Implementing the NIST Cybersecurity Framework

James Read

College of Cybersecurity
Old Dominion University
jread001@odu.edu

11/30/2021

The Need for a Cybersecurity Framework

In today's constantly escalating threat landscape companies of all shapes and sizes are under pressure to improve their cybersecurity postures. An information security governance paradigm that does not respond and adapt to these changing conditions is in the process of becoming obsolete. However, in a such a complex and technical field this is easier said than done.

Effective risk management now requires a re-examination of organizational structure with a focus on integrating information security into all activities of an enterprise. Cybersecurity risk now exists at nearly every level and sector of an organization. It brings new company-wide policies with a need for continuous monitoring and change. It necessitates conversing across many different disciplines at many different levels, requiring a wide variety of stakeholders to comprehend and communicate about security. It also needs clearly defined roles and responsibilities, making sure that there are individuals tasked with security as their primary duty while also making information security a responsibility of every employee. Without a guiding structure the task of identifying risks, implementing policies, and communicating between stakeholders quickly becomes overwhelmed in a sea of information and choices. From these challenges the need for a common cybersecurity framework has emerged.

Historically, companies and agencies have developed their information security programs independently. This resulted in wildly varying effectiveness and made comprehensive programs feasible only for larger organizations. The problem of cybersecurity has become too complicated with too many assets, threats, and stakeholders for this approach to be sustainable. Infrastructure is too complex, resources too limited, or technical skill too low. **C**ybersecurity frameworks make it possible to eat the elephant. A well designed framework will help you identify risks, communicate effectively, and put in place measures to detect, respond, and recover from a cybersecurity event.

The NIST Cybersecurity Framework

One such framework is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF).

The NIST CSF is a cybersecurity risk management tool designed to provide a common structure for approaching cybersecurity. It is the product of an ongoing collaborative effort involving industry, academia, and government. It draws on established standards, guidelines, and practices. It is also flexible, cost effective, and technology neutral.

The CSF is crafted to enable any organization regardless of size or sophistication to establish a cybersecurity program. It allows organizations to utilize its components piecemeal, choosing what controls fit their business needs. In this way each organization can adapt the framework to their unique threat model. It also establishes a common language for communicating security goals. This removes a major barrier, making it possible for engineers, management, and other stakeholders to have a shared understanding. Additionally, as a non-regulatory standard it is voluntary and free of charge, allowing organizations to adopt at their own pace and without fear of penalties.

It is this combination of flexibility and commonality that makes the NIST CSF an ideal choice for cybersecurity risk management.

How does it work?

The NIST CSF is composed of three parts; the *Framework Core*, *Implementation Tiers*, and *Framework Profiles*. When taken together they can be used to:

- Assess the current cybersecurity status of your organization or business
- Build a comprehensive security program
- Measure maturity and conduct industry comparisons
- Simplify communications with business leaders

Each part is examined in detail below.

Framework Core

The Framework Core outlines a continuous life-cycle for cybersecurity risk management. At the top level it is organized into five key functions representing the five key steps of the life-cycle; *Identify*, *Protect*, *Detect*, *Respond*, *Recover*. Each of these functions are divided into categories, subcategories, and informative references. Categories break down a function into broad goals common to that life-cycle step such as "Asset Management" or "Access Control". Subcategories further divide categories into specific, actionable outcomes such as "Data-at-rest is protected" and "Notifications from detection systems are investigated". Informative references then link given subcategories to existing standards, guidelines, and practices that describe methods for achieving the desired outcome.

