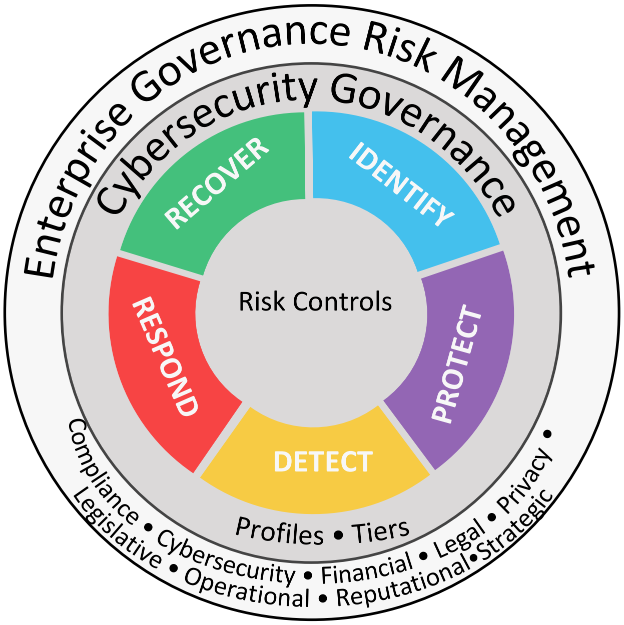
Thank you for inviting me to the NIST CSF 2.0 In person working session on 2/22/2023. I attended the governance and profile sessions.

Governance Feedback

I think that it is correct to make governance a function as it cuts across all the other functions. I particularly liked the concept where governance is the circle around the other functions, my version is below.


Enterprise Governance Risk Management
Cybersecurity Governance
RECOVER
IDENTIFY
Risk Controls
RESPOND
PROTECT
DETECT
Profiles • Tiers
Compliance • Cybersecurity • Financial • Legal • Privacy •
Legislative • Operational • Reputational•Strategic

I recommend reorganizing section 1 from CSF 1.1 to emphasize the relationship of the enterprise to its cybersecurity so that risks can be identified, assessed, and mitigated; essentially moving section 1.2 up and deemphasizing the history of the CSF in favor of perspective on its organizational use. I'm not sure what this would look like in NIST speak, but to better explain what I'm thinking, below is a partial rewrite of section CSF's sections 1, 2, and 4 (some of section 3 could also be moved up) to emphasize governance. I have liberally copied from CSF 1.1, without attribution.

At the in-person session one of your questions was what categories and sub-categories of version 1.1 would be changed by creating the new governance function. I'm focused on language. Where a current category or sub-category or their informative references relates an activity that links enterprise activity by policy, that functionality should probably be moved to the governance function. I'm making up a new GV function and creating categories to help pull out governance from the existing categories.

These fictional GV categories helped me to figure out, by the controls in each existing category, if the category should move, stay, or be partially moved to the new governance function. As most of the affected changes will be in Identify, I've gone through each identify category, sub-category, and 800-53r5 control to describe how I envision the new ID and GV functions would be in CSF 2.0. Similar exercises can be carried out for the remaining functions, but I'm hoping that this is more than enough feedback on what approach I would take at this point.

Function	Category	Sub-category
Governance (GV)	GV.PO Enterprise strategy is stated in policies	GV.PO-1: Business Alignment
		GV.PO-2: Regulatory Alignment
	GV.PL Enterprise governance planning	GV.PL-1: Risk Management Plans
	GV.CO Feedback mechanism to update policies and plans	GV.CO-1: Feedback to Improve Governance.
	GV.OR Enterprise organization	GV.OR-1: Organization Risk Responsibility Structure

Table 1. My Fictional New GV Function.

