



Cybersecurity & the abc's of GRC

Agenda

- Cybersecurity Trends
- The abc's of GRC
- Emphasis on Governance
- Risk Management
- Compliance
- When a plan comes together





Cybersecurity Trends

Gartner Top 9 Trends in Cybersecurity for 2024

1. Continuous Treat Exposure Management (CTEM)
2. Extending Identity and Access Management's Cybersecurity Value
3. Third-Party Cybersecurity Risk Management
4. Privacy-Driven Application and Data Decoupling
5. Generative AI
6. Security Behavior and Culture Programs
7. Cybersecurity Outcome-Driven Metrics
8. Evolving Cybersecurity Operating Models
9. Cybersecurity Reskilling

Source: [Top Cybersecurity Trends and Strategies for Securing the Future](#) | Gartner

Splunk: the CISO Report

Emerging trends, threats and strategies for today's security leaders



- Love it or hate it – AI is here to stay.
 - 70% of CISOs believe AI gives the advantage to attackers over defenders.
- CISOs often speak a different language than their board.
- CISOs are now the C-suite.
 - 47% of CISOs now report directly to their CEO.
- Most pay ransomware demands.
 - 90% of CISOs report that their organization experienced at least one disruptive attack last year.
- Boards prioritize security funding.
 - 93% of CISOs expect an increase in their cybersecurity budget over the next year.
- There is no resilience without collaboration.
 - Levels of cybersecurity collaboration are highest with IT operations.

CompTIA: State of Cybersecurity

Trends to Watch 2024



Policy: Risk management is the driving force behind cybersecurity



Process: Cybersecurity processes drive a wide range of decision-making



People: Talent pipelines get stronger as firms build skill resilience



Product: AI drives the cybersecurity product set to new heights.

KPMG: Cybersecurity considerations 2024: Government and public sector

Top priorities for government and public sector security professionals

- Strengthening cyber governance and risk management with appropriate frameworks and policies.
- Proactively plan for cyber incidents with meticulous documentation, regular training exercises and continuous evaluation.
- Using regulatory mandates as a catalyst for continuous improvement in cybersecurity practices.
- Actively seeking and integrating innovative technologies to stay ahead of the curve.



Source: <https://kpmg.com/xx/en/home/insights/2024/06/cybersecurity-considerations-2024-government-and-public-sector.html>



What Do These Trends Indicate?