To understand this risk management life-cycle and how to implement the NIST CSF a more detailed examination of the five functions of the Framework Core and their purposes is necessary. The goals of each step can be summarized as follows: [2]

Identify
Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities. [1]

- Inventory assets and critical processes
  - Identify critical activities and data.
- Document information flows
  - Know where your data is stored and how it is accessed.
- Identify threats and vulnerabilities
  - Understand risk exposure and identify mitigation priorities.
- Establish security policies
  - Use the knowledge gained from identification to set security expectations
  - Clearly establish roles and responsibilities

Protect
Develop and implement the appropriate safeguards to ensure delivery of services. [1]

- Establish access control
  - Assign use accounts
  - Set permissions
  - Enable Authentication, Authorization, and Accounting

- Secure data
  - Encrypt data at rest and in motion
  - Use integrity checking
  - Create backups.
  - Destroy data that is no longer needed.
  - Know applicable data privacy laws.
- Secure devices
  - Install host based protections such as software firewalls.
  - Use standardized configurations across devices.
  - Disable unnecessary features
  - Dispose of unneeded devices securely
- Train users
  - ensure that they are aware of security policies
  - ensure they are aware of their roles and responsibilities

Detect
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. [1]

- Know expected data flows
  - Establish a baseline for where user activity, data storage, and access.
  - Monitor for activity outside of this baseline.
- Maintain and monitor logs
  - Implement event notification systems
  - Aggregate logs
  - Monitor for anomalies from expected network behavior
- Understand the impact of cybersecurity events
  - Use monitoring to quickly identify the breadth and depth of the event
- Test detection controls
  - Regularly test your ability to identify inappropriate activity
  - Identify gaps and update detection processes

Respond
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.[1]

- Develop a response plan
- Analyze events
  - Use logs and event notifications to quickly understand the breadth and depth of the event.
- Contain impact
  - Use security controls to prevent further escalation.
  - Take appropriate steps to mitigate or eliminate the event.
- Coordinate with stakeholders
  - Ensure appropriate stakeholders are kept informed on incident
  - Ensure only appropriate information is shared
- Test and update response plan
  - Regularly test your ability to respond to inappropriate activity

- Identify gaps and update detection processes

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 cyber-security event. [1]

- Develop a recovery plan
  - Identify recovery priorities and activities prior to security event.
  - Execute recovery plan when response stage is complete.
- Communicate with stakeholders
  - Inform appropriate stakeholders on incident response and recovery.
  - Ensure only appropriate information is shared
- Test and update recovery plan.
  - Regularly test your recovery plans
  - Identify gaps and update detection processes

Implementation Tiers

Implementation Tiers describe an organization's approach to managing risk. There are four tiers representing a spectrum of increasing sophistication from reactive to proactive. Each tier is described in terms of the organizational risk management process, integrated risk management program, and external participation. Tiers level are not meant to represent maturity and organizations are intended to choose a desired tier to reach based on their business needs.

A brief summary of the Implementation Tiers shows: [1]

Tier 1: Partial
- *Risk management process*
  - No formal risk management practices
- *Integrated Risk Management Program*
  - Little to no risk awareness, management, and information sharing.
- *External Participation*
  - Little to no external collaboration and awareness.

Tier 2: Risk Informed
- *Risk management process*
  - Management approves risk management practices but has no organizational policy.
- *Integrated Risk Management Program*
  - Awareness of cybersecurity risk at the organizational level, but no organization-wide approach to managing cybersecurity
- *External Participation*
  - Organization understands its role in the larger ecosystem, collaborates, and understands its supply-chain risks.

Tier 3: Repeatable
- *Risk management process*
  - Risk management practices are formally approved and expressed as policy

- *Integrated Risk Management Program*
  - There is an organization-wide approach to managing cybersecurity risk
- *External Participation*
  - Organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks

Tier 4: Adaptive

- *Risk management process*
  - Risk management practices are adapted based on previous and current cybersecurity activities.
- *Integrated Risk Management Program*
  - Cybersecurity risk management is part of the organizational culture and evolves from a awareness of activities past an present.
- *External Participation*
  - Organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks

The NIST CSF provides no guidance regarding how to measure these attributes or methods to determine the applicable Tier. The Tiers are subjective, serving simply to help an organization consider current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. [6] Making the correct choice is a complicated and difficult task, guidance from experts or standardization institutes is recommended. [5]

Framework Profiles

Framework Profiles are an inventory of current or desired controls as mapped to the categories and subcategories of the Framework Core. It helps an organization catalog its cybersecurity activities and align them with its business needs and available resources. Profiles can also be used to help match legal and regulatory requirements or implement industry best practices.

