NIST Cybersecurity Framework and Tandem Mapping

Introduction

On February 12, 2014, the National Institute of Standards and Technology released the Framework for Improving Critical Infrastructure Cybersecurity. The framework was updated to Version 1.1 in April 2018. The *Framework Core* includes five functions that pertain to cybersecurity risk management. Each function contains multiple categories and subcategories.

Functions			
	Identify		
	Protect		
	Detect		
	Respond		
	Recover		

This mapping is for information purposes only. It serves to identify areas in Tandem where NIST cybersecurity topics are addressed and does not guarantee that a business using the Tandem software meets each NIST standard. However, the Tandem references throughout this document can be used to determine whether your organization's controls and documentation fulfill the corresponding NIST standards.

NIST Category	NIST Subcategory	Tandem References
Identify Asset Management (ID.AM): 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.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	Business Continuity Plan: Systems / Equipment Policies: • IT Asset Management • Network Diagrams
	ID.AM-2: Software platforms and applications within the organization are inventoried	Business Continuity Plan: Software Policies: IT Asset Management
	ID.AM-3: Organizational communication and data flows are mapped	Policies: Network Diagrams Risk Assessment: Information Security Risk Assessment Data Flow
	ID.AM-4: External information systems are catalogued	Business Continuity Plan: • Systems / Equipment • Software Policies: • IT Asset Management • Network Diagrams
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Business Continuity Plan: • Systems / Equipment • Software Risk Assessment: • Data Types • Data Classifications • Information Assets Vendor Management: Services

NIST Category	NIST Subcategory	Tandem References
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	See the Responsibility Reports in the following modules: • Business Continuity Plan • Cybersecurity • Policies • Risk Assessment • Vendor Management Incident Response Plan: Roles & Responsibilities Information Security Program Document Resource
Identify Business Environment (ID.BE): 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.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	Business Continuity Plan: Business Impact Analysis:
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Business Continuity Plan Risk Assessment Considering Critical Infrastructure Knowledge Base Article
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Business Continuity Plan: Policy
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Business Continuity Plan: • Business Impact Analysis • Business Process Dependency Report

NIST Category	NIST Subcategory	Tandem References
	ID.BE-5: Resilience requirements to support delivery of critical services are established	Business Continuity Plan: • Business Impact Analysis • Criticality Levels / Maximum Tolerable Downtimes (MTD) • Recovery Time Objectives (RTOs) • Recovery Point Objectives (RPOs)
Identify Governance (ID.GV): 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.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	Policies
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	See the Responsibility Reports in the following modules: • Business Continuity Plan • Cybersecurity • Policies • Risk Assessment • Vendor Management Incident Response Plan (Roles & Responsibilities)
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Policies: Information Sharing and Regulatory Monitoring
	ID.GV-4: Governance and risk management processes address cybersecurity risks	Risk Assessment: Risk Management Plan

NIST Category	NIST Subcategory	Tandem References
Identify Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	Risk Assessment: • Information Assets • Asset-Based Risk Assessments Policies: • IT Asset Management • Vulnerability and Patch Management Audit Management
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	Policies: Information Sharing and Regulatory Monitoring Risk Assessment: Controls: Information Sharing Forum
	ID.RA-3: Threats, both internal and external, are identified and documented	Risk Assessment: Threats
	ID.RA-4: Potential business impacts and likelihoods are identified	Risk Assessment: • Threat Potential Impacts • BCP Risk Matrix Business Continuity Plan: Business Impact Analysis
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Risk Assessment: Threat Likelihood, Potential Damage, and Risk Addressing Vulnerabilities in the Risk Assessment Knowledge Base Article
	ID.RA-6: Risk responses are identified and prioritized	Risk Assessment: Risk Management Plan
Identify Risk Management Strategy (ID.RM): The organization's	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	Risk Assessment: • Revision/Approval Log • Risk Management Plan

NIST Category	NIST Subcategory	Tandem References
priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed	Cybersecurity Assessment Tool: • Risk Appetite Statement • Target Risk Levels Risk Assessment: Risk Management Plan
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Risk Assessment: Risk Management Plan Considering Critical Infrastructure Knowledge Base Article
Identify Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Policies: • Cloud Computing • Third-Party Secure Application Development • Vendor Management Risk Assessment: • Information Security Risk Assessment Questionnaire • Threats: Supply Chain Attack • Controls: Code Review, Hardware Inspection, Vendor Contract, Vendor Management Program, Vulnerability Scans, etc. Vendor Management
	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a Cyber Supply Chain Risk Assessment process	Vendor Management