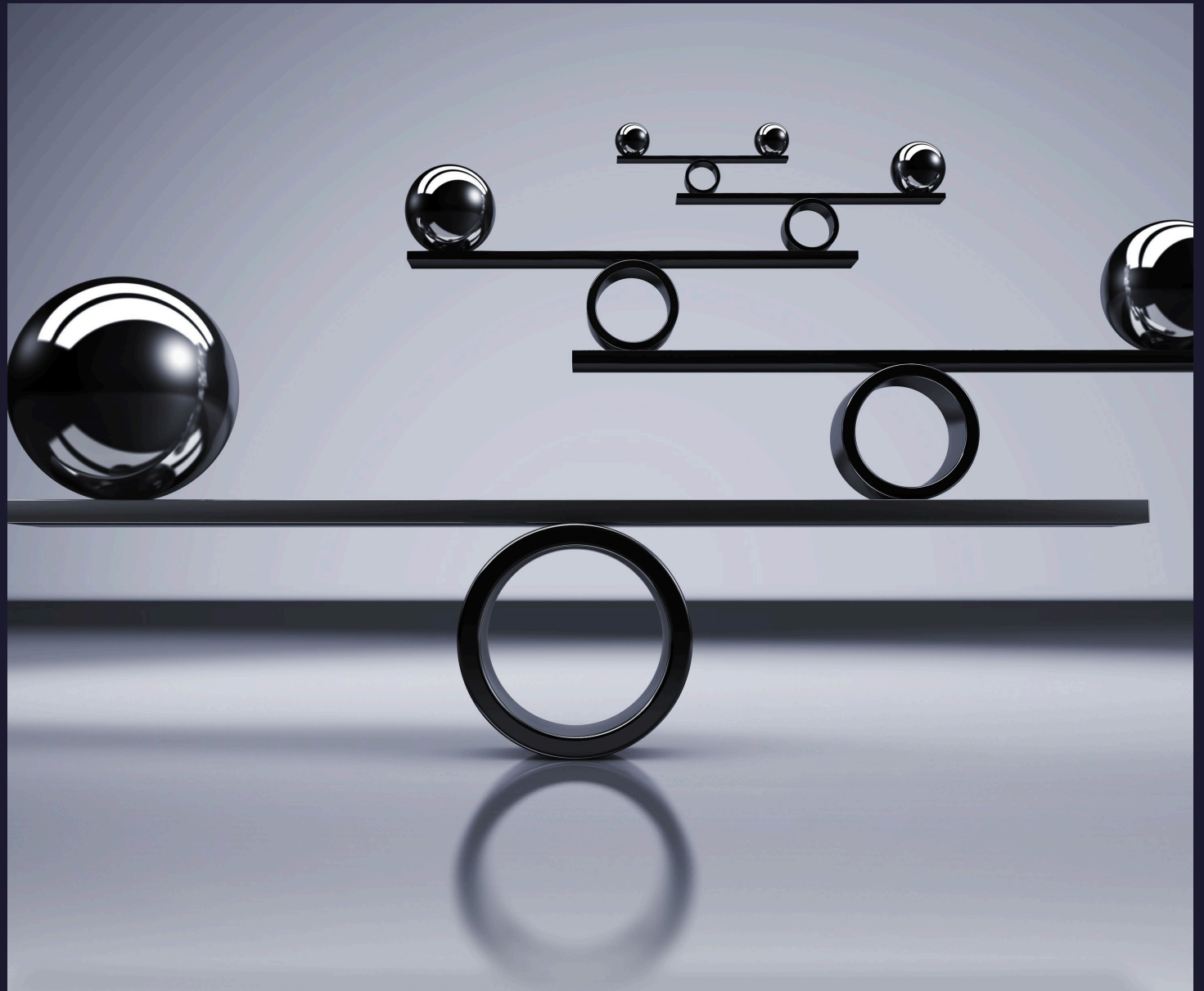
The abc's of GRC

The abc's of GRC

The balancing act between cybersecurity and business success is paramount.

The answer:

- Governance;
- Risk; and
- Compliance.



Governance Defined

Governance establishes requirements for how to achieve the proper balance of performance and conformance within an enterprise in order to meet stakeholder needs and deliver value.

It is the method by which an organization ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on organization objectives are achieved. It involves setting direction through prioritization and decision making, and monitoring performance and compliance against agreed-on direction and objectives. (ISACA)

Governance answers 4 questions:

- Are we doing the right things?
- Are we doing them the right way?
- Are we getting them done well?
- Are we seeing expected benefits?

Governance is the basic framework through which both long-term and day-to-day decisions will be made. (IIA)

Risk Defined

Cybersecurity Risk –

An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. (NIST)

Risk –

The possibility that an event will occur and adversely affect the achievement of objectives. (GAO)

Compliance Defined



The process of adhering to policies and decisions. Policies can be derived from internal directives, procedures and requirements, or from external laws, regulations, standards and agreements. (Gartner)

At its core, cybersecurity compliance means adhering to standards and regulatory requirements set forth by some agency, law or authority group. Organizations must achieve compliance by establishing risk-based controls that protect the confidentiality, integrity and availability (CIA) of information. (CompTIA)

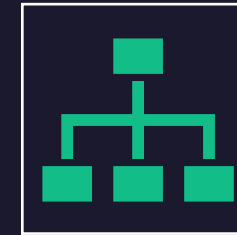


Governance, Risk, and Compliance (GRC)

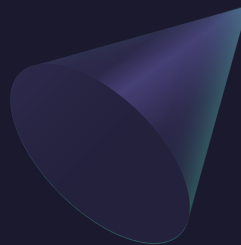
GRC is an organizational strategy to manage governance and risks while maintaining compliance with industry and government regulations.



GRC helps organizations effectively manage IT and security risks, reduce costs, reduce uncertainty and meet compliance requirements.



It also helps improve decision-making and performance through an integrated view of how well an organization manages its risks.