- Asset Management (**ID.AM**): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
    - **ID.AM-5**: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
        - **CP-2** Contingency plan: move to governance planning (GV.PL), should also have a new control, define contingency plan policy in governance policy (GV.PO) and a governance control feedback category (GV.CO, is the policy working?).
        - **RA-2** Security Categorization: leave the inventory part in ID, but the adverse impact portion should be reflected in governance.
        - **RA-9** Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle]. Need a new policy control to link governance to determine "criticality" to the business. This is different from the "criticality" of the technology to functionality (for example, a router firewall may be critical to the network working, but the network working is critical to the business working).
        - **SA-20** Customized Development of Critical Components leave in ID.
        - **SC-6** Resource Availability leave in ID.
    - **ID.AM-6**: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
        - **CP-2** Contingency plan: move to governance planning (GV.PL), should also have a new control, define contingency plan policy in governance policy (GV.PO) and governance control feedback (GV.CO, is the policy working?).
        - **PM-2** Information Security Leadership Role: move to governance organization (GO.OR).
        - **PM-29** Risk Management Program Leadership Roles: move to governance organization (GO.OR).
        - **PS-7** External Personnel Security: move to governance organization (GO.OR).
- Business Environment (**ID.BE**): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
    - **ID.BE-1**: The organization's role in the supply chain is identified and communicated.
        - **SR-1** Policy and Procedures fits in GV:PL and GV:PO.

        - **SR-3** Supply Chain Controls and Processes can stay in ID or move to GV.ID.
    - **ID.BE-2**: The organization’s place in critical infrastructure and its industry sector is identified and communicated.
        - **PM-8** Critical Infrastructure Plan, move to GV.PL, may have to add a policy on how to identify critical infrastructure.
    - **ID.BE-3**: Priorities for organizational mission, objectives, and activities are established and communicated.
        - **PM-11** Mission and Business Process Definition move to GV.PO, PM-11c move to GV.CO.
    - **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established.
        - **CP-2**, **PM-8**, **RA-9**, **SA-20** same as above
        - **CP-8, PE-9, PE-11,** leave in ID.BE
        - **SR-2** Supply Chain Risk Management Plan move to GV.PL
    - **ID.BE-5**: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).
        - **CP-2**, **RA-9**, **SA-20** same as above
        - **CP-11** Alternate Communications Protocols leave in ID.
        - **SA-8** Security and Privacy Engineering Principles leave in ID; however, it may be appropriate to identify a preferred provider of principles in GV.
- Governance (**ID.GV**): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. This has the potential for confusion as identifying these governance items should be in ID, but they naturally fall in the GV category. I would like to limit those in the ID to category to just identify actions. All controls that prioritize should be in the GV function.
    - **ID.GV-1**: Organizational cybersecurity policy is established and communicated
        - All security control families. Policies aligned with legal, regulatory, and contractual compliance are established using GV.PO and are controlled by GV.CO. Planning should align with policies. They may be identified in ID.GV.
    - **ID.GV-2**: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
        - **PM-1** Information Security Program Plan move to GV.PL
        - **PM-2, PM-29, PS-7** Same as above
        - **PS-9** Position Descriptions move to GV.OR
    - **ID.GV-3**: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
        - All security control families. Policies aligned with legal, regulatory, and contractual compliance are established using GV.PO and are controlled by GV.CO. Planning should align with policies. They may be identified in ID.GV.
    - **ID.GV-4**: Governance and risk management processes address cybersecurity risks.
        - PM-3 Information Security and Privacy Resources move this to GV.OR to make sure the organization has identified the need for appropriate resources. An argument may be made to leave this in ID, where those resources are identified.

- **PM-7** Enterprise Architecture move this to GV.PL. Enterprise architecture is a coordination activity to make sure the enterprise acts in as uniform manner as possible.
- **PM-9** Risk Management Strategy split this into three parts. A risk management policy that is aligned with the enterprise risk (GV.PO), who is responsible (GV.OR), and its implementation (GV.PL).
- **PM-10** Authorization Process split into two parts. Who is authorized (GV.OR) and the authorization process (GV.PL).
- **PM-11** Mission and Business Process Definition move to GV.PO to obtain enterprise impacts, GV.PL to identify the enterprise activities at risk, GV.CO for feedback. There may be some portions left in ID, where these policies and risks are identified.
- **PM-28** Risk Framing. Move organization priorities and risk tolerance to GV.PO, organization responsibility to GV.OR, feedback to GV.CO, and assumptions and constraints to GV.PL.
- **RA-1** Policy and Procedures can be divided among GV.PO, GV.PL, GV.OR, and GV.CO.
- **RA-2** Security Categorization leave in ID.
- **RA-3** Risk Assessment leave in ID who is informed is in GV.OR according to GV.PL or GV.PO.
- **SA-2** Allocation of Resources GV.OR is the source of resources as delineated in GV.PL planning that aligns with GV.PO policies. However, it would be appropriate to identify how resources are allocated in ID.

