SIMPLI GRC

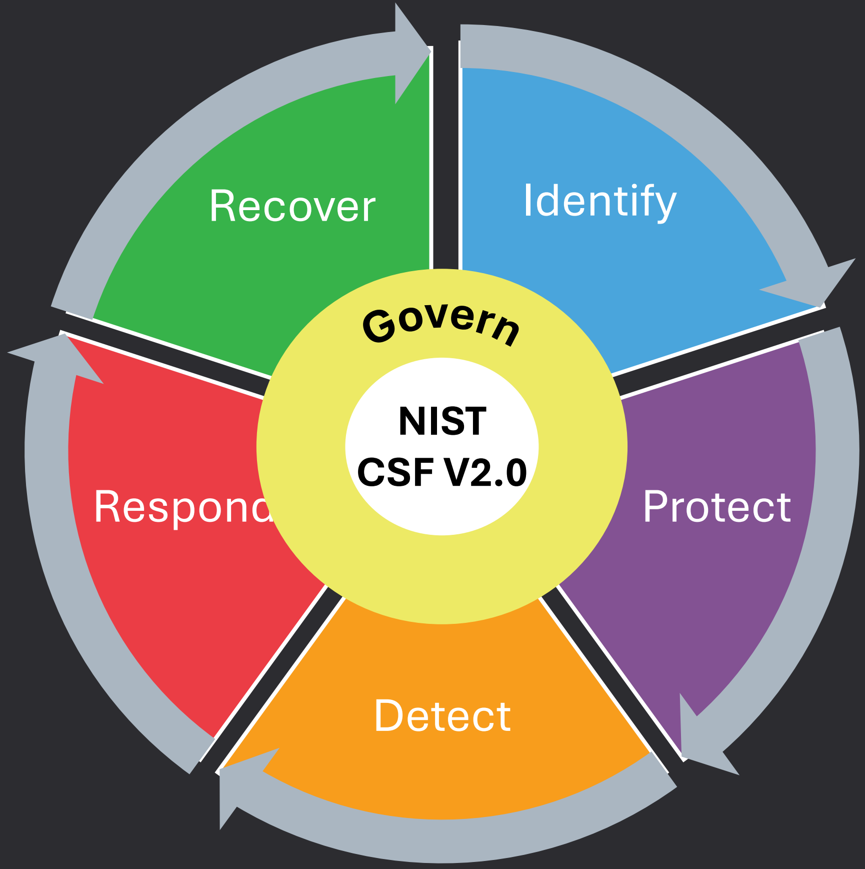
NIST CSF v2.0 Overview

Leveraging the NIST Cybersecurity Framework

August 2, 2024

Agenda

- NIST Cybersecurity Framework (CSF) 2.0 Benefits
- Changes from CSF v1.1 to CSF v2.0
- CSF v2.0 Overview
- Quick Implementation Walk-Through
  - Developing an Organizational Profile



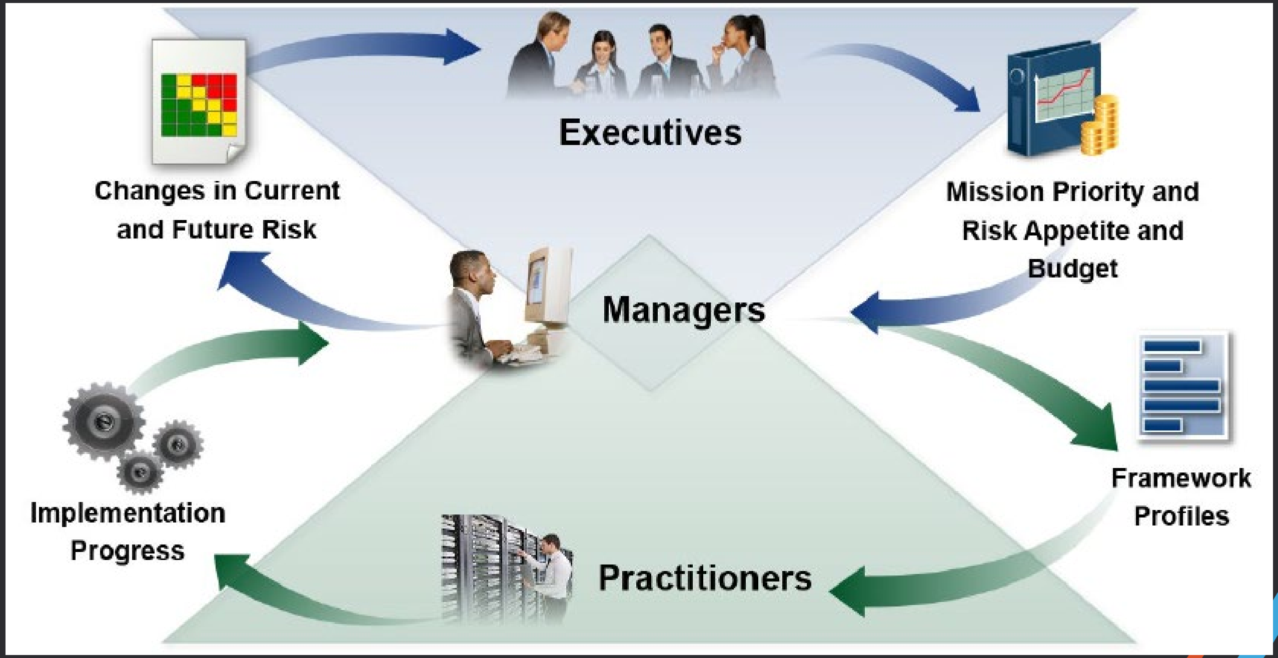
How Is CSF Used?

