NIST Cybersecurity Framework

Translated into Plain English

The NIST Framework to manage and control your cybersecurity threats and attacks is very complex and is not specifically written for a small business. This document translates the NIST Framework into plain English and provides a simple checklist.

This page is a summary only. It does not present our entire product. If you want to see the rest of the material, please sign up today. Our products are language that is clear, precise, and easy to understand.

ID. Identify your assets

1x at Identify all relevant assets.

- Identify the assets that enable you to achieve your business purposes.
- Manage your assets in a way that is consistent with their relative importance.

  - 1x at 1 Identify your physical devices and systems.
  - Inventory the devices that enable you to achieve your business purposes.
  - Inventory the systems that enable you to achieve your business purposes.

  - 1x at 2 Identify your software platforms and applications.
  - Inventory the software platforms that enable you to achieve your business purposes.
  - Inventory the applications that enable you to achieve your business purposes.

  - 1x at 3 Identify your communication and data flows.
  - Inventory the communications that enable you to achieve your business purposes.
  - Identify the data flows that enable you to achieve your business purposes.

  - 1x at 4 Identify your external information systems.
  - Identify the external systems that enable you to achieve business purposes.

  - 1x at 5 Identify your high priority security resources.
  - Identify high priority security facilities that support your organization's purposes.
  - Identify high priority security hardware that supports your organization's purposes.
  - Identify high priority software that supports your organization's purposes.
  - Identify high priority security devices that support your organization's purposes.
  - Identify high priority data that support your organization's purposes.
  - Identify high priority security personnel that support your organization's purposes.

  - 1x at 6 Establish your cybersecurity roles and responsibilities.
  - Identify the cybersecurity jobs that enable you to achieve business purposes.
  - Establish the cybersecurity jobs that enable you to achieve business purposes.
  - Manage the cybersecurity jobs that enable you to achieve business purposes.

1x at Identify business environment.

- Identify and understand your mission, objectives, activities, and stakeholders.
- Use your cybersecurity priorities to help define your approach to cybersecurity.

  - 1x at 1 Identify your place in the critical infrastructure.
  - Identify your place in the supply chain.
  - Understand your organization's role in the supply chain.

  - 1x at 2 Identify how you fit into your infrastructure environment.
  - Identify how your organization's infrastructure fits into your sector infrastructure.
  - Understand how the sector your infrastructure plays in your sector's infrastructure.

  - 1x at 3 Identify your organization's governance cybersecurity priorities.
  - Communicate your organization's infrastructure cybersecurity priorities.
  - Identify your critical functions, services, and mission.
  - Identify your critical dependencies, resources, and dependencies.
  - Communicate your organization's critical functions, services, and dependencies.

  - 1x at 4 Identify your organization's general resilience requirements.
  - Identify your organization's critical service delivery resilience requirements.
  - Prioritize your organization's critical service delivery resilience requirements.
  - Communicate your organization's critical service delivery resilience requirements.

1x at Identify governance framework.

- Identify and understand your organization's approach to governance.
- Use your approach to governance to guide cybersecurity risk management.

  - 1x at 1 Formulate your organization's cybersecurity policy.
  - Establish a cybersecurity policy for your organization.
  - Communicate your organization's cybersecurity policy.

  - 1x at 2 Align your cybersecurity roles and responsibilities.
  - Align internal cybersecurity roles and responsibilities with other functions.
  - Establish cybersecurity roles and responsibilities for partners and other functions.

  - 1x at 3 Understand your legal and regulatory requirements.
  - Understand your organization's legal and regulatory cybersecurity requirements.
  - Manage your organization's legal and regulatory cybersecurity requirements.

  - 1x at 4 Define processes to address your cybersecurity risks.
  - Define a governance process to address your organization's cybersecurity risks.
  - Define a management process to address your organization's cybersecurity risks.

1x at Identify threats and vulnerabilities.