- Risk Assessment (**ID.RA**): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
  - **ID.RA-4**: Potential business impacts and likelihoods are identified. Link to GV to determine business impacts.
    - **CA-2** Control Assessments leave in ID. GV.OR may describe the roles relative to managing and responding to this information.
    - **CA-5** Plan of Action and Milestones leave in ID. GV.OR may describe the roles relative to managing and responding to this information.
    - **CA-7** Continuous Monitoring leave in ID. Governance has its own continuous monitoring in GV.CO. Reporting is defined in GV.PL and the roles may be defined in GV.OR.
    - **CA-8** Penetration Testing leave in ID.
    - **PM-4** Plan of Action and Milestones Process leave in ID.
    - **PM-15** Security and Privacy Groups and Associations leave in ID.
    - **RA-3** Risk Assessment leave in ID who is informed is in GV.OR according to GV.PL or GV.PO.
    - **RA-5** Vulnerability Monitoring and Scanning leave in ID. GV.OR may describe the roles relative to sharing this information.
    - **SA-5** System Documentation leave in ID.
    - **SA-11** Developer Testing and Evaluation leave in ID.

        - **SI-2** Flaw Remediation leave in ID.
        - **SI-4** System Monitoring leave in ID. Legal opinion should be separated out to GV. Sinc change in risk can be due to organizational change, GV should make it clear that SI-4 is affected by this type of change. Should not be focused only on external risk changes. GV.OR may include a description of this role.
        - **SI-5** Security Alerts, Advisories, and Directives leave in ID. Maybe related to GV.PL on what the security alerts are and how they are disseminated. GV.PL should also specify response time frames.
    - **ID.RA-5**: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. Again, business impacts should be linked to GV.
        - **PM-12** Insider Threat Program, ID identifies the insider threat program but perhaps it should be defined in GV.PL.
        - **PM-16** Threat Awareness Program, ID identifies the threat awareness program but perhaps it should be defined in GV.PL.
        - **RA-3** Risk Assessment leave in ID, who is informed is in GV.OR according to GV.PL or GV.PO.
        - **RA-10** Threat Hunting
        - **SI-5** Security Alerts, Advisories, and Directives
    - **ID.RA-6**: Risk responses are identified and prioritized. Link to GV to determine priorities relative to business impacts.
- Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
    - **ID.RM-1**: Risk management processes are established, managed, and agreed to by organizational stakeholders. The agreement and management falls under GV.PO. Processes fall under GV.PL. Effectiveness falls under GV.CO.
    - **ID.RM-2**: Organizational risk tolerance is determined and clearly expressed. Move to GV.PO.
    - **ID.RM-3**: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis. Move to GV.PL.
- Supply Chain Risk Management (**ID.SC**): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
    - **ID.SC-1**: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
        - **PM-30** Supply Chain Risk Management Strategy Leave in ID but GV.OR says who is responsible for this strategy and needs to update it for org changes.
        - **SA-9** External System Services leave in ID.
        - **SR-1** Policy and Procedures Move to GV.OR and GV.PL, may still be identified in ID.SC.
        - **SR-2** Supply Chain Risk Management Plan Move to GV.PL, may still be identified in ID.SC.
        - **SR-3** Supply Chain Controls and Processes leave in ID.
        - **SR-5** Acquisition Strategies, Tools, and Methods leave in ID.