An organization can use the CSF with its supplementary resources to:

- **Understand:** Describe the current or target security posture of part, or all, of an organization.
- **Assess:** Determine gaps, and measure progress toward addressing those gaps.
- **Prioritize:** Identify, organize, and prioritize actions for managing cyber risks in alignment with organization's needs, and expectations.
- **Communicate:** Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations.

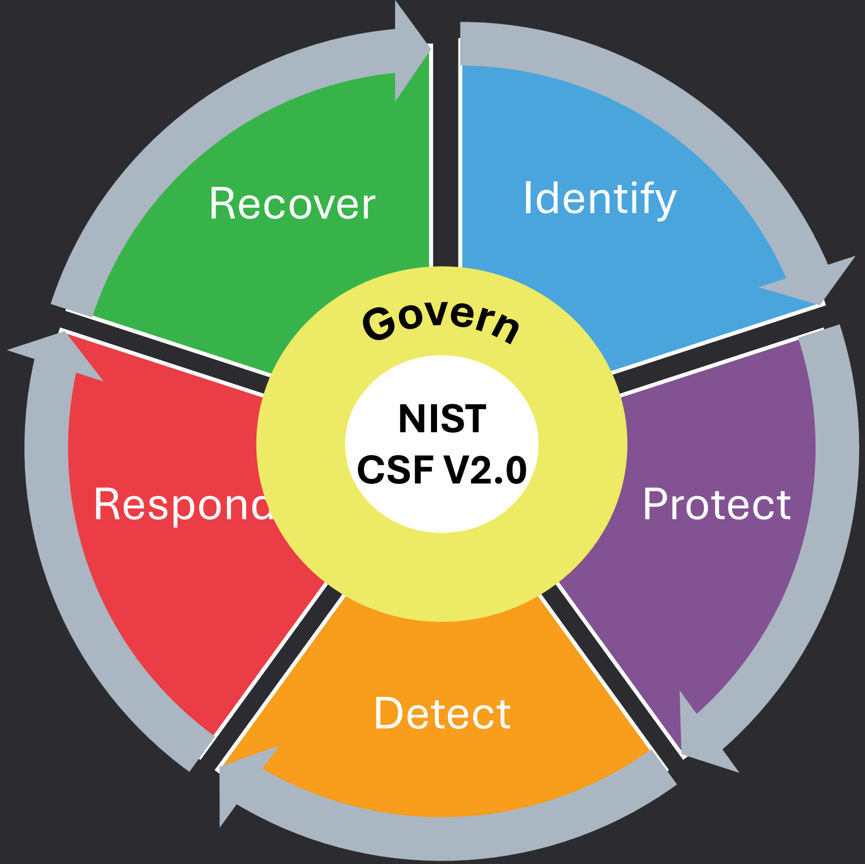
CSF 2.0 BENEFITS
Improving Risk Management Collaboration

- CSF 2.0 improves communication regarding cybersecurity expectations, planning, and resource needs.
- Promotes bidirectional information flow between:
  - Executives focused on the organization's priorities and strategic direction and managers who manage specific cybersecurity risks that could affect the achievement of those priorities.
  - Managers and the practitioners who implement and operate the services and underlying technologies.
- Provides a feedback mechanism for continuous improvement via "Implementation Progress" and "Changes in Risk".
- Helps managers and practitioners prioritize operating activities and resources to optimize mission achievement and mitigate risk.


