NIST-CSP Framework

2023

“

QUALITY IS THE BEST BUSINESS PLAN

”

OVERVIEW

The smooth operation of essential infrastructure is crucial to the success of any business. Threats to critical infrastructure data security, the economy, and public safety and health are exacerbated by the rising complexity and interconnectedness of these systems. Cybersecurity risk has an impact on a company’s bottom line, just like financial and reputational threats do. Costs may rise and revenue may be impacted. It can hinder a company’s capacity to attract and retain customers and spur creative problem solving. Organizational risk management strategies that include a focus on cyber security can be powerful.

Framework Basic.

Cybersecurity risk can be better comprehended, handled, and communicated to both internal and external stakeholders with the help of the Framework. It's a method for harmonizing the ways in which policy, business, and technology deal with cybersecurity risk, and it may be used to help pinpoint and prioritize measures to take to lessen that risk. Cybersecurity risk management can be applied to the entire organization, or it can be narrowed in on the delivery of mission-critical services. The Framework can be utilized by many entities, such as sector coordinating structures, associations, and organizations, for a variety of tasks, one of which is the development of shared Profiles.

FRAMEWORK CORE

THE FRAMEWORK'S FOUNDATION, OR "CORE," OUTLINES A SERIES OF STEPS THAT MAY BE TAKEN TO IMPROVE CYBERSECURITY AND PROVIDES EXAMPLES OF HOW TO TAKE THESE STEPS. THE ESSENTIALS ARE NOT A SERIES OF TASKS TO COMPLETE. STAKEHOLDERS' OPINIONS ON THE MOST IMPORTANT CYBERSECURITY OUTCOMES FOR RISK MANAGEMENT ARE PRESENTED.

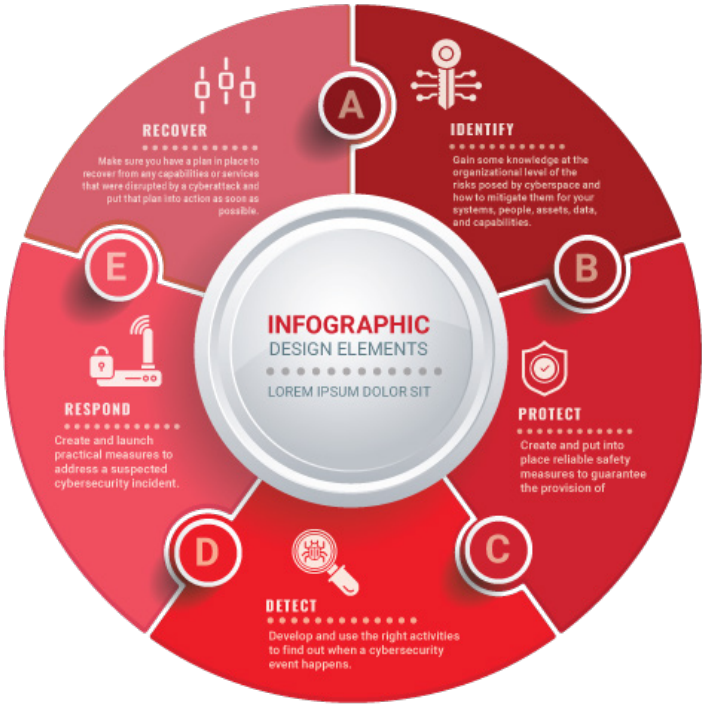
IDENTITY

Gain some knowledge at the organizational level of the risks posed by cyberspace and how to mitigate them for your systems, people, assets, data, and capabilities.

Effective utilization of the Framework relies heavily on the actions taken inside the Identify Function. A firm may better focus and prioritize its cybersecurity activities in accordance with its risk management strategy and business demands if it has a thorough understanding of the business environment, the resources that support important functions, and the relevant cybersecurity threats. Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy are all examples of result Categories that fall under this Function.

PROTECT

Create and put into place reliable safety measures to guarantee the provision of essential services. The Protect Operation helps ensure that the effects of a cyberattack may be mitigated. Identity and Access Management, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology are all examples of result Categories within this Function.



