

**NIST Cybersecurity Framework v2.0**

**Workbook**

**September 2024**

**Prepared by:**

Table of Contents

1 Introduction 3

1.1 NIST Cybersecurity Framework 2.0 Overview 3

1.2 Scoping - Cybersecurity in Business 4

2 Govern (GV) 5

2.1 Organizational Context (GV.OC) 5

2.1.1 GV.OC Considerations 5

2.2 Risk Management Strategy (GV.RM) 6

2.2.1 GV.RM Considerations 6

2.3 Roles, Responsibilities, & Authorities (GV.RR) 6

2.3.1 GV.RR Considerations 7

2.4 Policy (GV.PO) 7

2.4.1 GV.PO Considerations 7

2.5 Oversight (GV.OV) 8

2.5.1 GV.OV Considerations 8

2.6 Cybersecurity Supply Chain Risk Management (GV.SC) 8

2.6.1 GV.SC Considerations 9

3 Identify 10

3.1 Asset Management (ID.AM) 10

3.1.1 ID.AM Considerations 10

3.2 Risk Assessment (ID.RA) 10

3.2.1 ID.RA Considerations 11

3.3 Improvement (ID.IM) 11

3.3.1 ID.IM Considerations 11

4 Protect 13

4.1 Identity Management, Authentication, and Access Control (PR.AA) 13

4.1.1 PR.AA Considerations 13

4.2 Awareness and Training (PR.AT) 13

4.2.1 PR.AT Considerations 14

4.3 Data Security (PR.DS) 14

4.3.1 PR.DS Considerations 14

4.4 Platform Security (PR.PS) 15

4.4.1 PR.PS Considerations 15

4.5 Technology Infrastructure Resilience (PR.IR) 16

4.5.1 PR.IR Considerations 16

5 Detect 17

5.1 Continuous Monitoring (DE.CM) 17

5.1.1 DE.CM Considerations 17

5.2 Adverse Event Analysis (DE.AE) 17

5.2.1 DE.AE Considerations 18

6 Respond 19

6.1 Incident Management (RS.MA) 19

6.1.1 RS.MA Considerations 19

6.2 Incident Analysis (RS.AN) 19

6.2.1 RS.AN Considerations 20

6.3 Incident Response Reporting and Communication (RS.CO) 20

6.3.1 RS.CO Considerations 20

6.4 Incident Mitigation (RS.MI) 21

6.4.1 RS.MI Considerations 21

7 Recover 22

7.1 Incident Recovery Plan Execution (RC.RP) 22

7.1.1 RC.RP Considerations 22

7.2 Incident Recovery Communication (RC.CO) 23

7.2.1 RC.CO Considerations 23

# Introduction

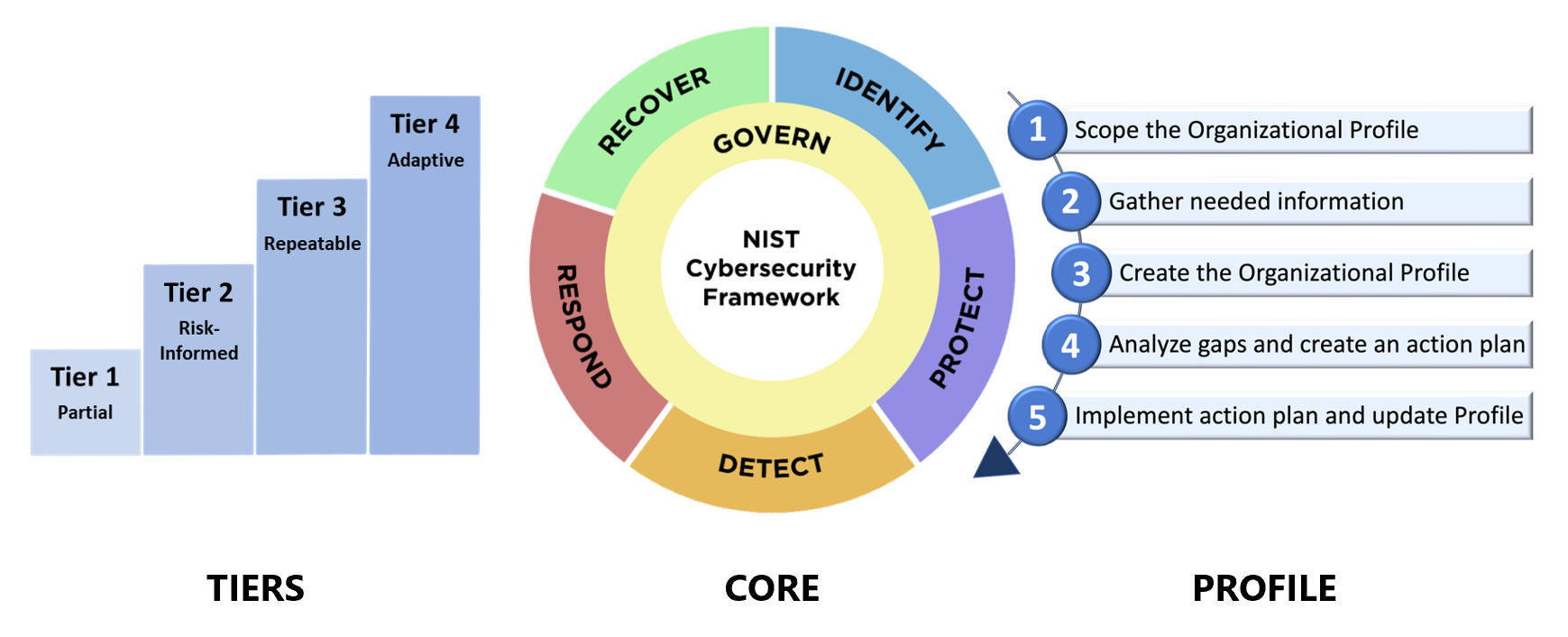
This workbook is provided as an introductory tool to assist organizations in creating a strategy aligned with the Cybersecurity Framework (CSF) v2.0. It provides an overview of the three key components of the CSF v2.0 and offers guidance on the Categories, including key questions to consider. The intent of this workbook is to help organizations in getting started with the CSF v2.0 by providing a foundational understanding of key aspects of their cybersecurity posture.

