

APPA-LPPC Att. B

3.0 How to Use the Framework

The Framework is designed to complement existing critical infrastructure cybersecurity operations or serve as the foundation for a new cybersecurity program. The Framework also provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps and improvements to critical infrastructure cybersecurity practices. Using the Framework, organizations can examine what capabilities they have implemented in the five high-level Functions identified in the Framework Core.

3.1 Coordination of Framework Implementation

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 critical infrastructure 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.

1/1/01 12:00 AM
Formatted: None, Indent: Left: 0", First line: 0", Space Before: 0 pt, After: 12 pt, Don't keep with next

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

1/1/01 12:00 AM
Deleted: It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program.

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

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

Scott Saunders 12/5/13 8:41 PM
Moved down [2]: The following examples present several options for using the Framework.

1/1/01 12:00 AM
Deleted: - ... [1]

1/1/01 12:00 AM
Deleted: 0

1/1/01 12:00 AM
Deleted: : Identify, Protect, Detect, Respond, and Recover

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

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

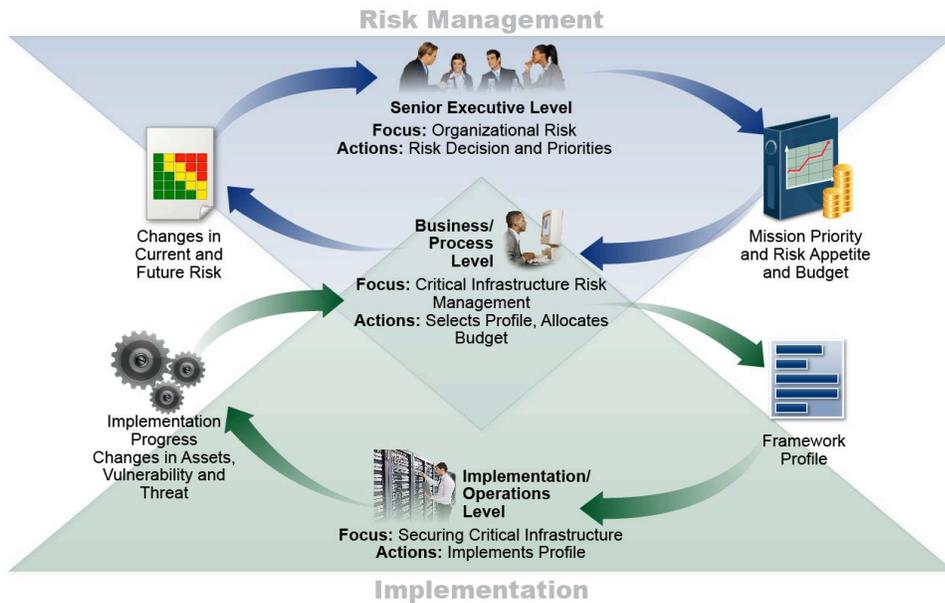


Figure 3: Notional Information and Decision Flows within an Organization

3.2 Using the Framework

The following recursive steps illustrate how an organization could use the Framework Core, Profiles and Tiers to assess and update an existing cybersecurity program; or create a new cybersecurity program. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to create an action plan for targeted improvements.

Step 1: The organization identifies the scope of the critical infrastructure operations that will be assessed in the Step 2 activity. The organization identifies relative to their critical infrastructure operations, systems and assets, the associated risk tolerances, threats, vulnerabilities, constraints, impacts of a cybersecurity event, voluntary and mandatory regulatory requirements and overall risk management approach. The organization also selects the appropriate Framework Informative References or chooses other Informative References that are sector or organization specific.

Step 2: The organization develops a Current Framework Profile using each of the Framework Core Functions, Categories and Subcategories. The organization performs an assessment of their existing critical infrastructure cybersecurity practices according to the critical infrastructure operations that were selected in the Step 1 activity.

- 1/1/01 12:00 AM
Formatted: None, Indent: Left: 0", First line: 0", Space Before: 0 pt, After: 12 pt, Don't keep with next
- Scott Saunders 12/5/13 8:41 PM
Moved (insertion) [2]
- 1/1/01 12:00 AM
Deleted: The following examples present several options for using the Framework. Organizations should have at least basic capabilities implemented in each of these areas, and can begin to review what particular categories and subcategories they currently use to help achieve those outcomes. ... [2]
- 1/1/01 12:00 AM
Formatted: Font:Font color: Auto, Not Expanded by / Condensed by
- 1/1/01 12:00 AM
Formatted: Font:Not Bold, Font color: Auto, Not Expanded by / Condensed by
- 1/1/01 12:00 AM
Deleted: 2
- 1/1/01 12:00 AM
Deleted: Establishing or Improving a Cybersecurity Program
- 1/1/01 12:00 AM
Deleted: recommended
- 1/1/01 12:00 AM
Deleted: or improve an existing cybersecurity program
- Scott Saunders 12/5/13 8:35 PM
Moved (insertion) [1]
- 1/1/01 12:00 AM
Deleted: perform
- 1/1/01 12:00 AM
Deleted: Identify.
- 1/1/01 12:00 AM
Deleted: its mission objectives, related systems and assets
- 1/1/01 12:00 AM
Deleted: Create a Current Profile.
- 1/1/01 12:00 AM
Deleted: Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.
- 1/1/01 12:00 AM
Formatted: File Stamp
- 1/1/01 12:00 AM
Formatted: File Stamp Character

Step 3: The organization analyzes the results of the Current Framework Profile to determine which Framework Tier corresponds to their existing critical infrastructure cybersecurity practices. The organization then determines whether the existing “Current State” Framework Profile is sufficient based on the risk management approach identified in the Step 1 activity.

Step 4: If the organization desires modify its Current Framework Profile, the organization can create a Target Framework Profile that focuses on determining the desired cybersecurity outcome along with a desired Framework Tier. The organization develops and implements an action plan to deploy the cybersecurity practices in the “Target State” Framework Profile.

Step 5: Once the organization achieves the Target Framework Profile, it then implements a monitoring plan to ensure selected cybersecurity practices are achieving the desired outcomes over time. The organization also develops a continuous monitoring strategy for when to initiate the recursive Step 1 activity.

1/1/01 12:00 AM

Deleted: Conduct a Risk Assessment.

1/1/01 12:00 AM

Deleted: 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 critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

1/1/01 12:00 AM

Comment [1]: Was implements here too. Thought that was too many implements in one sentence. Not sure the deploy is the right word either – thoughts?

1/1/01 12:00 AM

Deleted: The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization’s desired cybersecurity outcomes. ... [3]

Scott Saunders 12/5/13 8:35 PM

Moved up [1]: The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

1/1/01 12:00 AM

Deleted: Create a Target Profile.

1/1/01 12:00 AM

Formatted: Space After: 12 pt

1/1/01 12:00 AM

Deleted: 4

1/1/01 12:00 AM

Deleted: ... [4]

1/1/01 12:00 AM

Formatted: File Stamp

1/1/01 12:00 AM

Formatted: File Stamp Character

3.1 Basic Overview of Cybersecurity Practices

The following examples present several options for using the Framework. Organizations should have at least basic capabilities implemented in each of these areas, and can begin to review what particular categories and subcategories they currently use to help achieve those outcomes.

While it does not replace a risk management process, these Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including “How are we doing?” Then, they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization’s desired cybersecurity outcomes.

Step 5: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to perform targeted improvements.

Step 6: Implement Action Plan. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies Informative References regarding the practices described in the Categories and Subcategories. Appendix B, the Privacy Methodology, provides guidance on privacy and civil liberties considerations for the selected Categories and Subcategories.