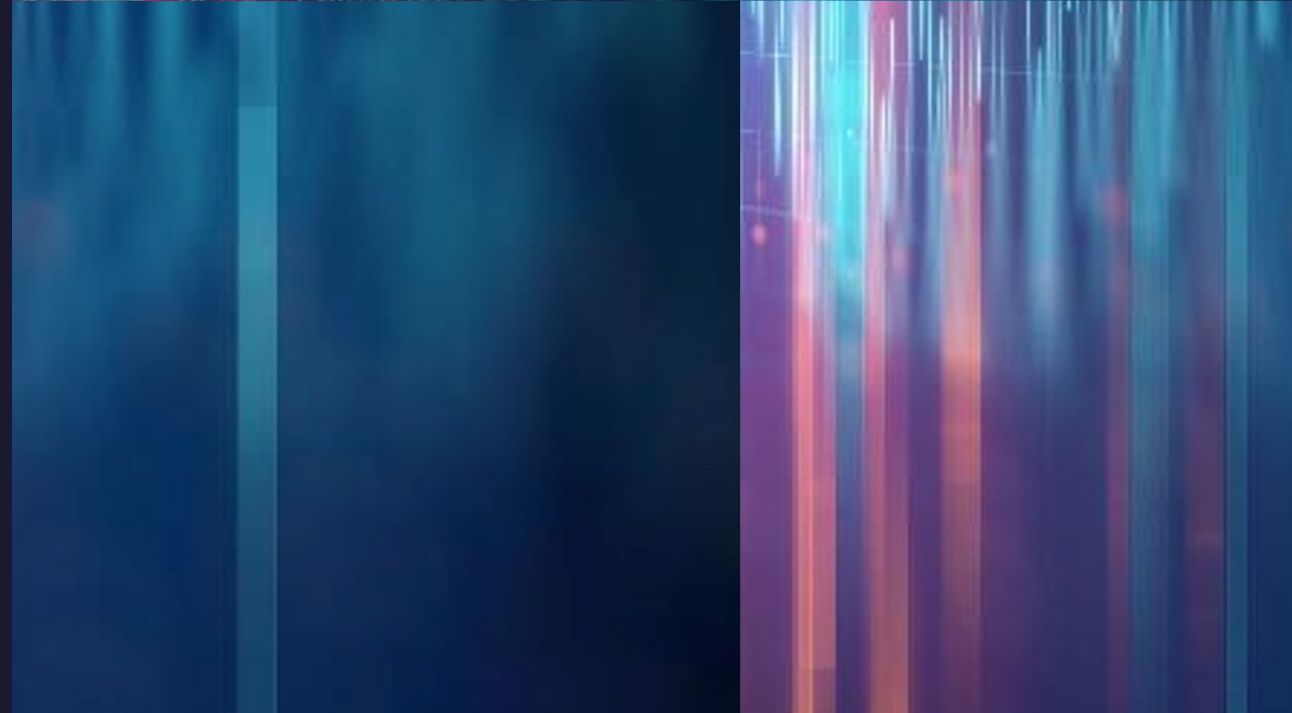




Emphasis on Governance

National Institute of Standards and Technology,
Cybersecurity Framework (NIST CSF) 2.0
(February 2024)

The Institute of Internal Auditors (the IIA)
Cybersecurity Topical Requirement Draft
(90-day public comment period)



NIST CSF 2.0 – Govern

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Category

Organizational Context (GV.OC) - The circumstances – mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements – surrounding the organization's cybersecurity risk management decisions are understood

Risk Management Strategy (GV.RM) - The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions

Roles, Responsibilities, and Authorities (GV.RR) - Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated

Policy (GV.PO) Organizational cybersecurity policy is established, communicated, and enforced

Oversight (GV.OV) Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy

Cybersecurity Supply Chain Risk Management (GV.SC) - Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders

The IIA: Cybersecurity Topical Requirement

Governance: Evaluating and Assessing Cybersecurity Governance

Policies and procedures related to cybersecurity risk management processes are established and periodically updated, including promotion of practices that strengthen the control environment based on widely adopted frameworks (NIST, COBIT, and others).

Roles and responsibilities that support the organization's cybersecurity objectives are clearly established and those roles are filled by individuals with the required knowledge, skills, and abilities.

Updates to cybersecurity objectives, strategies, risks, and mitigating controls are periodically communicated to the board.

Relevant stakeholders (for example, leadership, operations, strategic vendors, and others) are engaged to discuss how to best establish and improve cybersecurity risk management processes.

Required resources (such as leadership, funding, talent, hardware, software, and training) necessary to effectively execute cybersecurity risk management processes are communicated to the board.

Tie Back to Trends

- Alignment with Business Goals and Objectives (CompTIA: State of Cybersecurity, Splunk CISO Report, KPMG Cybersecurity Considerations)
- Supply Chain Risk Management (Gartner Top 9, CompTIA)
- People (CompTIA: State of Cybersecurity, Gartner Top 9)
- Generative AI (CompTIA: State of Cybersecurity, Gartner Top 9)



Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization’s cybersecurity risk management decisions are understood

**Alignment with Business
Goals and Objectives**

- **GV.RR-01:** Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.
- **GV.RR-02:** Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.
- **GV.RR-03:** Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.
- **GV.RR-04:** Cybersecurity is included in human resources practices.

Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders

- GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.
- GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.
- GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.
- GV.SC-04: Suppliers are known and prioritized by criticality.
- GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.
- GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.
- GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.
- GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.
- GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.
- GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.

People

Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks

- PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind
- PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind

Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

- GV.OC-01: The organizational mission is understood and informs cybersecurity risk management.
- GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.
- GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.
- GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.
- GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated.

Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced

- GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced
- GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission

Generative AI

Risk Management

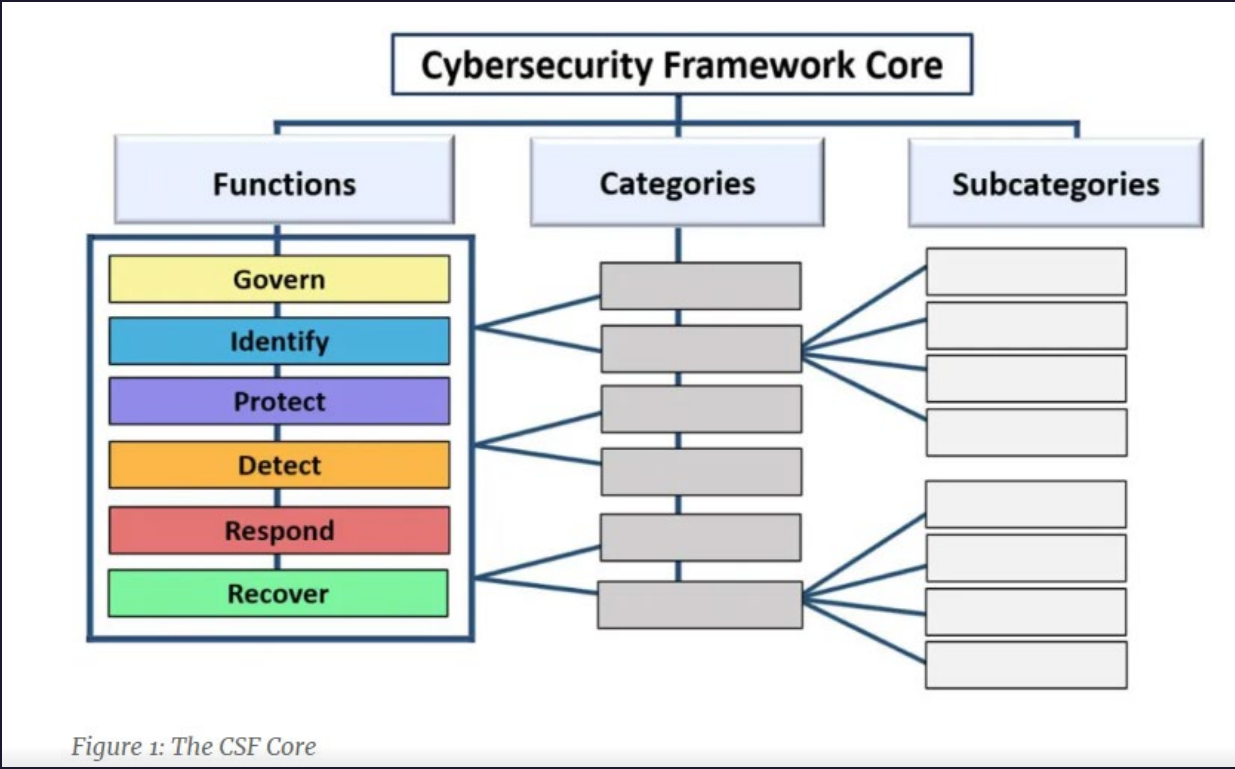
Risk management is the keystone of governance, and its core objectives are:

- Establish and maintain a common risk view.
- Integrate risk management into the enterprise.
- Make risk-aware business decisions.
- Ensure that risk management controls are implemented and operating effectively.



The CSF 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — to manage and reduce their cybersecurity risks.

Source: [Cybersecurity Framework \(CSF\) Overview](#)



NIST CSF 2.0 – Risk Management

Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.

Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.

Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization.

Cybersecurity Topical Requirement – Evaluating and Assessing Cybersecurity Risk Management

An organization wide risk management process is established that includes the identification, analysis, and management of risks related to IT and security, with a specific focus on cybersecurity risks and how those risks may affect the ability to achieve organizational objectives.

Cybersecurity risk management processes are conducted by a cross-functional team and engages external parties as applicable.

Cybersecurity risk management policies and procedures have been established and are periodically updated.

Accountability and responsibility regarding the management of cybersecurity risks is established and an individual or team has been identified that periodically monitors and communicates how cybersecurity risks are being managed.