While this workbook provides a foundational approach, it encourages users to think critically about their unique cybersecurity needs and goals. This tool fosters a proactive and strategic mindset, guiding users toward establishing a strong cybersecurity foundation. However, users are encouraged to consult additional resources for ensuring all aspects of your cybersecurity program are addressed as you finalize your organization’s cybersecurity strategy.

For questions or assistance completing this workbook, please contact Optic Cyber Solutions at [Info@OpticCyber.com](mailto:Info@OpticCyber.com).

## NIST Cybersecurity Framework 2.0 Overview

The NIST Cybersecurity Framework defines a risk management approach for implementing cybersecurity. This Framework contains three primary components: Framework Core, Implementation Tiers, and Profiles.



The **Framework** **Core** establishes a hierarchal definition of key cybersecurity expectations for a cybersecurity program.

The **Tiers** include four levels to provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.

The **Profiles** provide a mechanism to capture the current and target state of an organization’s cybersecurity program.

## Scoping - Cybersecurity in Business

When defining a cybersecurity program, it’s crucial to clearly scope the parameters and identify what needs protection—whether it’s a single department, a line of business, or the entire company. A clear understanding of the key business objectives that your cybersecurity efforts are meant to support is essential to ensuring the program is effective and aligned with organizational goals.

The cybersecurity triad represents three fundamental principles that are crucial for securing business data. In the context of business data, the cybersecurity triad emphasizes the need to protect data from unauthorized access (Confidentiality), ensure it remains accurate and trustworthy (Integrity), and guarantee it's always accessible for business operations (Availability).

1. What types of data does your organization process?
2. What are your business goals & objectives?
3. What systems and partners do you depend on for meeting those goals?
4. Do you expect everyone to meet the same cybersecurity outcomes, or will different teams have different expectations?

