#	NIST CSF Policies	Description
Identify Function		
1.	Asset Management	To describe the activities required to perform Asset Management (e.g. identify and manage business purposes).
2.	Business Environment	To describe the organizational cyber security roles and risk management decisions.
3.	Governance	To establish organizational policies, processes, and procedures for information security and risk management.
4.	Risk Assessment	To identify the organizational asset vulnerabilities and cybersecurity risk to operations.
5.	Risk Management Strategy	To describe organizational risk tolerance and established operational risk decisions.
Protect Function		
6.	Access Control	To provide management for limited access to facilities and organization assets.
7.	Awareness and Training	To provide cyber security awareness and training to organizational personnel covering their jobs and responsibilities.
8.	Data Security	To provide risk strategy to ensure the confidentiality, integrity, and availability (CIA) of information assets.
9.	Information Protection Processes and Procedures	To maintain policies, processes, and procedures to manage protection of information systems and assets.
10.	Maintenance	To maintain policies and procedures for the maintenance and repairs of organizational assets.
11.	Protective Technology	To provide technical security solutions to ensure the security and protection of systems and organizational assets.
Detect Function		
12.	Anomalies and Events	To ensure detection of anomalous activities and events in a timely manner.
13.	Security Continuous Monitoring	To ensure monitoring of the physical environment and information system and assets at discrete intervals to identify cybersecurity events.

#	NIST CSF Policies	Description
14.	Detection Processes	To provide awareness on anomalous events and test detection activities.
Respond Function		
15.	Response Planning	To maintain a response plan to ensure timely response to detected cybersecurity events.
16.	Communications	To coordinate response activities with stakeholders consistently to achieve broader cybersecurity situational awareness.
17.	Analysis	To conduct analysis to understand response and recovery activities.
18.	Mitigation	To perform activities to mitigate incident and newly identified vulnerabilities.
19.	Improvements	To improve the response plan by incorporating lessons learned from all response activities.
Recover Function		
20.	Recovery Planning	To ensure timely restoration of systems or assets affected by cybersecurity events.
21.	Improvements	To improve recovery planning and processes by incorporating lessons learned.
22.	Communications	To communicate recovery activities to internal stakeholders and repair the reputation after an event.