NIST Category	NIST Subcategory	Tandem References
	ID.SC-3: 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	Vendor Management Risk Assessment: • Risk Management Plan • Controls: Vendor Contracts
	ID.SC-4: 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	Vendor Management: • SOC Report Review • Security Testing Review Risk Assessment: Controls: Review Security Testing Reports
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Business Continuity Plan: Exercises & Tests Incident Management: Exercises & Tests Vendor Management
Protect Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of authorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices, users, and processes	Policies: User Authentication
	PR.AC-2: Physical access to assets is managed and protected	Policies: Physical Security of Sensitive Information Risk Assessment: Controls: Physical Access Controls
	PR.AC-3: Remote access is managed	Policies: Remote Access Risk Assessment: Controls: Logical Access Controls
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Policies: Access Control Risk Assessment: Controls: Logical Access Controls

NIST Category	NIST Subcategory	Tandem References
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policies: • ATM Security • Cloud Computing • Data Backup • Demilitarized Zone • Firewall • Virtual System Technology • Wireless Network Access Risk Assessment: Controls: Logical Access Controls
	PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions	Policies: User Authentication

Protect
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
	PR.AT-1: All users are informed and trained	Policies: Employee Security Awareness Training
		Phishing
		Training:
		• Acceptable Use Policy Training
		• Identity Theft Prevention Program (Red Flag) Training
		• Phishing Training
		• Security Awareness Training
		Risk Assessment:
		• Controls:
		  ○ Employee Training
		  ○ Employee Security Awareness Training

NIST Category	NIST Subcategory	Tandem References

	PR.AT-2: Privileged users understand their roles and responsibilities	Policies:
		• Acceptable Use
		• Employee Security Awareness Training
		• User Authentication
		Risk Assessment:
		• Controls:
		  ○ Employee Training
		  ○ Employee Security Awareness Training

	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	Incident Management: Roles & Responsibilities Policies: Vendor Management
	PR.AT-4: Senior executives understand their roles and responsibilities	Information Security Program Resource Document Incident Management: Roles & Responsibilities Policies: Employee Security Awareness Training

	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	Information Security Program Resource Document
		Incident Management: Roles & Responsibilities
		Policies:
		• Acceptable Use Policy
		• Employee Security Awareness Training Policy
		Training: Security Awareness Training
		Risk Assessment:
		• Controls:
		  ○ Employee Training
		  ○ Employee Security Awareness Training

NIST Category	NIST Subcategory	Tandem References
Protect Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	Policies: • Data Backup • Data Storage • Electronic Imaging • Encryption • Intrusion Detection and Prevention • Malicious Software Protection • Mobile Devices • Physical Security of Sensitive Information • User Authentication • Vulnerability and Patch Management Risk Assessment: Controls: Data Encryption
	PR.DS-2: Data-in-transit is protected	Policies: • Email Security • Encryption • Mobile Devices • Remote Access • Removable Media and Data Transfer Risk Assessment: Controls: Data Encryption
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Policies: • IT Asset Management • Data Retention and Destruction Risk Assessment: Information Assets

NIST Category	NIST Subcategory	Tandem References
	PR.DS-4: Adequate capacity to ensure availability is maintained	Business Continuity Plan Policies: Network Monitoring and Log Management Risk Assessment: • Threats: Capacity Saturation • Controls: Capacity Monitoring
	PR.DS-5: Protections against data leaks are implemented	Policies: • Acceptable Use Policy • Cloud Computing • Data Backup • Data Storage • Employee Security Awareness Training • Mobile Devices • Remote Access • Remote Work • Vulnerability and Patch Management Risk Assessment: • Threats: Data Loss • Controls: Data Loss Prevention (DLP) Program Training: Security Awareness Training

NIST Category	NIST Subcategory	Tandem References
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Business Continuity Plan: • Cyber Resilience Preparedness Control Policies: • Security Testing • Third-Party Secure Application Development • Vulnerability and Patch Management
	PR.DS-7: The development and testing environment(s) are separate from the production environment	Policies: Third-Party Secure Application Development Risk Assessment: Controls: Secure Coding Techniques
Protect Information Protection Processes and Procedures (PR.IP): 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.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Policies: • Change Management • System Hardening Risk Assessment: • Change Management
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	Policies: • IT Asset Management • Change Management • Third-Party Secure Application Development Risk Assessment: Controls: Secure Coding Techniques
	PR.IP-3: Configuration change control processes are in place	Policies: Change Management Risk Assessment: Controls: Change Management