# Govern (GV)

Establishes organizational cybersecurity risk management strategies, expectations, and policies enabling effective communications and monitoring of the cybersecurity program. This Function ensures everyone is working in the right direction.

## Organizational Context (GV.OC)

*What do you need to consider as you create your cybersecurity program?*

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

Organizational Context emphasizes a comprehensive understanding of an organization's mission, ensuring it shapes and guides cybersecurity risk management. This category recognizes the importance of identifying both internal and external stakeholders, understanding their expectations concerning cybersecurity, and effectively communicating critical objectives, capabilities, and services. Moreover, it underscores the significance of being well-informed about the prevailing legal, regulatory, and contractual requirements related to cybersecurity, including obligations towards privacy and civil liberties. Lastly, it underscores the need to determine and communicate the critical objectives, capabilities, services, and outcomes essential to the organization and its stakeholders.

### GV.OC Considerations

1. How does technology support your business goals? (or how could a cyber incident hinder your operations?)

1. What technology (e.g., devices, systems, platforms) do you depend on?
2. Do you have any cybersecurity related compliance or contractual requirements?
3. Are there any external factors or trends, like new regulations or market shifts, that you believe might impact how you handle digital information and security?

## Risk Management Strategy (GV.RM)

*What is keeping your business running?*

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

Risk Management Strategy centers on establishing and communicating the organization's priorities, constraints, risk tolerance, and assumptions to guide operational risk decisions. This strategy ensures that risk management objectives align with organizational stakeholders' expectations. It emphasizes the importance of defining and maintaining clear statements on risk appetite and tolerance. This Category integrates cybersecurity risk management into broader enterprise risk management processes and provides strategic direction on suitable risk response options. Effective communication lines are established across the organization, addressing risks from various sources, including third-party suppliers. The strategy also introduces a standardized approach for evaluating and prioritizing cybersecurity risks and recognizes the potential of strategic opportunities, or positive risks, in cybersecurity discussions.

### GV.RM Considerations

1. How do you currently decide what digital security measures to put in place or prioritize?
2. What is the most important to your business: Confidentiality, Availability, or Integrity
3. How confident are you that you could continue operating through a cyber-attack?
4. What is your risk appetite?
5. Have you defined your risk tolerance?

## Roles, Responsibilities, & Authorities (GV.RR)

*What are your cybersecurity responsibilities?*

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

Roles, Responsibilities, and Authorities emphasize the establishment and communication of clear cybersecurity roles, responsibilities, and authorities to ensure accountability, performance assessment, and continuous improvement. Organizational leadership is at the forefront, bearing responsibility and accountability for cybersecurity risk, and is instrumental in cultivating a culture that is risk-aware, ethical, and committed to continuous enhancement. This Category underscores the importance of allocating adequate resources in alignment with the organization's cybersecurity risk strategy, roles, responsibilities, and policies. Additionally, this Category integrates cybersecurity considerations into human resources practices, ensuring that cybersecurity awareness and responsibilities are ingrained in the organization's HR processes.

### GV.RR Considerations

1. Who is responsible for ensuring the cybersecurity of your business?
2. How do you define expectations for your team (e.g., cyber professionals and non-cyber professionals)?
3. How do you typically communicate and address digital or security issues within your team?

## Policy (GV.PO)

*How do you keep everyone on the same page?*

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

Policies, Processes, and Procedures focuses on establishing, communicating, and enforcing organizational cybersecurity policies, processes, and procedures. Guidelines should be formulated based on the organization's context, cybersecurity strategy, and priorities. Policies should be communicated, enforced, and undergo regular reviews and updates to ensure that they remain relevant and effective in the face of evolving requirements, threats, technological advancements, and shifts in the organizational mission.

### GV.PO Considerations

1. How is cybersecurity guidance (e.g., policies, procedures, announcements) communicated across the organization?
2. Is your team aware of the cybersecurity guidelines that have been provided?
3. Who sets the cybersecurity guidelines?