DETECT

Develop and use the right activities to find out when a cybersecurity event happens. The Detect Function makes it possible to find out about cybersecurity events in a timely manner. Some examples of outcome categories in this Function are Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

RESPOND

Create and launch practical measures to address a suspected cybersecurity incident.

The capability to mitigate the effects of a cyberattack is bolstered by the Respond Function. Response planning, communications, analysis, mitigation, and enhancements are all examples of result categories that can be found within this Function.

RECOVER

Make sure you have a plan in place to recover from any capabilities or services that were disrupted by a cyberattack and put that plan into action as soon as possible.
A swift return to normal activities is supported by the Recover Function to lessen the overall effect of a cyberattack. The Results in Various Cases Planned Recoveries, Enhanced Operations, and Enhanced Communications are all subsets of this Function.

RISK MANAGEMENT AND THE CYBERSECURITY FRAMEWORK

Risk management involves recognizing, assessing, and addressing risks. Organizations should understand event likelihood and potential implications to manage risk. This information helps organizations estimate their risk tolerance for attaining their goals.

Risk tolerance helps firms prioritize cybersecurity efforts and make informed cybersecurity spending decisions. Risk management systems help firms measure and explain cybersecurity program changes. Depending on the impact on key services, organizations may mitigate, transfer, avoid, or accept risk. Risk management helps firms prioritize cybersecurity decisions using the Framework. It provides recurrent risk assessments and business driver validation to help enterprises choose cybersecurity target states that match desired outcomes. Thus, the Framework lets enterprises dynamically pick and optimize IT and ICS cybersecurity risk management.
The Framework is adaptable to support a variety of cybersecurity risk management methods. ISO cybersecurity risk management processes (ISO)

HOW TO IMPLEMENT FRAMEWORK

The Framework Implementation Tiers (“Tiers”) explain how a company understands cybersecurity risk and manages it. Tiers define cybersecurity risk management approaches from Partial to Adaptive. They determine how much a company needs and risk management methods inform cybersecurity risk management. Cybersecurity risk management includes privacy and civil liberties considerations.

Current risk management methods, threat environment, legal and regulatory requirements, information sharing policies, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints are considered during Tier selection. Organizations should choose a Tier that fulfills their goals, is realistic to deploy, and reduces cybersecurity risk to vital assets and resources. Organizations should use external guidance from Federal government departments and agencies, ISACs, ISAOs, maturity models, or other sources to determine their intended tier.

Tiers don’t indicate maturity; however, Tier 1 (Partial) firms are urged to move up. Tiers help organizations decide how to manage cybersecurity risk and which areas need more resources. A cost-benefit analysis showing a possible and cost-effective cybersecurity risk reduction encourages Tier advancement.

The Framework’s success depends on the organization’s Target Profile(s) rather than Tier. Tier selection and designation inherently impact Framework Profiles. Business/Process Level managers’ Tier suggestion, accepted by the Senior Executive Level, will define the organization’s cybersecurity risk management tone, and affect Target Profile prioritization and gap assessments.

TIER 1: PARTIAL

- Organizational cybersecurity risk management methods are not codified, and risk is often managed on an ad hoc, even reactive basis. It's possible that risk objectives, the state of the threat landscape, and business/mission needs aren't used as a direct basis for prioritizing cybersecurity operations.
- Cybersecurity risk is not widely understood within organizations, despite the prevalence of risk management programs. Cybersecurity risk management is implemented on an ad hoc, case-by-case basis due to the organization's limited knowledge and the wide variety of external information sources. It's possible that the company lacks mechanisms to facilitate the internal sharing of cybersecurity data.
- Participation from the Outside World - The Company is Confused About Its Dependencies and Dependencies in the Ecosystem The company does not work with, receive information from, or exchange information with any outside parties (including customers, suppliers, dependencies, dependents, ISAOs, researchers, or governments) in any way, shape, or form. The company does not fully understand the cyber supply chain risks associated with the goods and services it sells and uses.