- **ID.SC-2**: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.
  - **PM-9** Risk Management Strategy split this into three parts. A risk management policy that is aligned with the enterprise risk (GV.PO), who is responsible (GV.OR), and its implementation (GV.PL).
  - **RA-3** Risk Assessment leave in ID, who is informed is in GV.OR according to GV.PL or GV.PO.
  - **SA-15** Development Process, Standards, and Tools GV.PL specifies the process/standard to follow, GV.OR specifies who reviews this.
  - **SR-2** Supply Chain Risk Management Plan Move to GV.PL, may still be identified in ID.SC.
  - **SR-3** Supply Chain Controls and Processes leave in ID.
  - **SR-5** Acquisition Strategies, Tools, and Methods leave in ID—may be specified in GV.PL.
  - **SR-6** Supplier Assessments and Reviews leave in ID.
- **ID.SC-3**: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
  - **SA-4** Acquisition Process leave in ID (driven by GV but this is documenting what is done).
  - **SA-9** External System Services leave in ID. This will often generate exceptions when an organization has less power than the supplier and must accept less than the expected security or privacy controls. How to handle exceptions should be described in GV.PL.
  - **SR-2** Supply Chain Risk Management Plan Move to GV.PL, may still be identified in ID.SC.
  - **SR-3** Supply Chain Controls and Processes, leave in ID.
  - **SR-5** Acquisition Strategies, Tools, and Methods, leave in ID.
- **ID.SC-4**: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
  - **AU-6** Audit Record Review, Analysis, and Reporting, leave in ID. GV.OR should describe how the organization manages audits, GV.PL should describe how to adjust the audit when there are changes in the organization.
  - **CA-2** Control Assessments leave in ID. GV.OR should describe reporting requirements.
  - **CA-7** Continuous Monitoring leave in ID. GV.OR should describe reporting requirements.
  - **PS-7** External Personnel Security leave in ID.
  - **SA-9** External System Services leave in ID. GV.PL should describe external service requirements.
  - **SA-11** Developer Testing and Evaluation leave in ID.

- **ID.SC-5**: Response and recovery planning and testing are conducted with suppliers and third-party providers.
  - **CP-2** Contingency Plan move to governance planning (GV.PL), should also have a new control, define contingency plan policy in governance policy (GV.PO) and a governance control feedback category (GV.CO, is the policy working?).
  - **CP-4** Contingency Plan Testing leave in ID. GV.OR specifies who is responsible.
  - **IR-3** Incident Response Testing leave in ID. GV.OR specifies who is responsible.
  - **IR-4** Incident Handling leave in ID. GV.OR specifies who is responsible.
  - **IR-8** Incident Response Plan move to governance planning (GV.PL), should also have a new control, define contingency plan policy in governance policy (GV.PO) and a governance control feedback category (GV.CO, is the policy working?).
  - **IR-9** Information Spillage Response move to GV-PL. Also clarify that this control includes work ahead of any incident create playbooks to follow for different kinds of information spills.

Partial Rewrite of CSF sections 1,2, and 4 to Emphasize Governance

Contents

1. Cybersecurity Framework: A Tool for Managing Cybersecurity Risk

Organizations depend on the reliable functioning of their critical infrastructure. Cybersecurity threats exploit the dependence of technology and connectivity of critical infrastructure systems, placing governments' and enterprises' strategic goals at risk. Cybersecurity is an important and amplifying component of an organization's overall risk management.

NIST developed the Cybersecurity Framework (Framework) to be "*a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.*" Version two broadens version one's definition of "critical infrastructure" to include any system at risk.

The Framework is effective and supports technical innovation because it combines a technology neutral approach that is linked to a variety of evolving, existing standards, guidelines, and practices. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes scale from small business to global enterprises, to local governments, and to federated governments. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by risk owners. Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture.
2) Describe their target state for cybersecurity.

3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
4) Assess progress toward the target state.
5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to their strategic goals and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at optimizing the return on resources used to manage cybersecurity risks.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. Since the Framework will be customized to match the needs of each organization, discussion about "compliance" with the Framework and its specific use should be defined by the organization's governance.

While the Framework was originally developed to improve cybersecurity risk management as it relates to US critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size. The common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

1.1 Risk Management and The Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

1.1.1 Enterprise Risk and Cybersecurity Risk

Office of Management and Budget (OMB) Circular A-11 defines risk as "the effect of uncertainty on objectives" [1]. The effect of uncertainty on enterprise mission and business objectives may then be considered an "enterprise risk" that must be similarly managed. The process of managing risks at the enterprise level is known as enterprise risk management (ERM) and calls for:

- identifying and understanding the core risks facing an enterprise,

- determining how best to address those risks, and
- ensuring that the necessary actions are taken.

