01 12:00 AM
Comment [3]: Move to How To Section intro.

1/1/01 12:00 AM
Deleted: **Figure 3** describes the notional flow of information and decisions within an organization: at the senior executive level, at the business/process level, and at the implementation/operations le... [1]

1/1/01 12:00 AM
Deleted: Partial (Tier 1)

1/1/01 12:00 AM
Deleted: sophistication

1/1/01 12:00 AM
Deleted: in

1/1/01 12:00 AM
Formatted

1/1/01 12:00 AM
Formatted: Font:Not Bold

1/1/01 12:00 AM
Deleted: **Partial**

1/1/01 12:00 AM
Deleted: Organizational

1/1/01 12:00 AM
Deleted: and an organization-wide approach to managing cybersecurity risk has not been established

Scott Saunders 12/6/13 9:13 AM
Moved down [1]: The organization may not have processes that enable cybersecurity information to be shared within the organization.

1/1/01 12:00 AM
Deleted: or information gained from outside sources

1/1/01 12:00 AM
Deleted: External Participation

Scott Saunders 12/6/13 9:13 AM
Moved (insertion) [1]

1/1/01 12:00 AM
Formatted: File Stamp

1/1/01 12:00 AM
Formatted: File Stamp Character

- **Tier 2: Risk-Informed**
  - Risk Management Process – The Framework Functions and critical infrastructure risk management practices are supported by management but may not be established as documented policy.
  - Integrated Program – There is an awareness of cybersecurity risk at the critical infrastructure operations level but an integrated, overall organization-wide approach to managing critical infrastructure cybersecurity risk has not been established. Risk-informed processes and procedures are identified. Cybersecurity personnel resources have been identified but may not be dedicated to or have sufficient knowledge and skills to perform their cybersecurity duties.
  - Information Sharing – Cybersecurity information is shared within the organization on an informal basis. The organization knows its role in critical infrastructure, but has not formalized its capabilities to interact and share information externally.
- **Tier 3: Risk-Informed and Repeatable**
  - Risk Management Process – The Framework Functions and critical infrastructure risk management practices are formally supported by management and expressed as policy. The cybersecurity practices are regularly updated based on the application of risk management processes to a changing threat and technology landscape.
  - Integrated Program – There is a formalized approach to manage cybersecurity risk for the critical infrastructure operations. Repeatable, risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. Consistent methods are in place to effectively respond to changes in risk. There are adequate personnel resource who possess the knowledge and skills to perform their appointed cybersecurity roles and responsibilities.
  - Information Sharing – Cybersecurity information is shared in a consistent documents process within the organization. The organization understands its critical infrastructure dependencies and partners and receives information from these partners enabling collaboration and risk-based management decisions within the organization in response to events.
- **Tier 4: Adaptive**
  - Risk Management Process – The Framework Functions and critical infrastructure risk management practices are implemented in a manner that allows the organization to readily adapt its cybersecurity practices based on lessons learned and predictive indicators derived from previous cybersecurity activities. Through a process of continuous improvement, the organization actively adapts to a changing cybersecurity landscape and responds to emerging/evolving threats in a timely manner.
  - Integrated 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

1/1/01 12:00 AM
Deleted: R

1/1/01 12:00 AM
Deleted: approved

1/1/01 12:00 AM
Deleted: organizational-wide

1/1/01 12:00 AM
Deleted: organizational

1/1/01 12:00 AM
Deleted: an

1/1/01 12:00 AM
Deleted: , management-approved

1/1/01 12:00 AM
Deleted: defined

1/1/01 12:00 AM
Deleted: and implemented and staff has adequate

Scott Saunders 12/6/13 9:14 AM
Moved down [2]: Cybersecurity information is shared within the organization on an informal basis.

1/1/01 12:00 AM
Deleted: External Participation

Scott Saunders 12/6/13 9:14 AM
Moved (insertion) [2]

1/1/01 12:00 AM
Deleted: the larger

1/1/01 12:00 AM
Deleted: ecosystem

1/1/01 12:00 AM
Deleted: organization's

1/1/01 12:00 AM
Deleted: approved

1/1/01 12:00 AM
Deleted: Organizational

1/1/01 12:00 AM
Deleted: an organization-wide

1/1/01 12:00 AM
Deleted: R

1/1/01 12:00 AM
Deleted: Personnel

1/1/01 12:00 AM
Deleted: External Participation

1/1/01 12:00 AM
Deleted: s

1/1/01 12:00 AM
Formatted: File Stamp

1/1/01 12:00 AM
Formatted: File Stamp Character

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 that support critical infrastructure.