## Oversight (GV.OV)

*Are you keeping an eye on the effectiveness of your cybersecurity?*

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

Oversight emphasizes the significance of utilizing the outcomes of organization-wide cybersecurity risk management activities to refine and adapt the overarching risk management strategy. It underscores the importance of regularly reviewing the results of the cybersecurity risk management strategy to ensure its alignment with the organization's goals and direction. Furthermore, the strategy is continually assessed to ensure its comprehensive coverage of the organization's requirements and potential risks. To ensure the strategy's effectiveness and relevance, the organization's cybersecurity risk management performance is consistently measured, reviewed, and adjusted as needed to align with the strategic direction.

### GV.OV Considerations

1. When was your cybersecurity capabilities last reviewed?
2. How successful is your cybersecurity program today?
3. What could be improved in your cybersecurity program? What is working well?

## Cybersecurity Supply Chain Risk Management (GV.SC)

*Do you know what your suppliers are up to?*

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

Cybersecurity Supply Chain Risk Management (C-SCRM) emphasizes the identification, establishment, and continuous improvement of cyber supply chain risk management processes by organizational stakeholders to include. It underscores the importance of defining clear cybersecurity roles and responsibilities for suppliers, customers, and partners, both internally and externally. C-SCRM into broader cybersecurity and enterprise risk management processes and prioritizes understanding suppliers based on their criticality and establishes requirements to address cybersecurity risks in contracts and agreements with suppliers and other third parties. C-SCRM promotes proactive planning and due diligence before formalizing relationships with suppliers and continuously monitors and assesses the risks posed by these external entities throughout the relationship. Additionally, it ensures the inclusion of relevant suppliers in incident response activities and integrates supply chain security practices into overarching risk management programs, monitoring their efficacy throughout the product and service lifecycle.

### GV.SC Considerations

1. Who are your partners and suppliers?
2. Do they have access to your systems, networks, or data?
3. How are they protecting your company’s resources?
4. What agreements and obligations do you have in place in the event of a cybersecurity incident?

# Identify

Defines organizational cybersecurity risk for the organization. Establishes cyber risk for business resources (e.g., people, technology, services). This Function identifies what you have and the risks associated with their loss.

## Asset Management (ID.AM)

*Do you know what you have?*

Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) 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

Asset management involves the identification, classification, and inventorying of an organization's information and technology assets. It includes understanding the value, criticality, and sensitivity of these assets to prioritize protection measures and allocate resources effectively. By implementing asset management practices, organizations can gain better visibility into their assets, assess potential risks and vulnerabilities, and implement appropriate security controls to safeguard their valuable assets from unauthorized access, loss, or compromise.

### ID.AM Considerations

1. How do you track inventories?
2. How are assets categorized?
3. What tools are used to record inventories?
4. How often are inventories reviewed and validated?
5. What is the process for decommissioning an asset?

## Risk Assessment (ID.RA)

*How do you assign and track cyber risk to your business?*

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

Risk assessment refers to the systematic process of identifying, analyzing, and evaluating potential cybersecurity risks to an organization's assets, systems, and data. It involves assessing the likelihood and potential impact of various threats and vulnerabilities, considering the organization's business environment and objectives. Risk assessment helps organizations prioritize and allocate resources effectively, enabling them to implement appropriate safeguards and controls to mitigate identified risks and reduce the overall cybersecurity risk exposure.

### ID.RA Considerations

1. How do you evaluate your cybersecurity risk?
2. Do you perform vulnerability assessments?
3. How are identified vulnerabilities and misconfigurations prioritized and tracked?
4. How do you gather and communicate threat intelligence information?
5. What is the process of vetting products and services before they are acquired?

## Improvement (ID.IM)

*How do you ensure your business doesn’t become complacent and stagnant?*

Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions

Improvement focuses on the continuous enhancement of organizational cybersecurity risk management across all the six CSF Functions (i.e., Govern, Identify, Protect, Detect, Respond, and Recover). It advocates for the application of continuous evaluation methods to pinpoint areas of improvement. Regular security tests and exercises, including collaborations with suppliers and relevant third parties, are conducted to further identify areas of enhancement. This Category also underscores the importance of utilizing lessons learned from operational processes and activities to inform improvements. Additionally, any cybersecurity plans that impact operations are not only communicated and maintained but are also subject to ongoing refinement to ensure optimal effectiveness.

