



# Nova Network Security NIST Cyber Security Framework

## NIST Cybersecurity Framework

Function	Category	
IDENTIFY (ID)	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	
	<b>Business Environment (ID.BE):</b> The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	<b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
PROTECT (PR)	<b>Access Control (PR.AC):</b> Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	
	<b>Awareness and Training (PR.AT):</b> The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	<b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
DETECT (DE)	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected in a timely manner and the potential impact of events is understood.	Nova Impact
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	
RESPOND (RS)	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure adequate response and support recovery activities.	
	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	
RECOVER (RC)	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	<b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	