- Identify and understand your organization's cybersecurity risks.
- Use your risk management process to prioritize your risks.

  - 1x at 1 Identify and document your organization's vulnerabilities.
  - Identify and document your organization's vulnerabilities.
  - Establish a vulnerabilities scan and vulnerability assessment process.
  - Manage asset vulnerability assessment risks and responsibilities.
  - Provide how vulnerabilities your organization's assets actually are.
  - Identify and document your organization's asset vulnerabilities.

  - 1x at 2 Gather threat intelligence from external sources.
  - Join information sharing forums that discuss cyber security risks and threats.
  - Review cyber security threat information from your information sharing forums.
  - Discuss and disseminate cyber security alerts, advisories, and warnings.

  - 1x at 3 Define and document your cybersecurity threats.
  - Identify and document your organization's cybersecurity threats.
  - Consider establishing an internal cybersecurity threat program.

  - 1x at 4 Identify potential business impacts and likelihoods.
  - Consider potential security threats and identify potential business impacts.
  - Identify the business impacts and likelihoods that your threats will actually occur.

  - 1x at 5 Use threats and vulnerabilities to determine risks.
  - Consider your organization's security threats and vulnerabilities.
  - Consider information about likelihoods and potential impacts.

  - 1x at 6 Specify and prioritize mechanisms and responses.
  - Specify your organization's risk treatment options and responses.
  - Prioritize your organization's risk treatment options and responses.

1x at Identify risk management strategy.

- Establish your organization's risk management strategy.
- Use your risk management strategy to guide your cybersecurity.

  - 1x at 1 Establish your risk management processes.
  - Establish your organization's risk management processes.
  - Establish your organization's risk management processes.
  - Manage your organization's risk management processes.

  - 1x at 2 Determine your organization's risk tolerance.
  - Determine how much risk your organization is willing to take.
  - Determine how much risk your organization is able to take.
  - Implement and apply risk tolerance levels for each type of risk.

  - 1x at 3 Use your infrastructure's role to guide decisions.
  - Consider how your infrastructure fits into your region's critical infrastructure.
  - Consider how your infrastructure fits into your organization's industrial sector.

1x at Identify strategies for supply Chains.

- Use your risk management strategy to help manage your supply chains.

  - 1x at 1 Develop supply chain risk management processes.
  - Develop your organization's cyber supply chain risk management processes.
  - Establish your organization's cyber supply chain risk management processes.
  - Manage your organization's cyber supply chain risk management processes.

  - 1x at 2 Identify suppliers and assess your supply chain risks.
  - Identify providers of information systems, services, and components.
  - Prioritize providers of information systems, services, and components.
  - Assess providers of information systems, services, and components.

  - 1x at 3 Use security contracts to contract supply chain risks.
  - Use contracts to ensure your cyber security requirements are met by your partners.
  - Use contracts to implement measures to control your cybersecurity risks.

  - 1x at 4 Evaluate the performances of suppliers and partners.
  - Confirm that your suppliers are meeting their contractual obligations.
  - Confirm that third party partners are meeting their contractual obligations.

  - 1x at 5 Conduct response and recovery planning and testing.
  - Carry out suitable incident response and recovery planning activities.
  - Carry out suitable incident response and recovery testing activities.

PR. Protect your assets

1x at Protect assets by managing access.

- Limit access to your assets and facilities.
- Use your access control to protect your assets.

  - 1x at 1 Control identities of users, devices, and processes.
  - Control identities and credentials for authorized users.
  - Control identities and credentials for authorized devices.
  - Control identities and credentials for authorized processes.

  - 1x at 2 Control of physical access to organization's assets.
  - Control physical access to your organization's assets and associated facilities.
  - Control physical access to your organization's assets and critical infrastructure.

  - 1x at 3 Control remote access to organization's assets.
  - Control remote access to your organization's assets and associated facilities.
  - Establish remote access control policies and procedures for your organization.