### ID.IM Considerations

1. How are self-assessments performed to determine the effectiveness of processes?
2. What is the process for reporting deficiencies or proposed improvements for business processes?
3. Do you have third-party assessments to review conformity to your cybersecurity program?
4. Who is responsible for identifying and developing cybersecurity plans (e.g., IRP, DRP, BCP)

# Protect

Defines and establishes safeguards for managing cybersecurity risk within an organization. This Function defines the capabilities required to properly operate and maintain your business.

## Identity Management, Authentication, and Access Control (PR.AA)

*Who’s allowed to do what?*

Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access

Identity management, authentication, and access control pertain to the processes and mechanisms employed by an organization to manage user identities, authenticate their identities, and control their access to systems, networks, and data. It involves implementing robust identity and access management practices, such as user provisioning, role-based access control, and multi-factor authentication, to ensure that only authorized individuals can access sensitive resources. By effectively managing identities and controlling access, organizations can reduce the risk of unauthorized access, insider threats, and privilege abuse, thus enhancing the overall security posture and protecting critical assets.

### PR.AA Considerations

1. How does your organization manage user access to systems and services?
2. Is identity verification conducted prior to providing access?
3. What measures are in place to review and revoke access when it's no longer needed?
4. How does your organization ensure that only authorized individuals have access to the systems and services they need?
5. How often do employees change or update their passwords?

## Awareness and Training (PR.AT)

*What do you actually want me to do?*

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

Awareness and training refers to the systematic approach adopted by organizations to educate their workforce on cybersecurity risks, best practices, and policies. It involves creating a culture of cybersecurity awareness and providing relevant training to employees at all levels of the organization. By promoting cybersecurity awareness and providing regular training, organizations can empower their workforce to recognize and respond to potential threats, make informed security decisions, and actively contribute to the protection of critical systems and data, thus enhancing the overall resilience of the organization.

### PR.AT Considerations

1. How often are your employees trained on cybersecurity topics?
2. Is specialized training provided for designated user types?
3. Are users trained on identifying and defending against social engineering attacks?

## Data Security (PR.DS)

*How do you ensure your secrets remain secret?*

Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information

Data security focuses on protecting the confidentiality, integrity, and availability of sensitive and critical data. It involves implementing appropriate safeguards and controls to prevent unauthorized access, disclosure, alteration, or destruction of data. This includes measures such as encryption, access controls, data loss prevention, backup and recovery, and secure data handling practices, aimed at minimizing the risks associated with data breaches, unauthorized disclosure, or data corruption, ensuring the protection and privacy of sensitive information.

### PR.DS Considerations

1. What are commons ways that your organization protects data?
2. How does your organization ensure that business data remains accurate and free from unauthorized modifications throughout its lifecycle?
3. How impactful would a short- or long-term loss of data access be to your business?
4. What data is backed up to ensure that it can be recovered?

## Platform Security (PR.PS)

Are you *protecting all your platforms?*

Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability

Platform Security emphasizes the importance of managing the hardware, software, and services of both physical and virtual platforms in alignment with an organization's overarching risk strategy. Central to Platform Security is the application of configuration management practices, ensuring that every component, from firmware to applications, is set up and maintained to meet the dual objectives of security and operational efficiency. The lifecycle of both software and hardware is rigorously managed, with decisions on their maintenance, replacement, or removal being informed by a thorough risk assessment. Continuous monitoring is facilitated through the generation and accessibility of log records, providing real-time insights into system operations and potential anomalies. Complementing this is the integration of secure software development practices, which are embedded throughout the software's lifecycle. This holistic approach ensures that software is developed, deployed, and maintained with security at its core, and its performance is under constant scrutiny from inception to retirement.

### PR.PS Considerations

1. How does your organization ensure that the software and platforms your team uses are up-to-date?
2. How does your organization ensure that system and platform configurations are aligned with established security standards and best practices?
3. What are you logging to help identify potential anomalies or security threats?
4. How do you integrate secure software development practices throughout the software lifecycle?
5. How do you align your Platform Security strategies with your organization's overall risk management activities?