- Information Sharing – The organization manages risk and actively shares information with internally and externally to ensure that accurate, current information is being distributed and consumed to improve the cybersecurity risk posture before an event occurs.

==========

The following is an alternative view of the Framework Tiers that more prominently displays the link to the Framework Functions.

- Tier 0: Not Initiated
  - Framework Functions – The implementation of the Framework Functions do not exist.
  - Risk Management Process – The critical infrastructure cybersecurity risk management practices do not exist.
  - Integrated Program – There is no approach to managing cybersecurity risk in the organization.
  - Information Sharing – The organization has not established internal or external cybersecurity information sharing.
- **Tier 1: Primary** /Elementary / Ad-hoc / Entry-Level /
  - Framework Functions – The implementation of the Framework Functions are not formalized and may be ad hoc, irregular, and sometimes reactive to cybersecurity events.
  - Risk Management Process – The critical infrastructure cybersecurity risk management practices are not formalized and risk is managed in an ad hoc, irregular and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or critical infrastructure business/mission requirements.
  - Integrated Program – There is a limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or inadequate resources.
  - Information Sharing – The organization may not have processes that enable cybersecurity information to be shared within the organization. An organization may not have the processes in place to participate in coordination or collaboration with other entities.
- **Tier 2: Risk-Informed**

1/1/01 12:00 AM
Deleted: External Participation

1/1/01 12:00 AM
Deleted: partners

1/1/01 12:00 AM
Comment [4]: May be better for the Informative References section or even added to the intro of the How To section.

1/1/01 12:00 AM
Deleted: Organizations should consider leveraging external guidance, such as information that could be obtained from Federal government departments and agencies, an Information Sharing and Analysis Center (ISAC), existing maturity models, or other sources to assist in determining their desired tier.

1/1/01 12:00 AM
Deleted: .

1/1/01 12:00 AM
Formatted: File Stamp

1/1/01 12:00 AM
Formatted: File Stamp Character

- Framework Functions – The implementation of the Framework Functions are approved by management, include limited information about cybersecurity risks, but may not be documented in policy.
- Risk Management Process – The critical infrastructure risk management practices are approved by management but may not be established as documented policy.
- Integrated Program – There is an awareness of cybersecurity risk at the critical infrastructure operations level but an integrated, overall organization-wide approach to managing critical infrastructure cybersecurity risk has not been established. Risk-informed processes and procedures are identified. Cybersecurity personnel resources have been identified but may not be dedicated to or have sufficient knowledge and skills to perform their cybersecurity duties.
- Information Sharing – Cybersecurity information is shared within the organization on an informal basis. The organization knows its role in the larger critical infrastructure ecosystem, but has not formalized its capabilities to interact and share information externally.

- **Tier 3: Repeatable**
  - Framework Functions – The implementation of the Framework Functions are formally approved by management expressed in policy and receive adequate resources for sustainability.
  - Risk Management Process – The critical infrastructure risk management practices are formally approved by management and expressed as policy. The cybersecurity practices are regularly updated based on the application of risk management processes to a changing threat and technology landscape.
  - Integrated Program – There is a formalized approach to manage cybersecurity risk for the critical infrastructure operations. Repeatable, risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. Consistent methods are in place to effectively respond to changes in risk. There are adequate personnel resource who possess the knowledge and skills to perform their appointed cybersecurity roles and responsibilities.
  - Information Sharing – Cybersecurity information is shared in a consistent documents process within the organization. The organization understands its dependencies and partners and receives information from these partners enabling collaboration and risk-based management decisions within the organization in response to events.
- **Tier 4: Adaptive**
  - Framework Functions – The implementation of the Framework Functions are continuously monitored to ensure they are still meeting the intended cybersecurity risk management outcomes.
  - Risk Management Process – The critical infrastructure risk management practices are implemented in a manner that allows the organization to readily adapt its cybersecurity practices based on lessons learned and predictive indicators derived from previous cybersecurity activities. Through a process of continuous

1/1/01 12:00 AM
Formatted: File Stamp
1/1/01 12:00 AM
Formatted: File Stamp Character

improvement, the organization actively adapts to a changing cybersecurity landscape and responds to emerging/evolving threats in a timely manner.