  - 1x at 4 Control access permissions and authorizations.
  - Control how access permissions and authorizations are managed.
  - Incorporate "separation of duties" and "least privilege" principles.

  - 1x at 5 Control access in networks by segmenting them.
  - Protect and control the integrity of your organization's networks.
  - Segment your organization's networks to protect their integrity and integrity.
  - Consider using network segmentation to control network access and integrity.

  - 1x at 6 Control how identities are proofed and asserted.
  - Control the unique identities of your users, devices, and processes.
  - 1x at 7 Control authentication commensurate with risk.
  - Control authentication of users that have access to physical and logical assets.
  - Control authentication of devices that have access to physical and logical assets.
  - Control authentication of processes that have access to physical and logical assets.

1x at Protect assets by managing awareness.

- Provide cybersecurity awareness services to personnel and partners.
- Provide cybersecurity training services to personnel and partners.

  - 1x at 1 Make users aware of their duties.
  - Provide cybersecurity awareness services to your organization's users.
  - Provide cybersecurity training services to your organization's users.

  - 1x at 2 Make privileged users aware of their duties.
  - Provide cybersecurity awareness services to all privileged users.
  - Provide cybersecurity training services to all privileged users.

  - 1x at 3 Make your stakeholders aware of their duties.
  - Make sure third party stakeholders understand their cybersecurity obligations.

  - 1x at 4 Make senior executives aware of their duties.
  - Make sure that your senior executives understand their cybersecurity functions.

  - 1x at 5 Make security people aware of their duties.
  - Make sure that physical security personnel understand their roles and responsibilities.
  - Make sure that cybersecurity personnel understand their roles and responsibilities.

1x at Protect assets by managing data security.

- Protect your data in accordance with the importance of your organization's data.

  - 1x at 1 Protect your data-at-rest.
  - Protect the confidentiality, integrity, and availability of your data-at-rest.

  - 1x at 2 Protect and preserve data-in-transit.
  - Protect the confidentiality, integrity, and availability of your data-in-transit.

  - 1x at 3 Manage asset transfers and disposals.
  - Manage assets throughout transfer, removal, and disposition.

  - 1x at 4 Ensure data is available when needed.
  - Protect the availability of your data by maintaining adequate capacity.

  - 1x at 5 Prevent data leaks, spills, and mishandling.
  - Protect the confidentiality of data by preventing data leaks.

  - 1x at 6 Check the integrity of your hardware.
  - Use integrity checking mechanisms to verify the integrity of software.
  - Use integrity checking mechanisms to verify the integrity of firmware.
  - Use integrity checking mechanisms to verify the integrity of hardware.

  - 1x at 7 Compartmentalize development activities.
  - Keep development environments separate from production environments.
  - Control access to development, testing, and production environments.

  - 1x at 8 Protect the integrity of hardware platforms.
  - Protect the integrity of your hardware platforms and guidelines.
  - Control and control access to hardware platforms and integrity mechanisms tools.

1x at Protect assets by managing information.

- Establish security policies to protect information systems and assets.
- Implement information security policies, processes, and procedures.

  - 1x at 1 Adopt security principles and create baselines.
  - Incorporate generally accepted security principles into your systems.
  - Establish baseline configurations of industrial control systems and technologies.

  - 1x at 2 Use a system development life cycle.
  - Use System Development Life Cycle Models to manage your system.

  - 1x at 3 Create configuration change control processes.
  - Establish configuration change control processes and procedures.
  - Use these processes and procedures to control systems change.

  - 1x at 4 Conduct regular backups of your information.
  - Establish a policy to control how backups are handled.
  - Make regular backup copies in accordance with your policy.
  - Maintain your organization's backups in a secure location.

  - 1x at 5 Comply with your organization's policies.
  - Comply with policies that affect your physical operating environment.
  - Comply with regulations that affect your physical operating environment.