Executives
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Managers
Framework Profiles
Implementation Progress
Practitioners

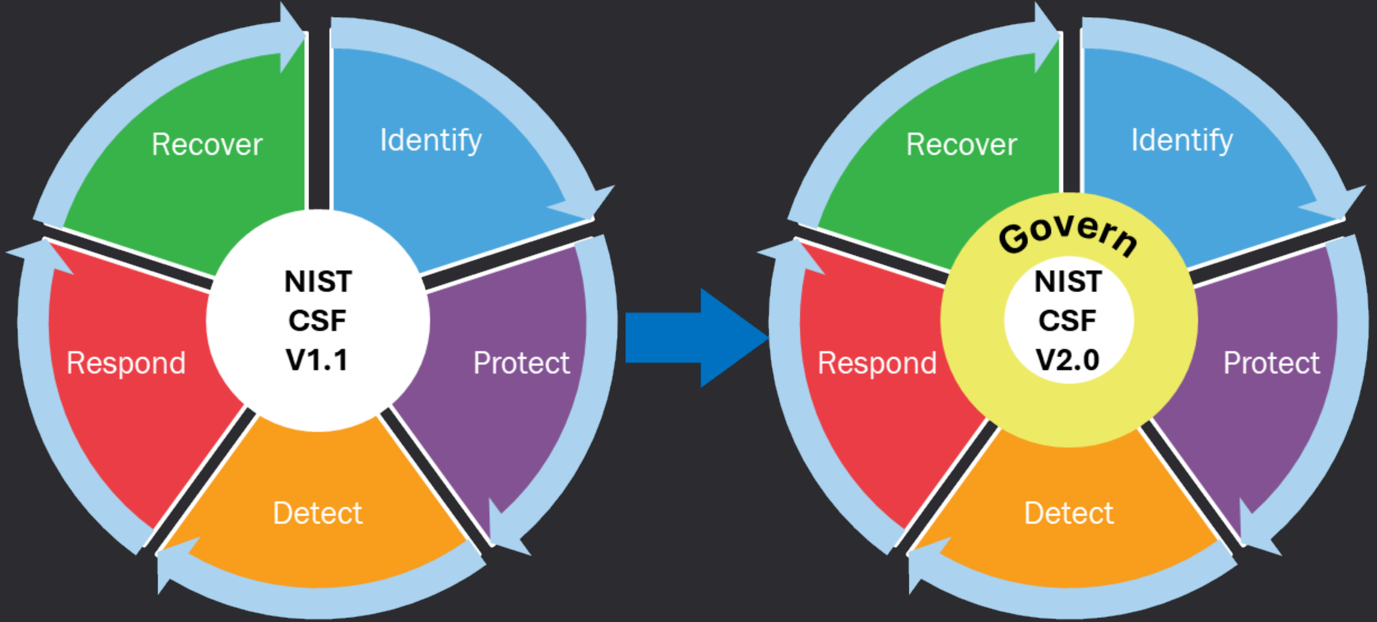
NIST Cybersecurity Framework (CSF) V2.0

- CSF is a framework that describes desired outcomes
  - Intended to be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise.
- Designed to help organizations of all sizes and sectors to manage and reduce their cybersecurity risks.
- Useful regardless of the maturity level and technical sophistication of an organization’s cybersecurity programs.
- CSF does not embrace a one-size-fits-all approach – it’s flexible
  - Organization have both common and unique risks, as well as varying risk appetites and tolerances.
- CSF is not prescriptive in its implementation
  - It’s a framework that organizations customize for their use.



Changes in CSF 1.1 to CSF 2.0 (Improvements)

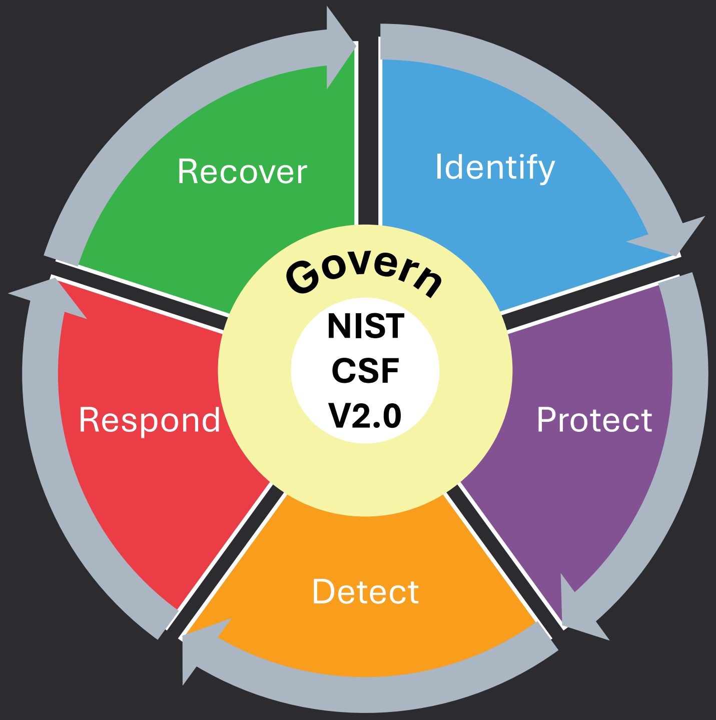
- CSF 2.0 adds new features that highlight the importance of governance and supply chains.
  - Note that Governance is now a separate core function
- Is now easier to work with and measure maturity (via CMMI V3.0)
- Special “Quick Start Guides” (QSGs) ensure applicability and easy accessibility by organizations of all sizes.