TIER 2: RISK INFORMED

- **Risk Management** - Management has sanctioned certain risk management procedures, although they may not have been formalized as policy. Organizational risk objectives, the threat landscape, or business/mission requirements directly impact the prioritization of cybersecurity operations and protection needs.
- **External and Integrated risk management** - Cybersecurity risk is recognized at the corporate level, but no unified strategy for mitigating this threat has been implemented. Within the company, cyber security knowledge is exchanged on a more casual basis. Cybersecurity may be factored into company goals and initiatives at some but not all levels. Organizational and external assets are assessed for cyber risk, but this is not a routine or recurring process.

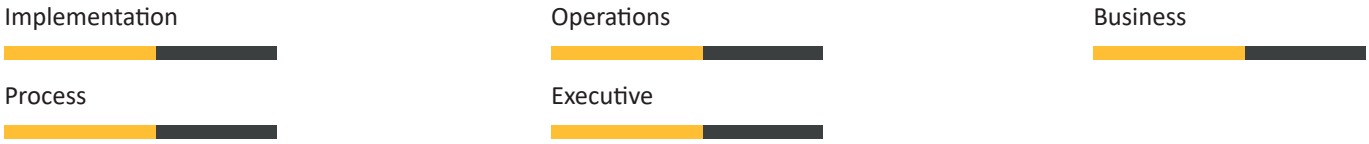
  Typically, the company has a firm grasp on its position in the ecosystem regarding its own dependencies or dependents, but not both. The company works with outside parties, gathers data from those partnerships and its own efforts, and produces some data as well, but it is not required to disclose any of this data to the public. The company is also conscious of the cyber supply chain risks related to the goods and services it offers and utilizes, although it does not always or properly address these concerns.

TIER 3: REPEATABLE AND ADAPTIVE

- The organization's approach to risk management is codified in written policy. Applying risk management methods to evolving business/mission requirements and the security threat/technology landscape results in continual updates to an organization's cybersecurity practices .
- The group is aware of how it fits into the ecosystem as a whole, how it is dependent on other groups, and how it may help broaden their understanding of hazards. As the threat and technological environments shift, it receives, generates, and reviews prioritized information to inform ongoing analysis of its risks. The company disseminates the data both within and beyond its walls to its network of partners. Cyber supply chain risks linked with the products and services provided and used by the company are understood and systematically addressed through the use of real-time or near real-time information. In addition, it uses both formal (such as agreements) and informal means of communication to build and sustain cooperative ties throughout the supply chain.

FRAMEWORK IN ACTION

The 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 the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact. Common flow of information and decisions at the following within an organization.



How to use the framework effectively

The Framework can help a company identify, assess, and manage cybersecurity risk. An organization can overlay its current process on the Framework to identify cybersecurity risk approach gaps and build a roadmap to change. As a cybersecurity risk management tool, the Framework helps a business identify vital service delivery operations and prioritize spending to maximize ROI.

The Framework supplements business and cybersecurity activities. It can start or improve a cybersecurity program. The Framework helps business partners and customers communicate cybersecurity requirements and detect cybersecurity weaknesses. It also outlines general privacy and civil liberties considerations for cybersecurity programs.

The Framework applies to plan, design, build/buy, deploy, operate, and decommission. Any system starts with a plan. Declare and explain broad cybersecurity concerns. The strategy should acknowledge that such concerns and requirements may change during the life cycle. Cybersecurity should be included during the design phase of multi-disciplinary systems engineering. 10 Validating that system cybersecurity parameters fit the organization's Framework Profile needs and risk disposition is an important design milestone. A Target Profile should be used to prioritize cybersecurity results when building and buying a system. The Target Profile should be used to check system cybersecurity aspects while installing the system. The Framework's cybersecurity results should guide system operation. A Current Profile is used to periodically examine cybersecurity requirements. Decommissioning systems require careful consideration of Target Profile outcomes because to a complex web of relationships (e.g., compensatory, and shared controls).

Step -1: Review and revisit cybersecurity Exercise.

An organization's cybersecurity operations can be compared to the Framework Core using the Framework. Using a Current Profile, companies may assess their performance in the Core Categories and Subcategories, matched with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may manage cybersecurity appropriately with the known risk if it is currently accomplishing the desired results. Alternatively, a company may decide to improve. The company can utilize such data to create a cybersecurity action plan. To accomplish results, a company may overinvest. This data can help the company reprioritize.