A process is established to quickly escalate any cybersecurity risks that rise to unacceptable levels based on the organization's established risk management guidelines or to comply with applicable legal and/or regulatory requirements.

Cybersecurity risk management includes the coordination between information security, legal, compliance, and other management to identify and comply with all legal and contractual obligations, such as laws and regulations.

Cybersecurity Topical Requirement – Evaluating and Assessing Cybersecurity Risk Management Continued

A process is established to identify and manage cybersecurity risks related to third parties.


Policies and processes related to data classification, retention, destruction, and encryption are adequately designed and effectively deployed.

A process is established for communicating cybersecurity operational risks to ensure awareness by management and employees. Noncompliance with cybersecurity policies is identified, investigated, reported, and remediated in a timely manner.



Tie Back to Trends

Risk management is becoming the primary method for solving one of our greatest challenges: The connection between cybersecurity strategy and business operations. (CompTIA: State of Cybersecurity, KPMG Cybersecurity Considerations)



Compliance

Name _____

Signature _____

Date _____



NIST CSF 2.0



Fig. 2. CSF Functions

GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.

Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.

IDENTIFY (ID): The organization's current cybersecurity risks are understood.

- Asset Management (ID.AM)
- Risk Assessment (ID.RA)
- Improvement (ID.RM)

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used.

- 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): Possible cybersecurity attacks and compromises are found and analyzed.

- Continuous Monitoring (DE.CM)
- Adverse Event Analysis (DE.AE)

RESPOND (RS): Actions regarding a detected cybersecurity incident are taken.

- Incident Management (RS.MA)
- Incident Analysis (RS.AN)
- Incident Response Reporting and Communication (RS.CO)
- Incident Mitigation (RS.MI)

RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored.

- Incident Recovery Plan Execution (RC.RP)
- Incident Recovery Communication (RC.CO)

Cybersecurity Topical Requirement – Evaluating and Assessing Cybersecurity Control Processes

Prioritizes cybersecurity controls and ensures the related budget and resources (such as personnel, software, tools, and others) are allocated to maximize expected benefits.

Ensures that cybersecurity controls are functioning in a manner that promotes the achievement of organizational cybersecurity objectives and timely resolution of issues.

Provides sufficient training to personnel responsible for cybersecurity operations.

Ensures that management has the resources necessary to stay informed about emerging cybersecurity issues from new technologies, identify opportunities to improve operations, and understand how cybersecurity efforts can best be deployed to impact broader organizational goals and objectives.

Adequately integrates cybersecurity into the system development life cycle for business applications, including software and acquired or custom-developed applications.

Has included cybersecurity in the management of hardware (such as laptops, desktops, mobile devices).

Cybersecurity Topical Requirement – Evaluating and Assessing Cybersecurity Control Processes Continued

Has implemented effective controls regarding production hardware support, such as configuring, patching, supporting user access management, and monitoring availability and performance. The organization has evaluated both the design adequacy and operational effectiveness of these controls.

Optimizes network-related controls regarding network segmentation, the use and placement of firewalls, limited connections to external networks and/or systems, and the use of preventive and detective technologies such as intrusion detection/prevention systems.

Has implemented effective controls surrounding common desktop communication services such as email, internet browsers, videoconferencing, messaging, and file-sharing protocols.

Has implemented appropriate service delivery controls to ensure the following areas are integrated with cybersecurity monitoring: change management, service/help desk, and end-user device administration.

Has implemented appropriate physical security controls to protect high-risk information centers (such as data centers, network operations centers, and security operations centers) from attacks.

Has implemented incident response and recovery controls.

A perspective view of a server room aisle. The server racks on both sides are filled with equipment, and their front panels are covered in numerous small, glowing lights, primarily in shades of white and green. The floor is a light-colored, perforated metal grating. The overall lighting is a cool, blue-toned glow, creating a sense of depth and technology.

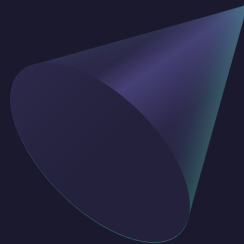
Tie Back to Trends

Cybersecurity outcome-driven metrics (Splunk: The CISO Report, Gartner: Top 9)

Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy

Cybersecurity outcome-driven metrics

- GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.
- GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.
- GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.





When a plan
comes
together...
GRC Rules!

Thank you

Sarah Kosberg, CGEIT, CISSP, CISA, CIA, CFE, CIG,
CIGA

Sarah.Kosberg@digital.fl.gov