CSF 2.0 Core Design

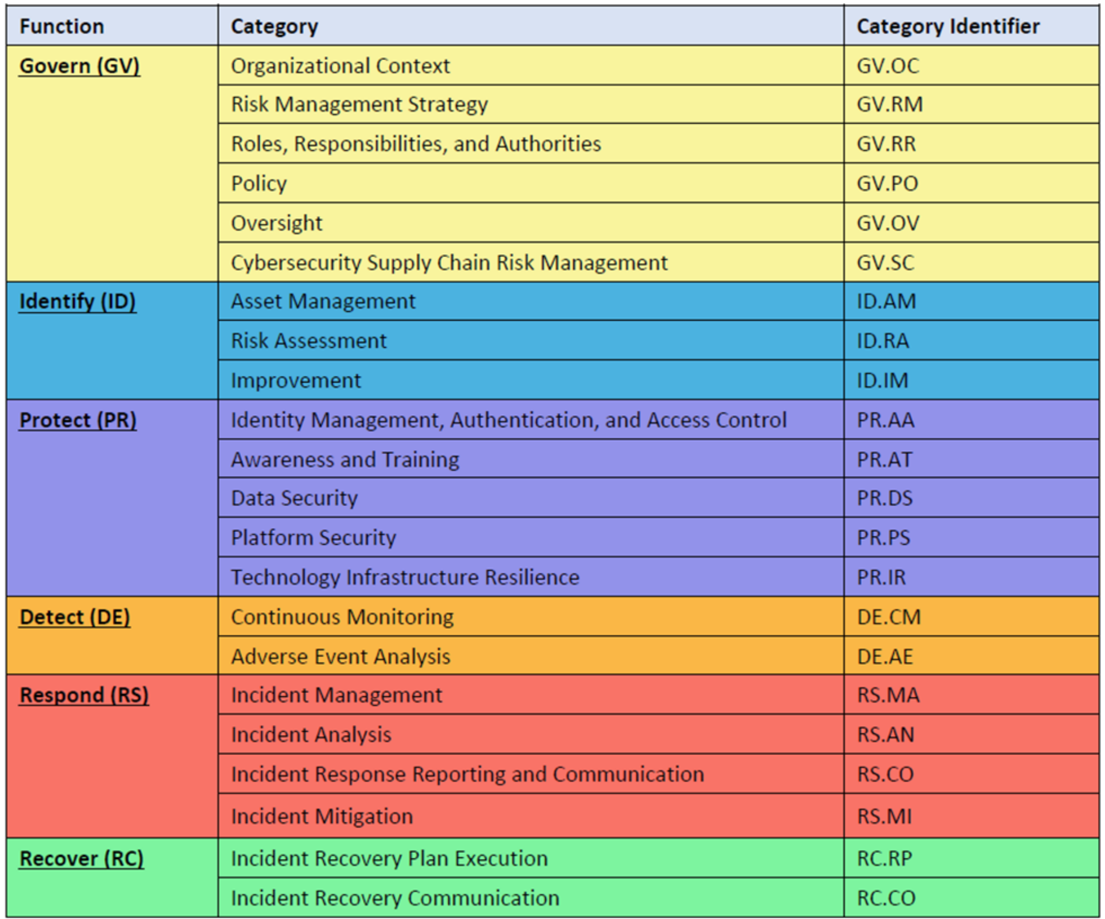
- CSF consists of a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks.
  - v2.0 has a hierarchy of 6 Functions, 22 Categories, and 106 Subcategories that detail each outcome.
- Outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise.
- Outcomes are sector-, country-, and technology-neutral.
  - Provides an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.