## Technology Infrastructure Resilience (PR.IR)

*What can you do today to prepare for problems tomorrow?*

Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience

Technology Infrastructure Resilience focuses on managing security architectures in alignment with the organization's risk strategy to safeguard asset confidentiality, integrity, availability, and bolster organizational resilience. Key components include the protection of networks and environments from unauthorized logical access and usage. This Category also emphasizes shielding the organization's technology assets from environmental threats. Resilience mechanisms are put in place to ensure the organization can function both under normal and adverse conditions. Additionally, sufficient resource capacity is deployed to ensure and maintain availability consistently.

### PR.IR Considerations

1. Does your network architecture protect your critical systems?
2. How do you ensure only trusted assets and users gain access to sensitive systems or data?
3. Do you have adequate environmental protections in place?
4. How does your organization ensure that it has adequate resource capacity, both in terms of hardware and bandwidth, to maintain the availability of critical systems and services?

# Detect

Detect enables organizations to identify and analyze potential cybersecurity incidents to determine appropriate response activities. This Function helps you know when something is, or is potentially, going wrong.

## Continuous Monitoring (DE.CM)

*How do you tell if something is a little off?*

Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events

Continuous monitoring involves the ongoing assessment and analysis of an organization's security posture to identify vulnerabilities, detect potential threats, and ensure the effectiveness of security controls. It encompasses the collection, analysis, and reporting of security-related data from various sources, including system logs, network traffic, and vulnerability scans. By implementing a robust security continuous monitoring program, organizations can proactively identify and respond to emerging threats, monitor the effectiveness of their security measures, and make informed decisions to improve their overall cybersecurity resilience.

### DE.CM Considerations

1. What types of monitoring capabilities do you have?
2. How often are monitoring capabilities reviewed to confirm their effectiveness?
3. Is the physical environment monitored?
4. Do you use behavior analytics software to detect anomalous user activity?
5. How do you align anomalous activity with threat intelligence information?

## Adverse Event Analysis (DE.AE)

*Was that odd or did an incident just occur?*

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents

Adverse Event Analysis encompasses the monitoring and analysis of system activities, logs, and events to identify abnormal behavior and potential security incidents. It involves the collection and analysis of security event data from various sources to detect and respond to cybersecurity events. By effectively monitoring and analyzing anomalies and events, organizations can identify and investigate suspicious activities, promptly respond to security incidents, and improve their overall incident detection and response capabilities.

### DE.AE Considerations

1. How are events analyzed to determine if an incident has occurred?
2. How are potential incidents reported to leadership?
3. How do you ensure information is available, and preserved, for incident responders?
4. How are false positives filtered out?

# Respond

Respond ensures capabilities are in place to address cyber incidents once they are identified. The Respond Function ensures you have a plan to handle incidents before they occur.

## Incident Management (RS.MA)

*Do you know what to do when something goes wrong?*

Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed

Incident Management focuses on the structured handling of detected cybersecurity incidents. Upon the declaration of an incident, the established incident response plan is executed, ensuring coordination with relevant third parties. Incidents undergo a process of triage and validation to ascertain their legitimacy. Following this, incidents are categorized and prioritized based on their severity and potential impact. Depending on the nature and gravity of the incident, it may be escalated or elevated to higher levels of attention. Specific criteria is defined to determine when the transition from incident management to incident recovery should commence.

### RS.MA Considerations

1. Do you have an incident response plan to aid in reacting quickly to cybersecurity incidents?
2. Who is authorized to declare a cyber incident?
3. Who triages cybersecurity events or potential incidents?
4. How are incidents categorized to determine appropriate response activities?
5. Do you know who should be informed and involved in the incident response activities?
6. Who can declare incident response complete?

## Incident Analysis (RS.AN)

*Do you know what really happened?*

Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities

Incident Analysis refers to the systematic examination and evaluation of cybersecurity-related data, information, and events to gain insights into the security posture of an organization. It involves the interpretation and correlation of security logs, incident reports, threat intelligence, and other relevant data sources to identify patterns, trends, and potential vulnerabilities. By conducting thorough analysis, organizations can identify emerging threats, assess the impact of security incidents, and make informed decisions to strengthen their cybersecurity defenses and improve incident response capabilities.

