safety, security, and privacy of its customers, employees, and other interested parties.

- **RC. Recover from incidents**
- **RS. Respond to incidents**
- **PR. Protect your assets**

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

- **RS.RP**
- **RS.MI**
- **RS.AN**

Recover from incidents by controlling steps.

Respond to incidents by making improvements.

Respond to incidents by coordinating action.

Respond to incidents by controlling steps.

Detect anomalies by monitoring systems.

Protect assets by managing technologies.

Protect assets by managing maintenance.

Protect assets by managing information.

Identify risk management strategy.

Identify threats and vulnerabilities.

Identify business environment.

Implement measures to meet resilience requirements.

Configure systems to provide only essential capabilities.

Protect removable media and restrict how it is used.

Control remote repair and maintenance activities.

Establish incident response and recovery plan.

Develop an appropriate data destruction policy.

Conduct regular backups of your information.

Use life cycle models to manage your systems.

Adopt security principles and create baselines.

Check the integrity of all hardware systems.

Prevent data leaks, spills, and breaches.

Ensure data is available when needed.

Manage asset transfers and disposals.

Make your stakeholders aware of their duties.

Make privileged users aware of their duties.

Make users aware of their security duties.

Control authentication commensurate with risk.

Control access to networks by separating them.

Control access permissions and authorizations.

Control physical access to organization's assets.

Control identity of users, devices, and processes.

Use security contracts to control supply chain risks.

Identify suppliers and assess your supply chain risks.

Use your infrastructure's role to guide decisions.

Determine your organization's risk tolerances.

Identify your external information systems.

Identify your communication and data flows.

Identify your software platforms and apps.

Identify your physical devices and systems.

Clarify potential business impacts and likelihoods.

Define and document your cybersecurity threats.

Gather threat intelligence from external sources.

Share information about your recovery activities.

Manage public relations and communicate externally.

Use lessons to improve recovery and restoration plans.

Execute recovery plans whenever incidents occur.

Use lessons to update response and continuity strategies.

Assess new vulnerabilities and decide how to handle them.

Carry out activities to contain your cybersecurity incidents.

Classify cybersecurity incidents consistent with response plans.

Examine cybersecurity incidents and gather forensic evidence.

Investigate notifications received from detection systems.

Raise awareness by sharing information with stakeholders.

Coordinate all response activities with your stakeholders.

Comply with response plans when sharing information.

Report incidents in accordance with reporting criteria.

Execute your organization's incident response plans.

Communicate anomalous event detection information.

Detect weaknesses by performing vulnerability scans.

Detect cybersecurity events by monitoring your suppliers.

Detect and contain malicious code by monitoring systems.

Detect events and anomalies by monitoring all personnel.

Detect events and anomalies by monitoring environment.

Configure cybersecurity incident alert thresholds.

Formulate vulnerability management plan.

Evaluate incident response and recovery plan.