CSF v2.0



Core Function and Category names and identifiers

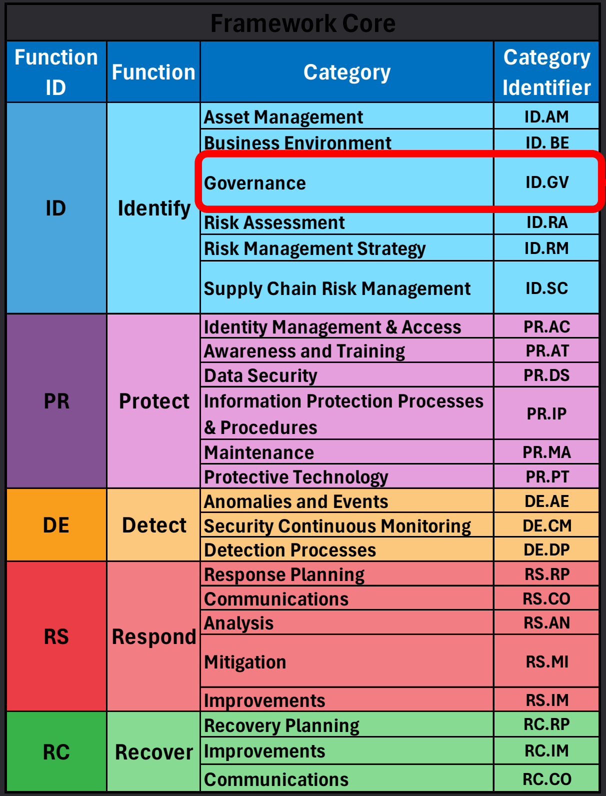
- Functions of the “iterative wheel” in table format.
  - With Function-specific Categories.
    - Within the Categories, there is the ability to create Subcategories:
    - These allow for greater decomposition of risk
  - Function and Categories names are intended to resonate most with those charged with operationalizing risk management within an organization.
- Order of Functions and Categories does not imply the importance of achieving them.
- Function gaps and risks should be assessed and addressed concurrently.
  - Actions that support GOVERN, IDENTIFY, PROTECT, and DETECT should all happen continuously, and;
  - Actions that support RESPOND and RECOVER should be ready at all times and happen when cybersecurity incidents occur.
- Organizations use existing policies, procedures, processes and technology in establishing their baselines
  - **Gaps and risks to** Functions, Categories and Subcategories will mature as the organization becomes more proficient



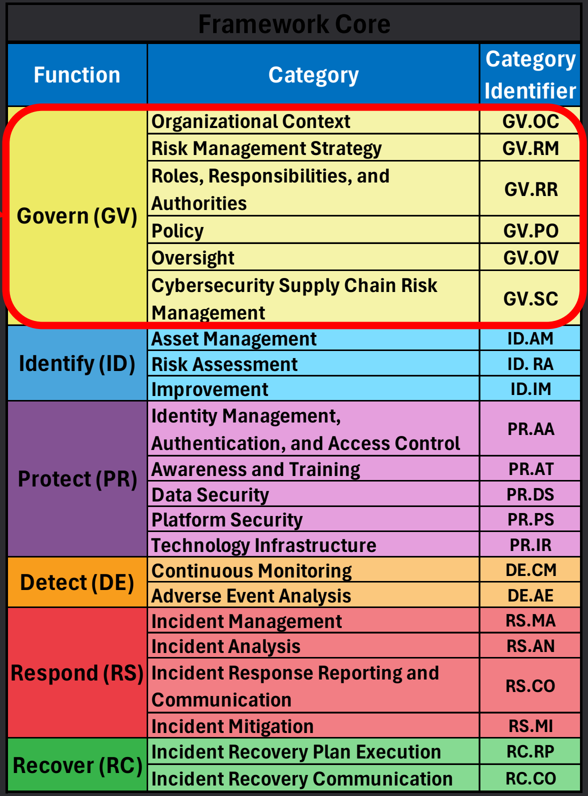
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF V1.1 – CSF V2.0 Change Details

- Most important – Governance is now a standalone function.
  - Some category activities are renamed and now within Governance function.
  - New categories added:
    - Roles and Responsibilities;
    - Policies, and;
    - Oversight.
- 12 other categories were renamed, realigned or removed entirely.
  - Reflects new cybersecurity needs.
- Overall, CSF 2.0 now easier to implement and provide better support to Operations and Enterprise Risk Management (ERM)



Framework Core			
Function ID	Function	Category	Category Identifier
ID	Identify	Asset Management	ID.AM
		Business Environment	ID. BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PR	Protect	Identity Management & Access	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
DE	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
RS	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
RC	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO



