Active Cyber Defense

NIST Cybersecurity Framework

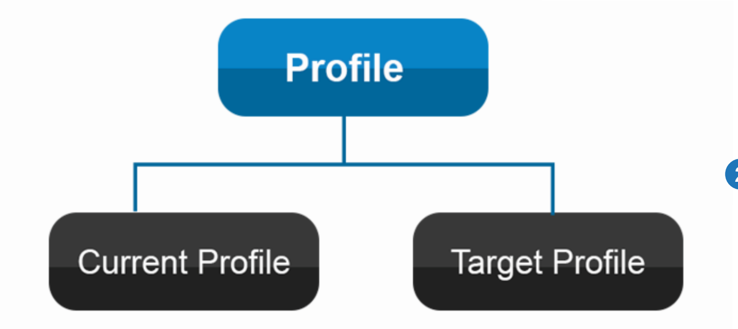
Framework Functions

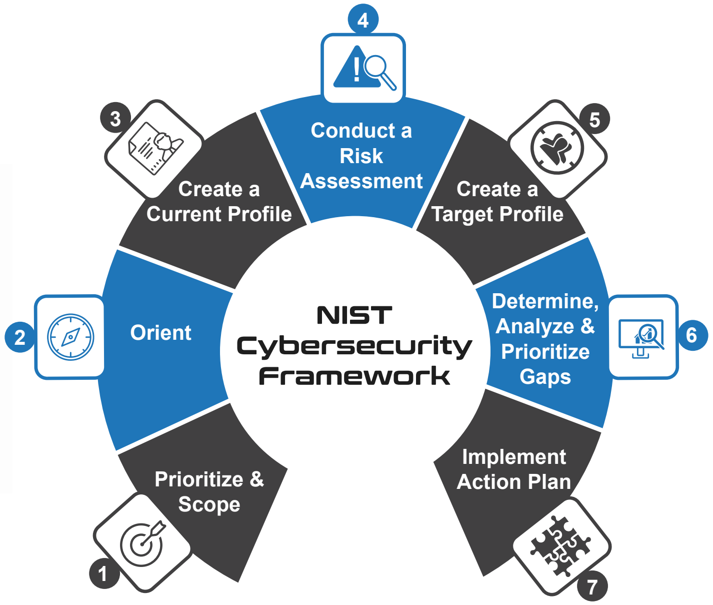
IDENTIFY	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
PROTECT	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
DETECT	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
RESPOND	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
RECOVER	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES

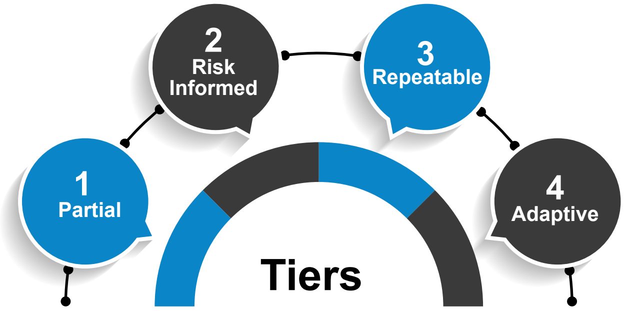
NIST Cybersecurity Framework key facts

5	Functions
23	Categories
108	Sub-Categories
4	Tiers
2	Profiles

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identify Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications







Cyber Resilience In the 2020s

Uday Ali Pabrai

Global Cybersecurity & Compliance Expert

Active Cyber Defense

NIST Cybersecurity Framework

1 Identify Function

Function	Category	Sub-Category	# of Sub-Category
Identify (ID)	Asset Management (ID.AM)	Physical devices and systems within the organization are inventoried. (ID-AM 1)	6
		Software platforms and applications within the organization are inventoried. (ID.AM-2)	
		Organizational communication and data flows are mapped. (ID.AM-3)	
		External information systems are catalogued. (ID.AM-4)	
		Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value. (ID.AM-5)	
		Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. (ID.AM-6)	
	Business Environment (ID.BE)	The organization's role in the supply chain is identified and communicated. (ID.BE-1)	5
		The organization's place in critical infrastructure and its industry sector is identified and communicated. (ID.BE-2)	
		Priorities for organizational mission, objectives, and activities are established and communicated. (ID.BE-3)	
		Dependencies and critical functions for delivery of critical services are established. (ID.BE-4)	
		Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations). (ID.BE-5)	
	Governance (ID.GV)	Organizational cybersecurity policy is established and communicated. (ID.GV-1)	4
		Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. (ID.GV-2)	
		Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. (ID.GV-3)	
		Governance and risk management processes address cybersecurity risks. (ID.GV-4)	
	Risk Assessment (ID.RA)	Asset vulnerabilities are identified and documented. (ID.RA-1)	6
		Cyber threat intelligence is received from information sharing forums and sources. (ID.RA-2)	
		Threats, both internal and external, are identified and documented. (ID.RA-3)	
		Potential business impacts and likelihoods are identified. (ID.RA-4)	
		Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. (ID.RA-5)	
		Risk responses are identified and Prioritized. (ID.RA-6)	
	Risk Management Strategy (ID.RM)	Risk management processes are established, managed, and agreed to by organizational stakeholders. (ID.RM-1)	3
		Organizational risk tolerance is determined and clearly expressed. (ID.RM-2)	
		The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis. (ID.RM-3)	
	Supply Chain Risk Management (ID.SC)	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. (ID.SC-1)	5
		Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process. (ID.SC-2)	
		Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. (ID.SC-3)	
		Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. (ID.SC-4)	
		Response and recovery planning and testing are conducted with suppliers and third-party providers. (ID.SC-5)	
	6		**29**

ecfirst | ecfirst Academy NIST CMMC CCSA Certified Cyber Security Architect

Cyber Resilience
In the 2020s

Global Cybersecurity & Compliance Expert

Active Cyber Defense

NIST Cybersecurity Framework

2 Protect function

Function	Category	Sub-Category	# of Sub-Category
Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. (PR.AC-1)	7
		Physical access to assets is managed and protected. (PR.AC-2)	
		Remote access is managed. (PR.AC-3)	
		Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. (PR.AC-4)	
		Network integrity is protected (e.g., network segregation, network segmentation). (PR.AC-5)	
		Identities are proofed and bound to credentials and asserted in interactions. (PR.AC-6)	
		Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks). (PR.AC-7)	
	Awareness and Training (PR.AT)	All users are informed and trained. (PR.AT-1)	5
		Privileged users understand their roles and responsibilities. (PR.AT-2)	
		Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities. (PR.AT-3)	
		Senior executives understand their roles and responsibilities. (PR.AT-4)	
		Physical and cybersecurity personnel understand their roles and responsibilities. (PR.AT-5)	
	Data Security (PR.DS)	Data-at-rest is protected. (PR.DS-1)	8
		Data-in-transit is protected. (PR.DS-2)	
		Assets are formally managed throughout removal, transfers, and disposition. (PR.DS-3)	
		Adequate capacity to ensure availability is maintained. (PR.DS-4)	
		Protections against data leaks are implemented. (PR.DS-5)	
		Integrity checking mechanisms are used to verify software, firmware, and information integrity. (PR.DS-6)	
		The development and testing environment(s) are separate from the production environment. (PR.DS-7)	
		Integrity checking mechanisms are used to verify hardware integrity. (PR.DS-8)	
	Information Protection Processes and Procedures (PR.IP)	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality). (PR.IP-1)	12
		A System Development Life Cycle to manage systems is implemented. (PR.IP-2)	
		Configuration change control processes are in place. (PR.IP-3)	
		Backups of information are conducted, maintained, and tested. (PR.IP-4)	
		Policy and regulations regarding the physical operating environment for organizational assets are met. (PR.IP-5)	
		Data is destroyed according to policy. (PR.IP-6)	
		Protection processes are improved. (PR.IP-7)	
		Effectiveness of protection technologies is shared. (PR.IP-8)	
		Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. (PR.IP-9)	
		Response and recovery plans are tested. (PR.IP-10)	
		Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). (PR.IP-11)	
		A vulnerability management plan is developed and implemented. (PR.IP-12)	
	Maintenance (PR.MA)	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. (PR.MA-1)	2
		Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. (PR.MA-2)	
	Protective Technology (PR.PT)	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. (PR.PT-1)	5
		Removable media is protected and its use restricted according to policy. (PR.PT-2)	
		The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. (PR.PT-3)	
		Communications and control networks are protected. (PR.PT-4)	
		Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. (PR.PT-5)	
	6		**39**