Today's information and technologies impact every aspect of enterprises. The scope of this Framework includes governance which links cybersecurity risks to enterprise risks.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. The implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management. The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:2009, ISO/International Electrotechnical Commission (IEC) 27005:2011, NIST Special Publication (SP) 800-39, and the Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline.

1.1.2 Coordination of Framework Implementation

Figure 1 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

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.

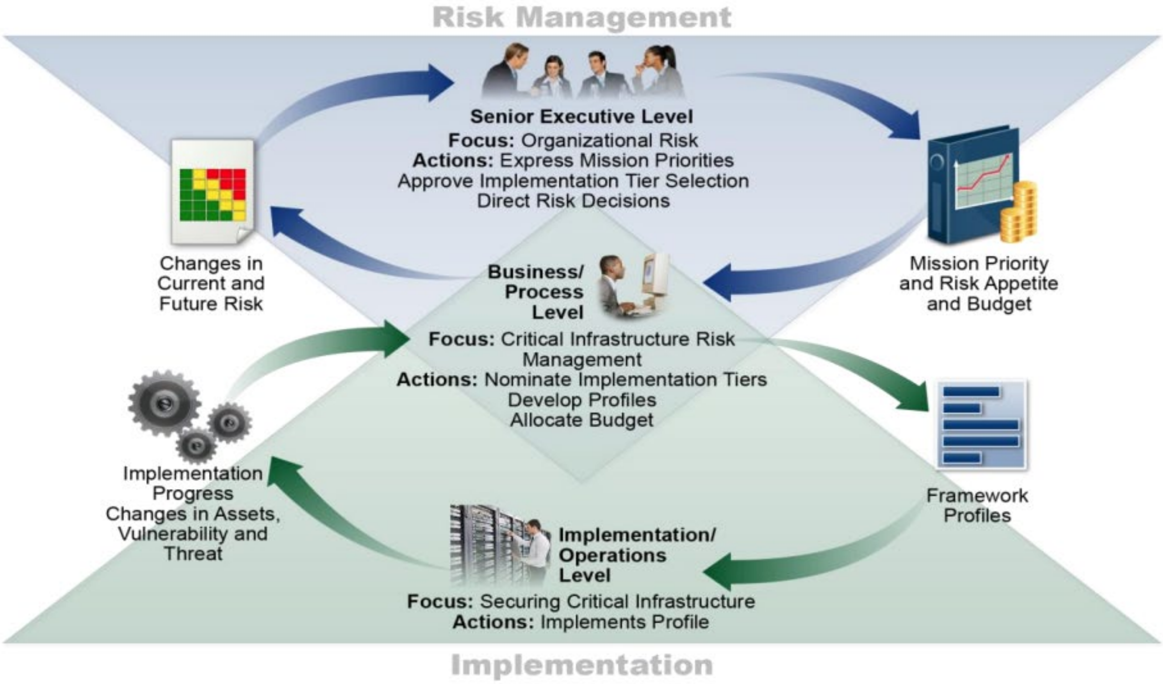

Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Figure 1: Notional Information and Decision Flows within an Organization

1.1.3 The Framework in an Enterprise's Risk Management Architecture

Organizations use governance to align business implementation with strategic goals. Governance specifies policies, how policies are created and updated, and measurement of policy compliance and policy effectiveness. Governance connects those responsible for the enterprise with the actions taken by the enterprise.

The framework can be a part of that connectivity. It provides a standard way for risk owners to describe and discuss risk. Framework profiles can describe how the enterprise risks should be controlled. The actual state of the enterprise can be assessed with the Framework and the difference between the desired state and the actual state becomes a gap to be managed. This feedback loop can even affect enterprise strategy.