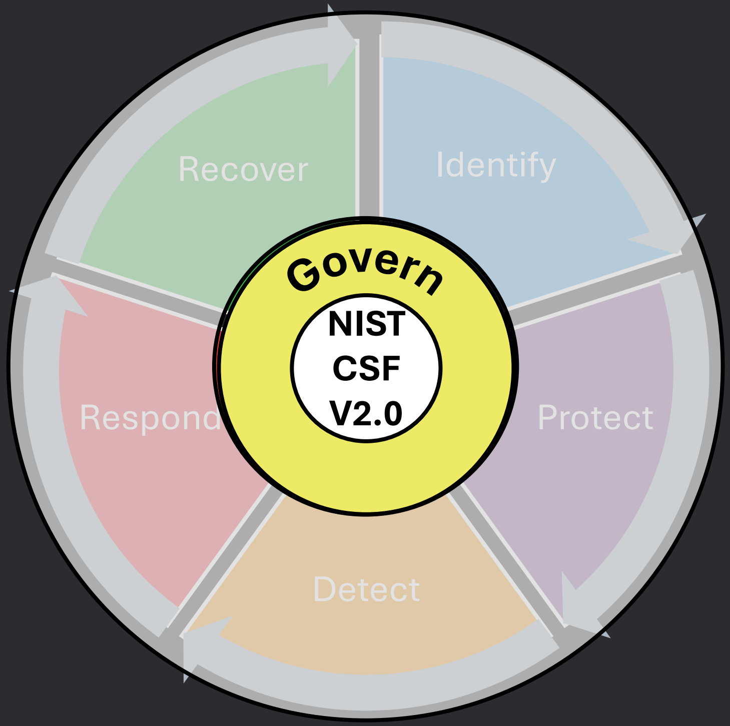
Framework Core		
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID. RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

5	Functions
23	Categories
108	Subcategories

6	Functions
22	Categories
106	Subcategories

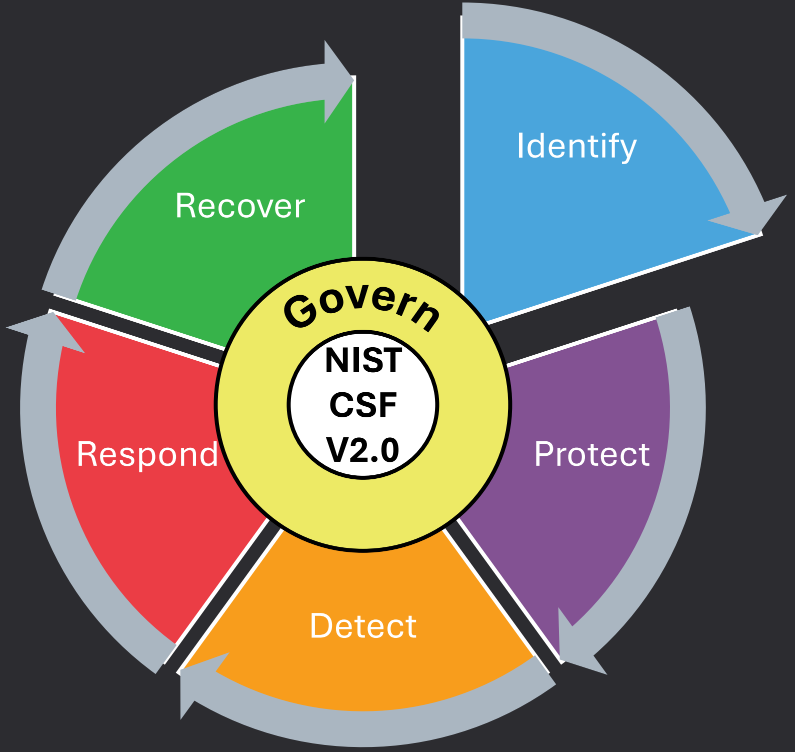
Core Function – Govern

- "**Govern**" – is for incorporating cybersecurity into the organization's broader enterprise risk management (ERM) strategy.
- Addresses:
  - an understanding of organizational context;
  - the establishment of cybersecurity strategy and cybersecurity supply chain risk management;
  - roles, responsibilities, and authorities;
  - policy; and
  - the oversight of cybersecurity strategy.
- The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- Provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations.