Profiles are particularly useful as tools for developing an action plan for reducing cybersecurity risk. This begins by identifying the current state and target state of of an organization's security controls. These are described as the *Current Profile* and the *Target profile*. The *Current Profile* is exactly that, an inventory of the organization's currently active controls as mapped to subcategories the Framework Core. The *Target Profile* is similarly created by mapping the organization's security goals to the subcategories of the Framework Core. The two profiles can then be compared to reveal gaps in an organization's security posture. Addressing these gaps can then be prioritized based on business needs so that an efficient, cost effective action plan can be formed.

Implementation

With a proper understanding of the NIST CSF structure we can now consider how to implement this framework. In short, a company identifies its mission, assesses the risks to that mission, targets desired security outcomes, prioritizes those outcomes, and enacts those priorities.

When considering implementing the NIST CSF it is important to keep in mind that the Framework is descriptive rather than prescriptive. It can help your organization understand and communicate its goal

but it does not tell you how to achieve those goals. It does provide references to common standards and practices for individual goals and synergizes well with other Framework documents such as the NIST Risk Management Framework and NIST SP 800-100 [1][3][12].

The NIST CSF outlines 7 steps for establishing or improving a cybersecurity program:

Step 1: Prioritize and Scope.

- Assess business needs/objectives.
  - Identify the organizational mission.
  - Identify the organizational structures and activities necessary to achieve that mission.
  - Identify the high level systems and assets that support those parts or processes.
  - Identify rIsk tolerances by selecting the desired Implementation Tier
  - Define roles and responsibilities

Step 2: Orient.

- Develop an understanding of the systems and processes that supports the business needs.
  - Inventory systems and assets covered by the chosen scope
    - Assets are not limited to IT and may include things such as facilities or essential personnel. [6]
  - Identify threats and vulnerabilities affecting those systems and assets.
  - Identify any regulatory requirements.

Step 3: Create a Current Profile.

- Know the current security controls and how they map to the Framework Core.
  - Map controls to appropriate subcategories of the Framework Core.
    - It may be helpful to first map existing security controls to the NIST controls catalog [4][10]
- Of the identified subcategories, indicate which are currently being achieved.
  - It may be helpful to indicate coverage for a as subcategory as green (goals fully achieved), yellow (goals partially achieved), or red (goals not achieved). [4]
  - Noting if an outcome is partially achieved will assist in analyzing gaps.

Step 4: Conduct a Risk Assessment.

- Analyze the likelihood and potential impact of known threats in the operational environment
  - Instructions for conducting a risk assessment are beyond the scope of this report but assistance can be found in the NIST Guide for Conducting Risk Assessments [12]

Step 5: Create a Target Profile.

- Identify the desired security posture by mapping desired outcomes to the appropriate subcategories to establish a Target Profile.
  - The end result result should be a comprehensive listing of the subcategories deemed necessary to achieve the organization's security goals.
  - The resulting profile should reflect the target Implementation Tier.
- Additional Categories and Subcategories may be created to account for unique organizational risks. [1]

Step 6: Determine, Analyze, and Prioritize Gaps.

- Compare the Current Profile and the Target Profile to determine the gaps
  - For each of the subcategories in the Target Profile, compare the target level of achievement with the level identified in the Current Profile. [6]
- Analyze the organizational resources needed to fix the identified gaps
  - The Informative References for a given subcategory can provide guidance on necessary actions.
- Create a prioritized action plan to address the identified gaps
  - Prioritization should weigh cost and benefit against potential impact.
  - Business needs, resources, and risk tolerance should all be considered.

Step 7: Implement Action Plan.

- Implement necessary controls to address the prioritized gaps.
  - Gradual implementation can be used to test the validity of the chosen approach.
- Establish Metrics to measure the success of the CSF implementation.