  - 1x at 6 Develop an appropriate data destruction policy.
  - Establish a policy to manage and control data destruction.
  - Comply with your organization's data destruction policy.

  - 1x at 7 Verify that all data has been destroyed before you reuse media.
  - Verify that all data has been destroyed before reuse.

1x at Protect assets by maintaining information protection processes.

- Improve your organization's information protection processes.

  - 1x at 1 Maintain information protection technologies.
  - Share information about the effectiveness of your protection technologies.

  - 1x at 2 Establish incident response and recovery plans.
  - Establish incident response and business continuity plans.
  - Establish incident recovery and business restoration plan.

  - 1x at 3 Develop incident response and recovery plans.
  - Test your incident response and business continuity plans.
  - Test your incident recovery and business restoration plans.

  - 1x at 4 Develop cybersecurity plans and procedures.
  - Develop a cybersecurity strategy and program.
  - Develop a cybersecurity vulnerability management plan.

  - 1x at 5 Include cybersecurity management plan.
  - Develop a cybersecurity vulnerability management plan.
  - Implement cybersecurity vulnerability management plan.

1x at Protect assets by managing maintenance.

- Use your maintenance programs to protect your control systems.
- Maintain and repair your organization's information system components.

  - 1x at 1 Control repair and maintenance of your assets.
  - Control the maintenance and repair of your organizational assets.
  - Control your repair and maintenance tools and technologies.

  - 1x at 2 Control remote repair and maintenance activities.
  - Establish remote maintenance and repair policies, plans, and procedures.

1x at Protect assets by managing technologies.

- Use technologies to protect the security and resilience of your systems and assets.

  - 1x at 1 Control your organization's removable media.
  - Prevent access to portable and removable media.
  - Control access to portable and removable media.

  - 1x at 2 Protect removable media and control how it is used.
  - Prevent the unauthorized use of unscrutinized use of removable media.

  - 1x at 3 Configure systems to provide only essential capabilities.
  - Configure your systems so that only essential capabilities are provided.

  - 1x at 4 Safeguard your communications and control networks.
  - Protect your organization's communications and control networks.
  - Protect your organization's communications and control networks.

  - 1x at 5 Protect your control systems and technologies.
  - Protect your control systems and technologies in normal situations.
  - Implement measures to meet resilience requirements in adverse situations.

DE. Detect your anomalies

1x at Detect anomalies by analyzing events.

- Use detection technologies to identify anomalies and events.
- Understand the impact that anomalies and events could have.

  - 1x at 1 Establish baselines for network users and systems.
  - Establish baselines of network operations and expected data flows.
  - Manage baselines of network operations and expected data flows.

  - 1x at 2 Analyze detected events to understand their impact.
  - Analyze detected events to understand their impact on your security.

  - 1x at 3 Collect and correlate event data from many sources.
  - Allocate responsibility for collecting and correlating event data.

  - 1x at 4 Determine the impact mishaps events could have.
  - Allocate responsibility for determining the impact mishaps events could have.

  - 1x at 5 Configure cybersecurity incident alert thresholds.
  - Establish incident alert thresholds for all relevant sources and servers.

1x at Detect anomalies by monitoring systems.

- Establish ways of monitoring your assets and information systems.
- Continuously monitor your organization's assets and information systems.

  - 1x at 1 Monitor your assets and systems by monitoring networks.
  - Establish your organization's network monitoring strategy and program.
  - Establish your organization's network monitoring strategy and program.

  - 1x at 2 Detect physical and cybersecurity by monitoring environment.
  - Detect cybersecurity events and anomalies by monitoring your physical environment.

  - 1x at 3 Detect events and anomalies by monitoring staff processes.
  - Detect internal cybersecurity events by monitoring personnel activity.
  - Detect external cybersecurity events by monitoring personnel activity.

  - 1x at 4 Detect and contain malicious code by monitoring systems.
  - Detect malicious code by continuously monitoring your information systems and assets.
  - Contain malicious code by continuously monitoring your information systems and updates are available.

