PR. Protect your assets
ID. Identify your context
RS. Risk Management

- Maintain and repair your organization's information system components.
- Establish security policies to protect information systems and assets.
- Provide cybersecurity awareness services to personnel and partners.
- Recover from incidents by coordinating activities.
- Recover from incidents by controlling steps.
- Respond to incidents by making improvements.
- Respond to incidents by mitigating the damage.

Identify risk management strategy.

Use NIST's Framework to manage and control your cybersecurity threats and attacks.

PR. Protect your assets
PR.IP-1
PR.DS-8
PR.AT-1
PR.AC-7
ID.SC-2
ID.RA
ID.RA
ID.RA
ID.BE-4
RS.IM-2
RS.IM-1
RS.MI-3
RS.AN-1
RS.CO-2
DE.DP-4
DE.DP-1
DE.CM-8

- Share information about recovery activities with your stakeholders.
- Repair your organization's reputation after incidents have occurred.
- Assign responsibility for managing your organization's cybersecurity public relations.
- Carry out activities to mitigate incidents and limit the damage they cause.
- Assign responsibility for mitigating the damage that incidents can cause.
- Assign responsibility for managing information about cybersecurity vulnerabilities.
- Assign responsibility for using incident response plans to categorize incidents.
- Examine cybersecurity incidents and events and carry out forensic investigations.
- Assign responsibility for reviewing the impact that cybersecurity incidents could have.
- Raise cybersecurity awareness by voluntarily sharing information about incidents.
- Follow established incident response plans when sharing information internally.
- Execute your organization's continuity plans after incidents have occurred.
- Evaluate your organization's anomaly detection processes and procedures.
- Establish and maintain procedures to detect anomalous events.
- Detect cybersecurity events and anomalies by monitoring your physical environment.
- Implement your organization's network monitoring strategy and program.
- Protect your organization's communications and control networks.
- Prevent the unauthorized and uncontrolled use of removable media.
- Establish controls to protect audit log information and facilities.
- Formulate a policy to control the use of audit logs and records.
- Comply with policies that affect your physical operating environment.
- Use integrity checking mechanisms to verify the integrity of firmware.
- Use integrity checking mechanisms to verify the integrity of software.
- Make sure that third-party stakeholders understand their cybersecurity obligations.
- Provide cybersecurity awareness services to all privileged users.
- Control authentication of processes that have access to physical and logical assets.
- Control identities and credentials for authorized processes.
- Document your organization's risk tolerance for each type of risk.
- Define a management process to address your organization's cybersecurity risks.
- Manage your organization's legal and regulatory cybersecurity requirements.
- Establish a cybersecurity policy for your organization.
- Prioritize your organization's critical service delivery resilience requirements.
- Understand your organization's role in the supply chain.
- Identify your organization's role in the supply chain.
- Identify high priority security personnel that support your organization's purpose.
- Identify high priority security data that support your organization's purpose.
- Identify high priority security hardware that supports your organization's purpose.
- Identify the data flows that enable you to achieve your business purposes.
- Use contracts to implement measures to control your cybersecurity risks.
- Manage the cybersecurity jobs that enable you to achieve business purposes.
- Consider using network segmentation to control network access and integrity.
- Use security contracts to control supply chain risks.
- Develop supply chain risk management processes.
- Align your cybersecurity roles and responsibilities.
- Clarify your organization's role in overall supply chain.
- Identify your high priority security resources.
- Identify your communication and data flows.
- Use threats and vulnerabilities to determine risk.
- Gather threat intelligence from external sources.
- Evaluate incident response and recovery plans.