- Integrated 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.
- Information Sharing – The organization manages risk and actively shares information with internally and externally to ensure that accurate, current information is being distributed and consumed to improve the cybersecurity risk posture before an event occurs.

1/1/01 12:00 AM
Formatted: File Stamp

1/1/01 12:00 AM
Formatted: File Stamp Character

Figure 3 describes the notional flow of information and decisions within an organization: at the senior executive level, at the business/process level, and at the implementation/operations level.

The senior executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into their risk management process, and then collaborates with the implementation/operations level to create a Profile. The implementation/operation level communicates the Profile implementation to the business/process level. The business/process level uses this information to perform an impact assessment. The outcomes of that impact assessment are reported to the senior executive level to inform the organization's overall risk management process.

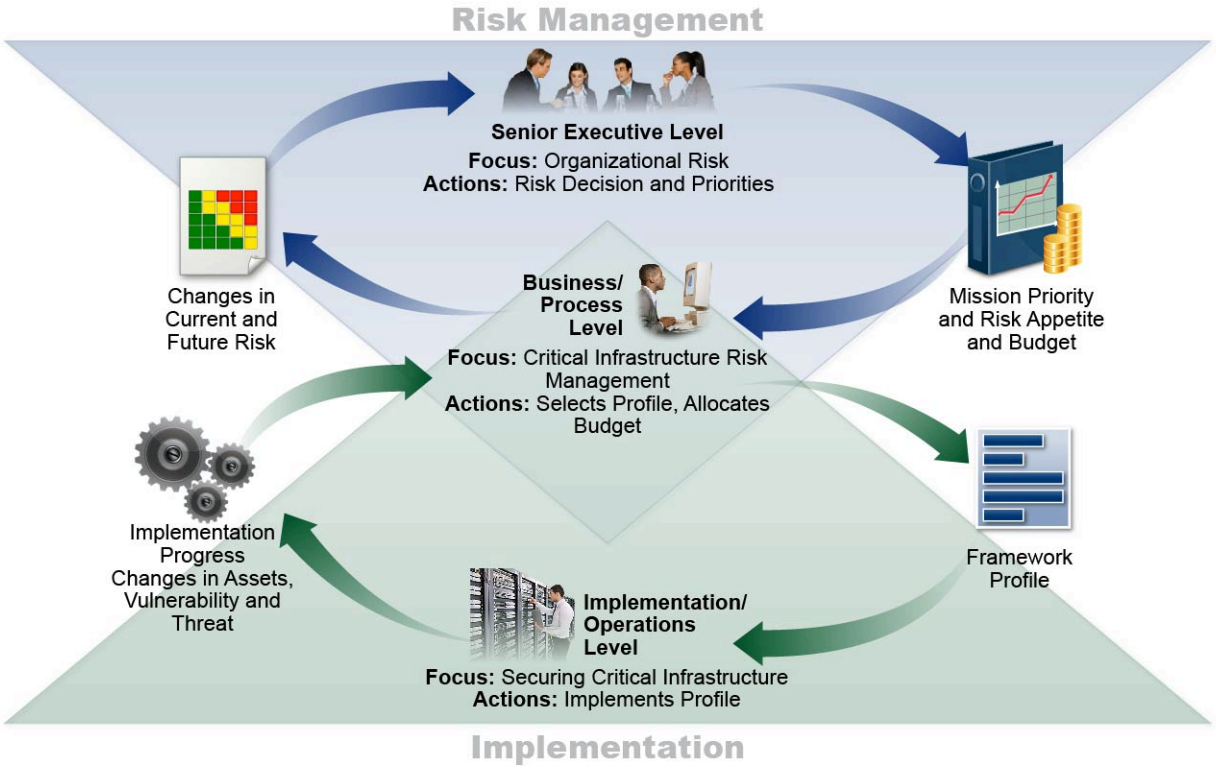

Figure 3: Notional Information and Decision Flows within an Organization