  - 1x at 5 Detect unauthorized mobile code and unauthorized code.
  - Detect unauthorized mobile code by continuously monitoring your systems.
  - Detect unauthorized code by continuously monitoring your systems.

  - 1x at 6 Detect cybersecurity events by monitoring your suppliers.
  - Develop a continuous monitoring strategy and program for external service providers.
  - Establish cybersecurity responsibilities and requirements for external service providers.
  - Detect potential cybersecurity events by monitoring external service provider activity.
  - Detect unauthorized personnel by monitoring external providers.

  - 1x at 7 Monitor your organization's computing and networking environments.
  - Develop a continuous monitoring strategy and program for internal service providers.
  - Detect potential cybersecurity events and anomalies by monitoring internal activity.

1x at Detect anomalies by performing vulnerability scans.

- Develop a continuous monitoring strategy and programs to detect vulnerabilities.
- Detect cybersecurity vulnerabilities and weaknesses by monitoring your systems.

1x at Detect anomalies by maintaining processes.

- Establish your organization's detection processes and procedures.
- Maintain continuous event detection and anomalous processes.

  - 1x at 1 Define clear detection roles and responsibilities.
  - Establish accountability for detecting anomalous cybersecurity events.

  - 1x at 2 Establish detection activities that meet requirements.
  - Establish anomalous event detection activities that comply with requirements.

  - 1x at 3 Test your anomaly detection processes and procedures.
  - Establish and maintain processes to detect anomalous events.
  - Establish and maintain procedures to detect anomalous events.

  - 1x at 4 Communicate anomalous event detection information.
  - Communicate information about your anomaly detection activities and events.

  - 1x at 5 Improve your detection processes and procedures.
  - Continuously improve your anomaly detection processes and procedures.
  - Use what you learn to improve your anomaly detection and procedures.

RS. Respond to incidents

1x at Respond to incidents by controlling steps.

- Establish your organization's incident response processes and procedures.
- Establish your organization's business continuity processes and procedures.

  - 1x at 1 Execute your organization's incident response plan.
  - Execute your organization's response plans while incidents are happening.
  - Execute your organization's continuity plan when incidents have occurred.

1x at Respond to incidents by coordinating with others.

- Manage your relationships with your partners and others.

  - 1x at 1 Confirm that incident responders know their roles.
  - Confirm that responders know what to do when a timely response is needed.

  - 1x at 2 Report incidents in accordance with reporting criteria.
  - Establish criteria to control how cybersecurity incidents are reported.
  - Follow established criteria when you report cybersecurity incidents.

  - 1x at 3 Comply with response plans when sharing information.
  - Follow established incident response plans when sharing information internally.
  - Follow established incident response plans when sharing information externally.

  - 1x at 4 Coordinate all response activities with your stakeholders.
  - Follow incident response plans when coordinating response with internal stakeholders.
  - Follow incident response plans when coordinating response with external stakeholders.

  - 1x at 5 Share resources by sharing information with organizations.
  - Share cybersecurity awareness by voluntarily sharing information about incidents.

1x at Respond to incidents by analyzing the situation.

- Assign responsibility for analyzing cybersecurity events and incidents.
- Analyze the cybersecurity events and incidents that are being detected.

  - 1x at 1 Notify your organization's incident response teams.
  - Assign responsibility for investigating notifications coming from intrusion detection systems.
  - Investigate and analyze incidents and events that from an impact on your organization.

  - 1x at 2 Review and understand the potential impact that cybersecurity incidents could have.
  - Review and understand the potential impact that cybersecurity incidents could have.

  - 1x at 3 Examine cybersecurity incidents and gather forensic evidence.
  - Assign responsibility for examining incidents and gathering investigation evidence.
  - Examine cybersecurity incidents and events and carry out forensic investigations.