Other Uses

In addition to establishing or improving a cybersecurity program the NIST CSF identifies the following Framework uses:

1. Basic Review of Cybersecurity Practices
2. Communicating Cybersecurity Requirements with Stakeholders
3. Buying Decisions
4. Identifying Opportunities for New or Revised Informative References
5. Methodology to Protect Privacy and Civil Liberties

For more information on these uses see the NIST CSF document. [1]

Implementation Challenges

As with any organizational change, implementing the NIST CSF comes with significant challenges. A survey of industry professionals regarding the factors limiting implementation of the CSF was conducted at Colorado Technical University in 2020 and identified 3 key issues; *Complexity*, *lack of skillsets/staff*, and *cost*. [8]

While the NIST CSF strives to be comprehensive many participants found it too *complex*. A majority 59% of participants reported this issue. [8] They voiced a desire for a more prescriptive format, finding it too difficult to bridge the gap between the CSF's descriptive approach and the procedures to implement it. Too much was left to the participants to determine, giving them a workload that exceeded their abilities. Many felt that the framework was not well suited for smaller to medium size businesses. The perceived complexity also was a barrier to understanding for senior management.

If experiencing this issue consider that supporting documents are available. NIST provides many documents some of which address more prescriptive concerns. Outside help is another option, there are many resources in the cybersecurity community available. To make it easier to translate the framework for executives consider adding categories or subcategories to the Framework Core for other business needs to help frame risk management goals in the larger context of the organization as a whole.

Lack of skillsets/staff was the second most reported issue with 41% of participants reporting difficulty. [8] There is a well know shortfall of cybersecurity professionals. Often, even when businesses

have a handle on the framework complexity they simply can't find the personnel to fill the necessary roles. This shortage also makes it hard to keep skilled employees, with many being poached by other organizations with offers of higher salaries. What personnel they do have are then stretched thin, often filling multiple roles . This means means any one role may not be getting the focus it needs and leads to burnout. Lastly, senior management often struggles to understand and implement the framework due to lack of cybersecurity knowledge.

In the low availability, high demand market for cybersecurity professionals this is a difficult challenge to mitigate. A organization should lean on providing competitive benefits to keep existing personnel. Internal cybersecurity training should be a focus if possible, upskilling existing security personnel and providing baselines knowledge for entry level hires. Matching experienced professionals with entry level employees can also help accelerate expansion of an organization's skill pool. For executives, some cybersecurity knowledge is simply a must these days; similar training initiatives should be considered.

Cost was another highly reported issue in the study. 37% of participants identified this as a limiting factor. [8] Managing the budget is a major challenge. Businesses have many competing priorities for the budget and cybersecurity is often seen as an additional expenditure. It can be hard to convince management that the requested funding is necessary. When management is on board it may still be difficult to understand what allowances are needed to properly offset risks and the CSF does little to address this. Even when a budget is established unexpected costs can appear.

As far as understanding costs goes, documents such as the NIST Risk Management Framework can provide prescriptive methods on calculating costs. It can also help with evaluating them against potential risks. Actually reducing costs is more difficult. The scalable nature the the CSF may be of some use here. An organization should take care to choose an Implementation Tier that is within their means and create a Target profile what has budgetary restrictions in mind. The CSF can help an organization scale its security operations to a budget but can't reduce the cost of controls themselves.

Leadership and Management Approaches

Successful implementation of the NIST CSF depends on effective leadership and management.

Of primary importance is that leadership be directly involved in cybersecurity governance. Risk management practices should be formally approved by senior management and established as organization-wide policy. [1] Cybersecurity should be part of the organizational culture. Cybersecurity considerations should extend beyond the IT domain. They should be a part a part of planning activities across the organization. Cybersecurity risk considerations should be given the same importance as other organizational risks. The organizational budget should reflect an understanding of the the increasing need for resources to be devoted to cyber risk management. Ultimately, management should be accountable for the organization's cybersecurity posture.