Cyber Resilience
In the 2020s

Ali Pabrai

Global Cybersecurity & Compliance Expert

Active Cyber Defense

NIST Cybersecurity Framework

3 Detect Function

Function	Category	Sub-Category	# of Sub-Category
Detect (DE)	Anomalies and Events (DE.AE)	A baseline of network operations and expected data flows for users and systems is established and managed. (DE.AE-1)	5
		Detected events are analyzed to understand attack targets and methods. (DE.AE-2)	
		Event data are collected and correlated from multiple sources and sensors. (DE.AE-3)	
		Impact of events is determined. (DE.AE-4)	
		Incident alert thresholds are established. (DE.AE-5)	
	Security Continuous Monitoring (DE.CM)	The network is monitored to detect potential cybersecurity events. (DE.CM-1)	8
		The physical environment is monitored to detect potential cybersecurity events. (DE.CM-2)	
		Personnel activity is monitored to detect potential cybersecurity events. (DE.CM-3)	
		Malicious code is detected. (DE.CM-4)	
		Unauthorized mobile code is detected. (DE.CM-5)	
		External service provider activity is monitored to detect potential cybersecurity events. (DE.CM-6)	
		Monitoring for unauthorized personnel, connections, devices, and software is performed. (DE.CM-7)	
		Vulnerability scans are performed. (DE.CM-8)	
	Detection Processes (DE.DP)	Roles and responsibilities for detection are well defined to ensure accountability. (DE.DP-1)	5
		Detection activities comply with all applicable requirements. (DE.DP-2)	
		Detection processes are tested. (DE.DP-3)	
		Event detection information is communicated. (DE.DP-4)	
		Detection processes are continuously improved. (DE.DP-5)	
	3		**18**

4 Respond Function

Function	Category	Sub-Category	# of Sub-Category
Respond (RS)	Response Planning (RS.RP)	Response plan is executed during or after an incident. (RS.RP-1)	1
	Communications (RS.CO)	Personnel know their roles and order of operations when a response is needed. (RS.CO-1)	5
		Incidents are reported consistent with established criteria. (RS.CO-2)	
		Information is shared consistent with response plans. (RS.CO-3)	
		Coordination with stakeholders occurs consistent with response plans. (RS.CO-4)	
		Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. (RS.CO-5)	
	Analysis (RS.AN)	Notifications from detection systems are investigated. (RS.AN-1)	5
		The impact of the incident is understood. (RS.AN-2)	
		Forensics are performed. (RS.AN-3)	
		Incidents are categorized consistent with response plans. (RS.AN-4)	
		Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers). (RS.AN-5)	
	Mitigation (RS.MI)	Incidents are contained. (RS.MI-1)	3
		Incidents are mitigated. (RS.MI-2)	
		Newly identified vulnerabilities are mitigated or documented as accepted risks. (RS.MI-3)	
	Improvements (RS.IM)	Response plans incorporate lessons learned. (RS.IM-1)	2
		Response strategies are updated. (RS.IM-2)	
	5		**16**

5 Recover Function

Function	Category	Sub-Category	# of Sub-Category
Recover (RC)	Recovery Planning (RC.RP)	Recovery plan is executed during or after acybersecurity incident. (RC.RP-1)	1
	Improvements (RC.IM)	Recovery plans incorporate lessons learned. (RC.IM-1)	2
		Recovery strategies are updated. (RC.IM-2)	
	Communications (RC.CO)	Public relations are managed. (RC.CO-1)	3
		Reputation is repaired after an incident. (RC.CO-2)	
		Recovery activities are communicated to internal and external stakeholders as well as executive and management teams. (RC.CO-3)	
	3		**6**

ecfirst | ecfirst Academy | NIST | CMMC | CCSA Certified Cyber Security Architect

Cyber Resilience
In the 2020s

Uday Ali Pabrai

Global Cybersecurity & Compliance Expert