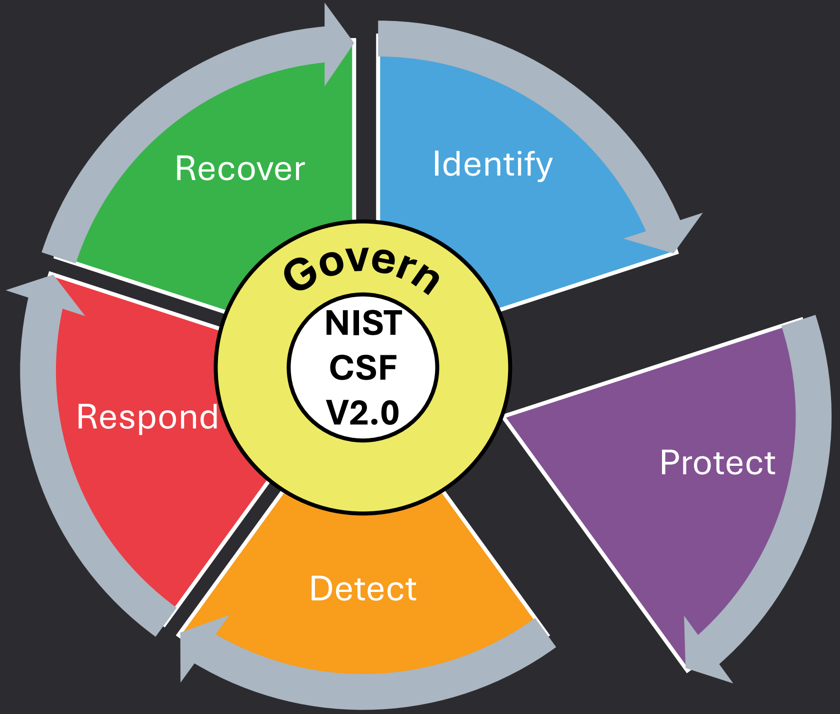
Core Function – Identify

- “**Identify**” – The organization’s current cybersecurity risks are captured and understood.
- Encompasses an understanding the organization’s assets and exposure – e.g.:
  - Information;
  - Processes;
  - People;
  - Technology (hardware, software, systems, services);
  - Facilities and infrastructure;
  - External resources/services; and
  - Related cybersecurity threats, vulnerabilities and risks to the organization
- Enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under “**GOVERN**”.



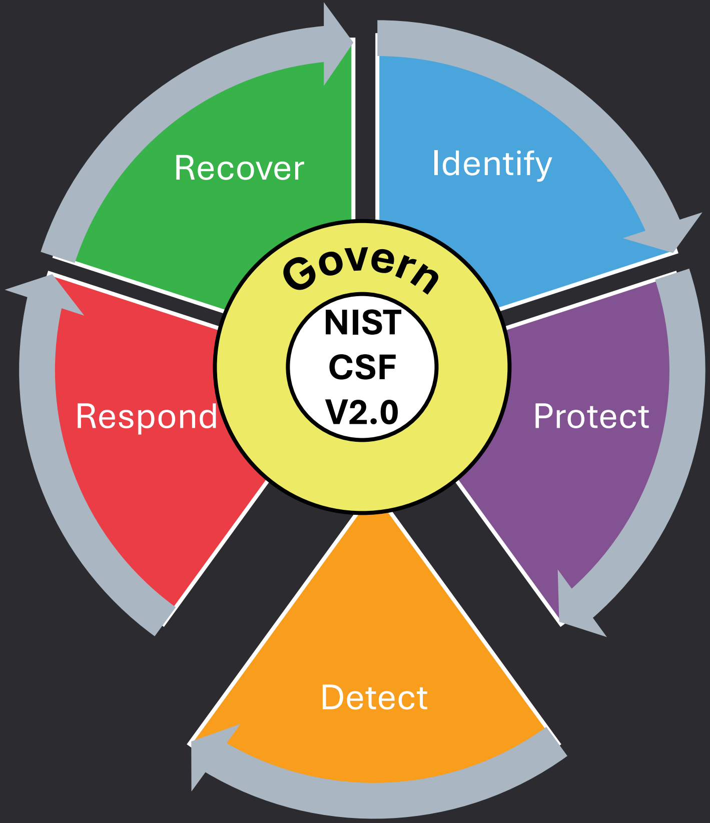
Core Function – Protect

- "**Protect**" – Safeguards to manage the organization's cybersecurity risks are implemented and used.
- Supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities.
- Outcomes addressed by "**Protect**" Function include:
  - identity management, authentication, and access control;
  - awareness and training;
  - data security;
  - platform security (i.e., securing the hardware, software, and services of physical and virtual platforms), and;
  - the resilience of technology infrastructure.