While they do not replace a risk management process, these five high-level Functions will help senior executives and others distill the fundamental concepts of cybersecurity risk so they can assess how identified risks are managed and how their organization compares to existing cybersecurity standards, guidelines, and practices. "How are we doing?" can be answered by the Framework. Then they may make more educated decisions to improve their cybersecurity policies.

Step 2: Cybersecurity Program Development/Improvement

Here we show how a company could utilize the Framework to develop a brand new cybersecurity strategy or enhance an existing one. For the sake of maintaining a high level of cybersecurity, these procedures should be repeated as often as is necessary.

2.1: Prioritize and Scope - Organizational goals, mission statements, and other such lofty statements are laid out. This data is used to guide the company's strategic decisions on cybersecurity measures and to outline the full scope of the systems and assets that serve the chosen business line or activity. The Framework can be tailored to meet the demands of individual departments or processes within an organization, each of which may have unique requirements and levels of comfort with risk. A desired Implementation Tier can be reflective of one's comfort level with risk.

2.2: Orient - The organization then defines the systems and assets, regulatory requirements, and overall risk approach that pertain to the business line or process that will be covered by the cybersecurity program. The company then looks to other sources to determine what kinds of dangers and weaknesses those systems and assets face.

2.3: Get Your Profile Up to Date - By detailing the Framework Core Category and Subcategory results that have been achieved up to this point, the organization creates a Current Profile. Noting the extent to which an outcome has been accomplished is useful for future planning because it establishes a point of reference.

2.4: Perform a Threat Analysis - The organization's overall risk management procedure or results from earlier risk assessments may serve as pointers for this evaluation. Foreseeing the potential for a cyber-attack and its potential consequences, the company examines its operational environment. In order to better comprehend the possibility and effect of cybersecurity incidents, it is crucial that businesses recognize emerging risks and leverage cyber threat information from internal and external sources.

2.5: Create a Target Profile: A Target Profile is developed to evaluate the Framework Categories and Subcategories that characterize the anticipated cybersecurity results for the organization. Further Categories and Subcategories may be created by organizations to account for their own special hazards. When developing a Target Profile, the firm may also consider the opinions and needs of external stakeholders including industry organizations, customers, and strategic alliance partners. All relevant criteria from the intended Implementation Level should be reflected in the Target Profile.

2.6: Determine, Analyze, and Prioritize Gaps. The organization looks at the differences between the Current Profile and the Target Profile to find out where there are problems. Then, based on the mission drivers, costs, benefits, and risks, a prioritized action plan to close the gaps is developed in order to finally reach the objectives outlined in the Target Profile. The organization next figures out what kind of financial and human assets are needed to fill the voids. As a result of using Profiles in this way, businesses are more likely to engage in risk-informed decision-making regarding their cybersecurity activities; risk management is bolstered; and the business is able to implement efficient, targeted enhancements with less cost.

2.7: Have a plan and put it into action - The company evaluates its present cybersecurity policies and decides what steps to take in order to close any gaps discovered in the previous stage. Although the Framework provides some examples Informative References for each of the Categories and Subcategories, it is ultimately up to each individual business to select which standards, rules, and practices, including industry-specific ones, are most applicable to their circumstances.

The process of assessing and bettering a company's cybersecurity is repeated as often as is necessary. Increasing the frequency with which businesses do the orient step may, for instance, lead to more accurate risk evaluations. Further, businesses can track development by regularly updating the Current Profile and comparing it to the Target Profile. This method can also be used to bring an organization's cybersecurity program into compliance with the tier of the Framework they wish to use.

HOW TO TALK TO YOUR STAKEHOLDERS ABOUT CYBERSECURITY NEEDS

The Framework establishes a standard vocabulary for the coordination of needs across the many parties involved in critical infrastructure product and service delivery. To cite a few instances:

01 A Target Profile is a document that can be used by a company to communicate with a third-party service provider about the necessities of cyber risk management on the company's part (e.g., a cloud provider to which it is exporting data).

02 With a Current Profile, a company can report on its cybersecurity performance or evaluate its readiness for an acquisition.

03 To communicate necessary Categories and Subcategories to a previously specified external partner, a critical infrastructure owner/operator may use a Target Profile.