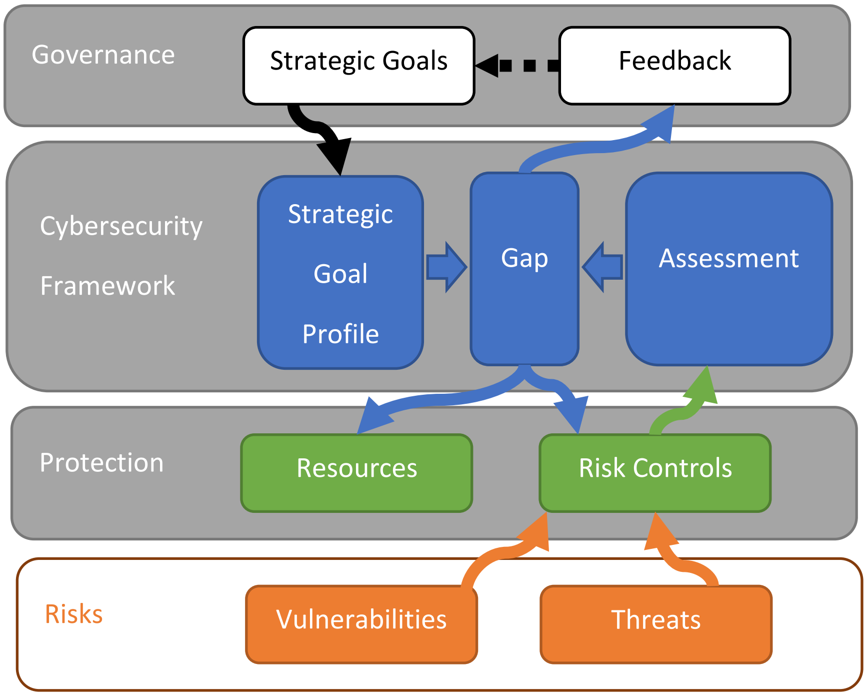


Figure 2: The Framework can connect strategic goals to risk management. The effectiveness of resource expenditure, controls, and even the enterprise's strategic goals can be evaluated relative to potential losses due to cybersecurity risks.

1.1.4 Self-Assessing Cybersecurity Risk with the Framework

The Cybersecurity Framework is designed to reduce risk by improving the management of cybersecurity risk to organizational objectives. Ideally, organizations using the Framework will be able to measure and assign values to their risk *along with* the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be.

Over time, self-assessment and measurement should improve decision making about investment priorities. For example, measuring – or at least robustly characterizing – aspects of an organization's cybersecurity state and trends over time can enable that organization to understand and convey meaningful risk information to dependents, suppliers, buyers, and other parties. An organization can accomplish this internally or by seeking a third-party assessment. If done properly and with an appreciation of limitations, these measurements can provide a basis for strong trusted relationships, both inside and outside of an organization.

To examine the effectiveness of investments, an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes, and how those discrete cybersecurity outcomes are implemented and managed. While measurements of all those items is beyond the scope of the Framework, the cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities in the following ways:

- Making choices about how different portions of the cybersecurity operation should influence the selection of Target Implementation Tiers,
- Evaluating the organization's approach to cybersecurity risk management by determining Current Implementation Tiers,
- Prioritizing cybersecurity outcomes by developing Target Profiles,
- Determining the degree to which specific cybersecurity steps achieve desired cybersecurity outcomes by assessing Current Profiles, and
- Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References.

The development of cybersecurity performance metrics is evolving. Organizations should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use, while avoiding reliance on artificial indicators of current state and progress in improving cybersecurity risk management. Judging cyber risk requires discipline and should be revisited periodically. Any time measurements are employed as part of the Framework process, organizations are encouraged to clearly identify and know why these measurements are important and how they will contribute to the overall management of cybersecurity risk. They also should be clear about the limitations of measurements that are used.

For example, tracking security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives. Verifying achievement of some organizational objectives requires analyzing the data only after that objective was to have been achieved. This type of lagging measure is more absolute. However, it is often more valuable to predict whether a cybersecurity risk *may* occur, and the impact it might have, using a leading measure.

Organizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with a full appreciation of their usefulness and limitations.

Framework Overview

…

Framework Components

…

How to Use the Framework

…

Framework History

…

Tables and Appendices

…