Plain English Structure of NIST Cybersecurity Framework

Use NIST's Framework to manage and control your cybersecurity threats and attacks. Use it to protect your organization's critical infrastructure and to safeguard the health, safety, security, and privacy of its customers, employees, and other interested parties.

This page is a summary only. It does not present our entire product.
If you would like to see the rest of this material, please place an order.
Our products use language that is clear, precise, and easy to understand.

ID. Identify your context

- ID.AM Identify all relevant assets.
  - ID.AM-1 Identify your physical devices and systems.
  - ID.AM-2 Identify your software platforms and apps.
  - ID.AM-3 Identify your communication and data flows.
  - ID.AM-4 Identify your external information systems.
  - ID.AM-5 Identify your high priority security resources.
  - ID.AM-6 Identify your security roles and responsibilities.
- ID.BE Identify business environment.
  - ID.BE-1 Clarify your organization's role in overall supply chain.
  - ID.BE-2 Clarify how you fit into your infrastructure environment.
  - ID.BE-3 Clarify your organization's general cybersecurity priorities.
  - ID.BE-4 Clarify your critical functions, services, and dependencies.
  - ID.BE-5 Clarify your organization's general resilience requirements.
- ID.GV Identify governance framework.
  - ID.GV-1 Formulate your organization's cybersecurity policy.
  - ID.GV-2 Align your cybersecurity roles and responsibilities.
  - ID.GV-3 Understand your legal and regulatory requirements.
  - ID.GV-4 Define processes to address your cybersecurity risks.
- ID.RA Identify threats and vulnerabilities.
  - ID.RA-1 Identify and document your asset vulnerabilities.
  - ID.RA-2 Gather threat intelligence from external sources.
  - ID.RA-3 Define and document your cybersecurity threats.
  - ID.RA-4 Clarify potential business impacts and likelihoods.
  - ID.RA-5 Use threats and vulnerabilities to determine risk.
  - ID.RA-6 Specify and prioritize treatments and responses.
- ID.RM Identify risk management strategy.
  - ID.RM-1 Establish your risk management processes.
  - ID.RM-2 Determine your organization's risk tolerances.
  - ID.RM-3 Use your infrastructure's role to guide decisions.
- ID.SC Identify strategy for supply chains.
  - ID.SC-1 Develop supply chain risk management processes.
  - ID.SC-2 Identify suppliers and assess your supply chain risks.
  - ID.SC-3 Use security contracts to control supply chain risks.
  - ID.SC-4 Evaluate the performance of suppliers and partners.
  - ID.SC-5 Conduct response and recovery planning and testing.

PR. Protect your assets

- PR.AC Protect assets by managing access.
  - PR.AC-1 Control identity of users, devices, and processes.
  - PR.AC-2 Control physical access to organization's assets.
  - PR.AC-3 Control remote access to organization's assets.
  - PR.AC-4 Control access permissions and authorizations.
  - PR.AC-5 Control access to networks by separating them.
  - PR.AC-6 Control how identities are proofed and asserted.
  - PR.AC-7 Control authentication commensurate with risk.
- PR.AT Protect assets by managing awareness.
  - PR.AT-1 Make users aware of their security duties.
  - PR.AT-2 Make privileged users aware of their duties.
  - PR.AT-3 Make your stakeholders aware of their duties.
  - PR.AT-4 Make senior executives aware of their duties.
  - PR.AT-5 Make security people aware of their duties.
- PR.DS Protect assets by managing data security.
  - PR.DS-1 Protect and preserve data-at-rest.
  - PR.DS-2 Secure and preserve data-in-transit.
  - PR.DS-3 Manage asset transfers and disposals.
  - PR.DS-4 Ensure data is available when needed.
  - PR.DS-5 Prevent data leaks, spills, and breaches.
  - PR.DS-6 Verify the integrity of data and software.
  - PR.DS-7 Compartmentalize development activities.
  - PR.DS-8 Check the integrity of all hardware systems.
- PR.IP Protect assets by managing information.
  - PR.IP-1 Adopt security principles and create baselines.
  - PR.IP-2 Use life cycle models to manage your systems.
  - PR.IP-3 Create configuration change control processes.
  - PR.IP-4 Conduct regular backups of your information.
  - PR.IP-5 Control your physical operating environment.
  - PR.IP-6 Develop an appropriate data destruction policy.
  - PR.IP-7 Improve your information protection processes.
  - PR.IP-8 Share information about protection technologies.
  - PR.IP-9 Establish incident response and recovery plan.
  - PR.IP-10 Evaluate incident response and recovery plan.
  - PR.IP-11 Build security into human resource practices.
  - PR.IP-12 Formulate vulnerability management plan.
- PR.MA Protect assets by managing maintenance.
  - PR.MA-1 Control repair and maintenance of your assets.
  - PR.MA-2 Control remote repair and maintenance activities.
- PR.PT Protect assets by managing technologies.
  - PR.PT-1 Establish audit logs to record user events and faults.
  - PR.PT-2 Protect removable media and restrict how it is used.
  - PR.PT-3 Configure systems to provide only essential capabilities.
  - PR.PT-4 Safeguard your communications and control networks.
  - PR.PT-5 Implement measures to meet resilience requirements.