04 It is possible for a critical infrastructure sector to construct a Target Profile that may be used by its constituents as a starting point from which their own individualized Target Profiles can be developed.

Using Implementation Tiers, a company can determine its place in the key infrastructure and the broader digital economy, allowing it to effectively manage cybersecurity risk among its stakeholders

It is crucial for all parties involved in a supply chain to communicate both up and down the chain. Complex, internationally dispersed, and intricately linked, supply chains involve a wide range of entities and activities working together. Products and services are first sourced, then designed, developed, manufactured, processed, handled, and finally delivered to the customer, all within the scope of a supply chain. Due to the interdependencies and complexity of the supply chain, SCRM is an essential business process. Cyber SCRM refers to the processes required to deal with third-party cyber threats. Cyber SCRM especially tackles the impact of external parties' cybersecurity measures on an organization as well as the business's own impact on those measures. encompass the cybersecurity ecosystem of a company. These connections underline the significance of cyber SCRM in mitigating the threat of cyberattacks to vital sectors of the economy. Organizational protective and detective skills, as well as response and recovery methods, should take into account these connections, the goods and services they supply, and the threats they pose.

Cybersecurity Risk Evaluation for Yourself Using the Framework

The Cybersecurity Framework's main goal is to make the management of cybersecurity risk less of a threat to the organization's overall goals. In an ideal world, businesses employing the Framework would be able to quantify their risk and the associated cost and benefit of implementing measures to bring it down to an acceptable level. An organization's cybersecurity strategy and investments will be more reasonable, efficient, and worthwhile the better it is able to analyze the risk, costs, and advantages of cybersecurity strategies and steps.

Decisions regarding where to put money should be improved with time thanks to self-evaluation and measurement. A company can better comprehend and communicate risk information to its dependents, suppliers, purchasers, and other parties if it measures, or at least robustly characterizes, components of its cybersecurity posture and trends across time. This can be done either in-house or by consulting an outside source. When used correctly and with an understanding of their limitations, these metrics can form the cornerstone of reliable relationships within and outside a company.

In order to evaluate the value of investments, a company must first have a firm grasp on its own objectives, the connection between those objectives and supplementary cybersecurity results, and the means by which those individual cybersecurity outcomes are implemented and controlled. Although it is outside the scope of the Framework to measure all of these things, the cybersecurity outcomes of the Framework Core do support self-assessment of investment effectiveness and cybersecurity actions.

• Target Implementation Tiers are determined after deliberation about how various aspects of the cybersecurity operation should be handled.

• Determining Current Implementation Tiers, a business may assess its current level of cyber risk management.

• Prioritizing cybersecurity outcomes by developing Target Profiles

• Evaluating Current Profiles to find out how well various cybersecurity measures work to reach set goals, and

• Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References

Metrics for measuring cybersecurity effectiveness are still in development. Organizations should exercise forethought, creativity, and caution when employing metrics for the purpose of optimizing utilization and should steer clear of relying on artificial indicators of the state of cybersecurity or the progress made in reducing risk. Cyber risk assessment calls for discipline and periodic review. Organizations are encouraged to clearly identify and know why these metrics are significant and how they will help the overall management of cybersecurity risk whenever they use measurements as part of the Framework process. Additionally, they need to be forthright about the caveats of the measurements they employ

Summary:

A Framework Target Profile can be used to guide product and service purchases by providing a prioritized list of an organization's cybersecurity needs. As discussed in Section 3.3, Communicating Cybersecurity Requirements with Stakeholders, it may not be viable to enforce a set of cybersecurity requirements on the supplier in this transaction. Given a detailed list of cybersecurity needs, the goal should be to select the best vendor from among several possible candidates. There will likely be some sacrifices made as you weigh the pros and cons of several options, each of which falls short of perfectly fitting the Target Profile.

The Profile can be used after a purchase has been made to monitor and manage any lingering cybersecurity risk. For instance, if the acquired service or product fell short of meeting all the criteria outlined in the Target Profile, the company can take further precautions to mitigate the remaining risk. The Profile also gives the company a way to test and review the product on a regular basis to see if it's up to par with cybersecurity goals.