  - 1x at 4 Classify your cybersecurity incidents and events.
  - Assign responsibility for using incident response plans to categorize incidents.
  - Create a process for recognizing, differentiating, and categorizing your incidents.
  - Use categories, criteria and incident response plans to classify your incidents.

  - 1x at 5 Set up processes to handle information about vulnerabilities.
  - Assign responsibility for managing information about cybersecurity vulnerabilities.
  - Establish processes to manage information about cybersecurity vulnerabilities.

1x at Respond to incidents by mitigating the situation.

- Assign responsibility for contained, mitigating, and handling cybersecurity incidents.
- Prevent the expansion of cybersecurity events and contain cybersecurity incidents.

  - Mitigate the harm cybersecurity events cause and resolve cybersecurity incidents.

  - 1x at 1 Carry out activities to contain your cybersecurity incidents.
  - Assign responsibility for containing the harm that cybersecurity incidents can cause.
  - Carry out activities to contain cybersecurity incidents and limit the harm they cause.

  - 1x at 2 Mitigate the harm that cybersecurity incidents cause.
  - Carry out activities to mitigate harm that cybersecurity incidents cause.
  - Carry out activities to mitigate harm that the damage from cyber attacks.

  - 1x at 3 Assess new vulnerabilities and decide how to handle them.
  - Assign responsibility for investigating and mitigating new vulnerabilities.
  - Manage how to investigate new vulnerabilities and mitigate your security risks.

1x at Respond to incidents by making improvements.

- Improve your organization's incident response by improving lessons learned.
- Improve your organization's response by improving business continuity activities.

  - 1x at 1 Improve your incident response by improving lessons learned.
  - Use lessons learned to improve your organization's incident response plans.
  - Use lessons learned to improve your organization's business continuity plans.

  - 1x at 2 Use lessons to update response and recovery strategies.
  - Use lessons learned to improve your organization's incident response strategies.
  - Use lessons learned to improve your organization's business continuity strategies.

RC. Recover from incidents

1x at Recover from incidents by controlling steps.

- Establish your organization's incident recovery processes and procedures.
- Establish your organization's business restoration processes and procedures.

  - 1x at 1 Execute recovery plans whenever incidents occur.
  - Execute your organization's incident recovery plan when incidents are happening.
  - Execute your organization's restoration plan when incidents have occurred.

1x at Recover from incidents by making improvements.

- Improve your cybersecurity incidents by improving recovery activities.
- Recover from cybersecurity incidents by improving restoration activities.

  - 1x at 1 Use lessons learned to improve your organization's incident recovery plans.
  - Use lessons learned to improve your organization's incident recovery plans.

  - 1x at 2 Use lessons to update recovery and restoration strategies.
  - Use lessons learned to improve your organization's incident recovery strategies.
  - Use lessons learned to improve your organization's restoration strategies.

1x at Recover from incidents by coordinating activities.

- Coordinate your organization's recovery activities with interested parties.
- Coordinate your organization's restoration activities with interested parties.

  - 1x at 1 Manage public relations and communicate carefully.
  - Assign responsibility for managing your organization's cybersecurity public relations.
  - Manage your organization's cybersecurity public relations and communications.

  - 1x at 2 Repair your organization's reputation after incidents.
  - Repair your organization's reputation after incidents have occurred.

  - 1x at 3 Share information about your recovery activities.
  - Share information about recovery activities with your stakeholders.

This page is a summary only. It does not present our entire product. If you want to see the rest of the material, please sign up today. Our products are language that is clear, precise, and easy to understand.

Prescium Research Group Limited
First Edmonton Place 14 Floor 10665 Jasper Ave
Edmonton, Alberta, Canada, T5J 3B1 (780-461-4114)
info@prescium.com info@prescium.org prescium@gmail.com
We ship worldwide. Our products are available in over 100 countries.

©2021 Prescium Research Group Limited. All Rights Reserved.