Effective communication is also of vital importance. Cybersecurity management involves many distinct sets of stakeholders each with their own priorities, vocabularies, and subcultures. Management should take advantage of the common language provided by the NIST CSF to facilitate shared understanding of objectives and responsibilities. Priorities should also be communicated with stakeholders of all levels.

Communication needs to be directed at the right people. Management should establish clear roles as responsibilities for themselves, security personnel, other employees, and other stakeholders. An emphasis

should be placed on identifying and acquiring talent for key security positions.

A policy review cycle should be established. Gaps and opportunities for improvement should be identified and updates applied accordingly. To support this, performance measures and other appropriate metrics should be assessed and implemented. The effectiveness of security policies should be continuously monitored. Lessons learned from this monitoring should inform security policy and budget decisions. [1]

Lastly, management should seek outside help. The scale and complexity of cybersecurity risk management is enormous. Today it touches nearly every aspect of an organization and involves stakeholders at every level. It is a difficult landscape to navigate even for large, well funded companies. Luckily much of the cybersecurity community collaborates to expand a shared understanding of these challenges. There are a wide variety of free and paid resources available. Any organization seeking to establish a cybersecurity program should join this community.

Conclusion

The NIST Cybersecurity Framework may seem complex at first but at its core is a simple 5 step information security life-cycle who's complexity can be adjusted to the needs of any organization. It is flexible, scalable, cost effective, and provides a common language for shareholders across multiple disciplines.

Organizational change doesn't come without challenges. For the CSF those challenges primarily revolve around complexity, personnel, and cost. These can be mitigated my making use of supporting documents, reaching out the the community, implementing training and provided competitive benefits.

To succeed, implementation requires the direct involvement of senior management and integration of cybersecurity into the organizational culture. It requires a focus on effective communication, establishing clear roles and responsibilities, review and revision, and community participation. By following the guidelines above any organization should be able to implement an information security program tailored to their unique needs.

References

1. Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.CSWP.04162018

2. Mahn, A. , Topper, D. , Quinn, S. and Marron, J. (2021), Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide. *National Institute of Standards and Technology, Special Publication (NIST SP)* https://doi.org/10.6028/NIST.SP.1271

3. Bowen, P. , Hash, J. and Wilson, M. (2006), Information Security Handbook: A Guide for Managers. *National Institute of Standards and Technology, Special Publication (NIST SP).* https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50901

4. Murphy, G. (2021). IMPLEMENTING CYBERSECURITY. *Strategic Finance, 103*(1), 62-63.

5. Udroiu, A., & Dumitrache, M. (2020). *The Frameworks For Implementing Critical Infrastructure Cybersecurity*. Bucharest: "Carol I" National Defence University.

6. Information Systems Audit and Control Association. (2014). *Implementing the NIST: Cybersecurity Framework*. ISACA. https://is.bryant.edu/files/36176381/36176467/1/1563546609000/implementing_nist_framework.pdf

7. Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. *The Journal of Supercomputing, 74*(10), 5171-5186. https://doi-org.proxy.lib.odu.edu/10.1007/s11227-018-2479-2

8. Yvon, T. (2020). *Exploring factors limiting implementation of the national institute of standards and technology cybersecurity framework* (Order No. 28028658). Available from ProQuest Dissertations & Theses Global. (2435199859).

9. U.S. Department of Homeland Security. (2015) Transportation Systems Sector Cybersecurity Framework Implementation Guidance. *Cybersecurity and Infrastructure Security Agency, website. https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf*

10. Ross, R. and Pillitteri, V. (2020), Control Baselines for Information Systems and Organizations, *National Institute of Standards and Technology (NIST SP)* https://doi.org/10.6028/NIST.SP.800-53B

11. Ross, R. (2018), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. *National Institute of Standards and Technology (NIST SP)* https://doi.org/10.6028/NIST.SP.800-37r2 (Accessed December 7, 2021)

12. Ross, R. (2012), Guide for Conducting Risk Assessments. *National Institute of Standards and Technology (NIST SP)* https://doi.org/10.6028/NIST.SP.800-30r1 (Accessed December 6, 2021)