DE. Detect your anomalies

- DE.AE Detect anomalies by analyzing events.
  - DE.AE-1 Establish baselines for network users and systems.
  - DE.AE-2 Analyze events to understand targets and methods.
  - DE.AE-3 Collect and correlate event data from many sources.
  - DE.AE-4 Determine the impact malicious events could have.
  - DE.AE-5 Configure cybersecurity incident alert thresholds.
- DE.CM Detect anomalies by monitoring systems.
  - DE.CM-1 Detect events and anomalies by monitoring networks.
  - DE.CM-2 Detect events and anomalies by monitoring environment.
  - DE.CM-3 Detect events and anomalies by monitoring all personnel.
  - DE.CM-4 Detect and contain malicious code by monitoring systems.
  - DE.CM-5 Detect unauthorized mobile code by monitoring activities.
  - DE.CM-6 Detect cybersecurity events by monitoring your suppliers.
  - DE.CM-7 Detect unauthorized devices, software, and connections.
  - DE.CM-8 Detect weaknesses by performing vulnerability scans.
- DE.DP Detect anomalies by maintaining processes.
  - DE.DP-1 Define clear detection roles and responsibilities.
  - DE.DP-2 Establish detection activities that meet requirements.
  - DE.DP-3 Test your anomaly detection processes and procedures.
  - DE.DP-4 Communicate anomalous event detection information.
  - DE.DP-5 Improve your detection processes and procedures.

RS. Respond to incidents

- RS.RP Respond to incidents by controlling steps.
  - RS.RP-1 Execute your organization's incident response plans.
- RS.CO Respond to incidents by coordinating action.
  - RS.CO-1 Confirm that incident responders know their roles.
  - RS.CO-2 Report incidents in accordance with reporting criteria.
  - RS.CO-3 Comply with response plans when sharing information.
  - RS.CO-4 Coordinate all response activities with your stakeholders.
  - RS.CO-5 Raise awareness by sharing information with stakeholders.
- RS.AN Respond to incidents by analyzing the situation.
  - RS.AN-1 Investigate notifications received from detection systems.
  - RS.AN-2 Review and understand the impact of cybersecurity incidents.
  - RS.AN-3 Examine cybersecurity incidents and gather forensic evidence.
  - RS.AN-4 Classify cybersecurity incidents consistent with response plans.
  - RS.AN-5 Set up processes to handle information about vulnerabilities.
- RS.MI Respond to incidents by mitigating the damage.
  - RS.MI-1 Carry out activities to contain your cybersecurity incidents.
  - RS.MI-2 Mitigate the damage that cybersecurity incidents can cause.
  - RS.MI-3 Assess new vulnerabilities and decide how to handle them.
- RS.IM Respond to incidents by making improvements.
  - RS.IM-1 Use lessons to improve response and continuity plans.
  - RS.IM-2 Use lessons to update response and continuity strategies.

RC. Recover from incidents

- RC.RP Recover from incidents by controlling steps.
  - RC.RP-1 Execute recovery plans whenever incidents occur.
- RC.IM Recover from incidents by making improvements.
  - RC.IM-1 Use lessons to improve recovery and restoration plans.
  - RC.IM-2 Use lessons to update recovery and restoration strategies.
- RC.CO Recover from incidents by coordinating activities.
  - RC.CO-1 Manage public relations and communicate externally.
  - RC.CO-2 Repair your organization's reputation after incidents.
  - RC.CO-3 Share information about your recovery activities.

This page is a summary only. It does not present our entire product.
If you would like to see the rest of this material, please place an order.
Our products use language that is clear, precise, and easy to understand.

Praxiom Research Group Limited
First Edmonton Place 14 Floor 10665 Jasper Ave
Edmonton, Alberta, Canada, T5J 3S9 780-461-4514
info@praxiom.com info@praxiom.org praxiom@gmail.com
We ship worldwide. Our products are used in over 100 countries.