### RS.AN Considerations

1. Do you perform root cause analysis of cyber incidents?
2. How do you determine the magnitude of the incident?
3. Who determines if ‘rules of evidence’ need to be followed to enable forensic analysis post incident?
4. How are incident response activities tracked?

## Incident Response Reporting and Communication (RS.CO)

*When responding to an incident, who do you tell what?*

Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies

Incident Response Reporting and Communication involve the timely and effective exchange of information during cybersecurity incidents. It encompasses establishing clear communication channels, protocols, and procedures to facilitate communication among incident response teams, organizational stakeholders, and external entities. By ensuring efficient response communications, organizations can facilitate collaboration, share critical information, coordinate incident response efforts, and make informed decisions to mitigate the impact of security incidents and minimize the potential damage caused by cyber threats.

### RS.CO Considerations

1. What notifications do you provide during an incident?
2. Do you know who to notify during an incident?
3. What information regarding the incident can be shared publicly?

## Incident Mitigation (RS.MI)

*How will you keep the fire from spreading?*

Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects

Incident Mitigation involves the implementation of measures and controls to reduce or eliminate cybersecurity risks and vulnerabilities. It encompasses the proactive steps taken to address identified weaknesses, including patching systems, reconfiguring networks, updating security policies, and deploying additional security controls. By effectively mitigating cybersecurity risks, organizations can minimize the likelihood and impact of security incidents, protect critical assets, and improve the overall security posture of their systems and networks.

### RS.MI Considerations

1. What immediate steps does your organization take to contain and mitigate the effects of a detected incident?
2. Can you isolate affected workstations / servers to contain an incident?
3. What other technologies are available to you to isolate an incident?
4. How does your organization prioritize mitigation efforts for incidents affecting critical assets or operations?
5. Does your detection and response capability enable eradication capabilities?
6. How does your organization ensure that the lessons learned from incident response are incorporated into preventive measures for the future?

# Recover

Recover defines the processes and capabilities to return business to normal, or the new normal, business operations. This Function ensures you know when business operations are restored, and responders can resume their normal duties.

## Incident Recovery Plan Execution (RC.RP)

*How do you know which business process needs to be recovered first and to what degree?*

Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents

Incident Recovery Plan Execution focuses on the restoration of systems and services impacted by cybersecurity incidents. Upon initiation from the incident response process, the recovery segment of the incident response plan is set into motion. This involves determining, scoping, and prioritizing the necessary recovery actions. Before restoration, the integrity of backups and other assets used for recovery is thoroughly verified. As recovery progresses, there's a consideration of critical mission functions and cybersecurity risk management to establish post-incident operational standards. Once assets are restored, their integrity is confirmed, ensuring systems and services return to their normal operating status. Specific criteria to ascertain the conclusion of the incident recovery phase is defined and all incident-related information is documented.

### RC.RP Considerations

1. How are recovery activities activated?
2. How are systems prioritized for recovery?
3. Is a test plan available to confirm system functionality during recovery?
4. When is recovery complete?
5. How does your organization ensure that lessons learned from the recovery process are documented and communicated to relevant teams for future preparedness?

## Incident Recovery Communication (RC.CO)

*Who can declare the all-clear and when?*

Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties

Recovery communications involve the communication efforts aimed at managing and facilitating the recovery process following a cybersecurity incident. It includes effective communication with stakeholders, employees, customers, and external entities to provide updates on the recovery progress, actions taken, and expected timelines for system and data restoration. By maintaining transparent and timely recovery communications, organizations can instill confidence, manage expectations, and ensure the smooth restoration of systems and services, minimizing the impact on operations and maintaining trust in the aftermath of a cybersecurity incident.

### RC.CO Considerations

1. How are recovery activities communicated internally and externally?
2. Who on the executive team needs to be informed of recovery activities?
3. What types of information regarding recovery can be shared with the public?