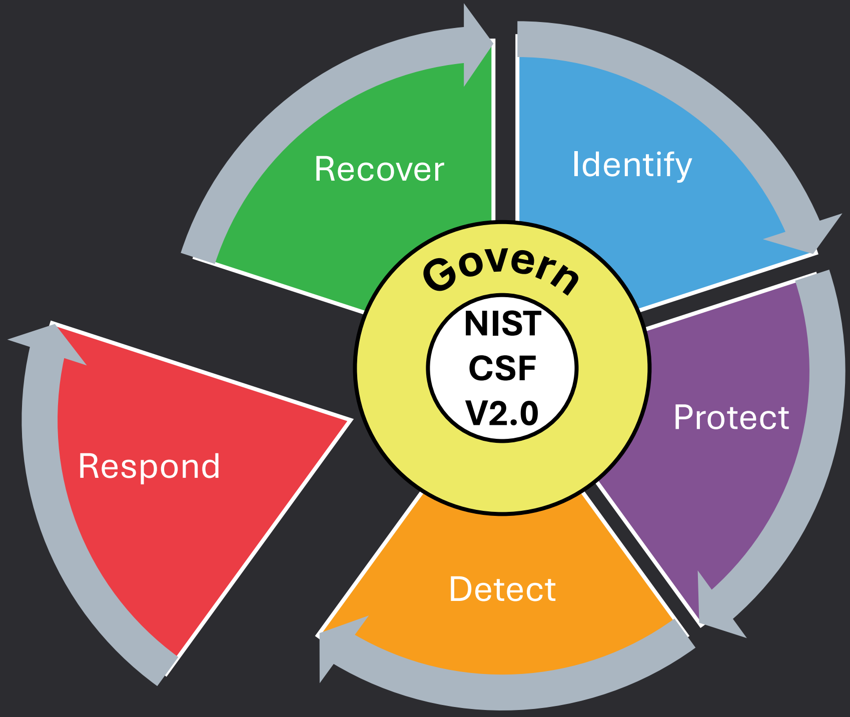
Core Function – Detect

- "**Detect**" – Possible cybersecurity attacks and compromises are found and analyzed.
    - Enables the timely discovery and analysis of anomalies, indicators of compromise; and
    - Other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring.
- Outcomes of the "**Detect**" Function includes:
    - Effective and successful incident response and recovery processes; and
    - Regular testing of detection processes in response emerging threats, vulnerabilities and risks.



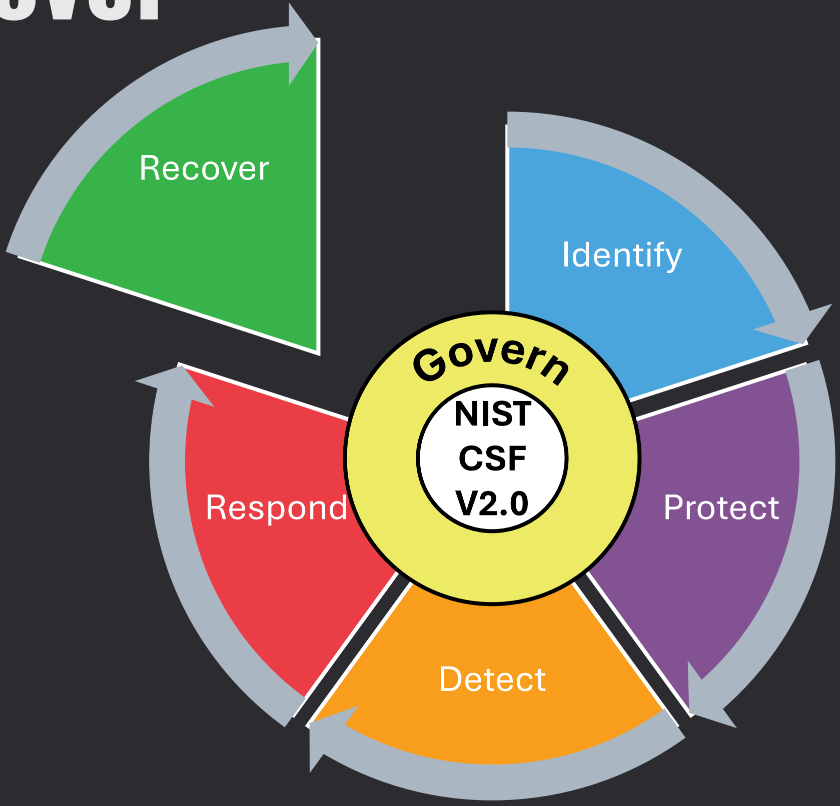
Core Function – Respond

- "**Respond**" – Actions regarding a detected cybersecurity incident are taken.
  - Ensures the ability to contain the effects of cybersecurity incidents using pre-defined incident response processes; and
  - Agility to adapt processes to unexpected threats and risks.
- Outcomes within the "**Respond**" Function cover
  - Incident containment, eradication, handling/management;
  - Analysis and mitigation:
  - Escalation, reporting; and
  - Appropriate communication with relevant parties via approved channels.



Core Function – Recover

- “**Recover**” – Assets and operations/services affected by a cybersecurity incident are restored.
- Outcomes of the “**RECOVER**” Function are:
  - Timely restoration of normal operations to reduce the effects of cybersecurity incidents;
  - Appropriate and timely communications during and post recovery efforts; and
  - Contribution to “Lessons Learned” for the improvement of cybersecurity and risk management.



How SimpliGRC Can Support

NIST CSF v1.1 and v2.0 assessment and implementation experience

Successfully completed several assessments and audits including NIST CSF, CIP, CIS, ISO, TSA

Softening silos and sub-cultures to achieve enterprise or project goals

Experienced in Business Impact Analysis and Risk Assessments

Senior analysis and project management services

IT / OT convergence services in complex environments

Strategy development and implementation

Process development and re-engineering

The managing directors deliver the services to offer the direct experience and competencies

Local to Calgary and Edmonton in Alberta, Canada

Contact Us

For more information:

visit https://simpligrc.com

OR

email: info@simpligrc.com

SIMPLI GRC

THANK YOU