NIST Category	NIST Subcategory	Tandem References
	PR.IP-4: Backups of information are conducted, maintained, and tested	Policies: Data Backup Business Continuity Plan: • Backup Profiles • Exercises & Tests Risk Assessment: Controls: Data Backup
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Policies: • Physical Security of Sensitive Information • Remote Work • Security Testing
	PR.IP-6: Data is destroyed according to policy	Policies: • Acceptable Use Policy • Data Retention and Destruction • Remote Work • Security Testing Risk Assessment: Controls: Data retention and Destruction Procedures
	PR.IP-7: Protection processes are improved	Policies: Security Committee
	PR.IP-8: Effectiveness of protection technologies is shared	Policies: • Information Sharing and Regulatory Monitoring • Security Committee • Security Testing Risk Assessment: Controls: Information Sharing Forum

NIST Category	NIST Subcategory	Tandem References

	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Business Continuity Plan
		Incident Management
		Policies: Incident Management
		Risk Assessment:
		• Controls:
		  ○ Business Continuity Plan
		  ○ Incident Response Plan

	PR.IP-10: Response and recovery plans are tested	Business Continuity Plan: Exercises & Tests Incident Management: Exercises & Tests Risk Assessment: Controls: BCP/DR Testing

	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Business Continuity Plan: Cross Training Matrix
		Policies:
		• Access Control
		• Personnel Security
		Risk Assessment:
		• Controls
		  ○ Access Control
		  ○ Background Checks
		  ○ Employee Termination Procedures

	PR.IP-12: A vulnerability management plan is developed and implemented	Policies: Vulnerability and Patch Management Risk Assessment: Controls: Vulnerability Scans Addressing Vulnerabilities in the Risk Assessment Knowledge Base Article

NIST Category	NIST Subcategory	Tandem References
● **Protect** Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	Policies: • Change Management • Vulnerability and Patch Management Risk Assessment: Controls: Change Management
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policies: • Remote Access • Vendor Management Vendor Management
● **Protect** Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policies: Network Monitoring and Log Management
	PR.PT-2: Removable media is protected and its use restricted according to policy	Policies: Removable Media and Data Transfer Risk Assessment: Information Security Risk Assessment Questionnaire

	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Policies: Access Control
		Risk Assessment:
		• Controls:
		  ○ Physical Access Controls
		  ○ Logical Access Controls

	PR.PT-4: Communications and control networks are protected	Business Continuity Plan: Preparedness Controls Policies: • Voice over Internet Protocol • Wireless Network Access Vendor Management

NIST Category	NIST Subcategory	Tandem References
	PR.PT-5: Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Business Continuity Plan: • Preparedness Controls • Backup Profiles • Exercises & Tests • System/Equipment Recovery
Detect Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	Policies: • Intrusion Detection and Prevention • Network Monitoring and Log Management Risk Assessment: Information Security Risk Assessment Data Flows
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	Incident Management: • Incident Handling Process: Detection • Action Plans Policies: • Intrusion Detection and Prevention • Malicious Software Protection • Network Monitoring and Log Management
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Incident Management: Action Plans Policies: • Intrusion Detection and Prevention • Network Monitoring and Log Management
	DE.AE-4: Impact of events is determined	Incident Management: Severity Levels Policies: Intrusion Detection and Prevention

NIST Category	NIST Subcategory	Tandem References
	DE.AE-5: Incident alert thresholds are established	Incident Management: • Incident Handling Process: Detection • Additional Documentation: Internal Communication Policies: • Incident Management • Intrusion Detection and Prevention
Detect Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	Incident Management: Incident Handling Process: Detection Policies: • Firewall • Intrusion Detection and Prevention • Malicious Software Protection • Network Monitoring and Log Management
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Incident Management: Incident Handling Process: Detection Policies: Physical Security of Sensitive Information
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Incident Management: Incident Handling Process: Detection Policies: • Acceptable Use Policy • Network Monitoring and Log Management • Personnel Security

NIST Category	NIST Subcategory	Tandem References
	DE.CM-4: Malicious code is detected	Incident Management: • Incident Handling Process: Detection • Action Plans: Malicious Code Policies: Malicious Software Protection
	DE.CM-5: Unauthorized mobile code is detected	Incident Management: • Incident Handling Process: Detection • Action Plans: Malicious Code Policies: Malicious Software Protection
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Incident Management: • Incident Handling Process: Detection • Action Plans: Third Party Policies: Vendor Management Vendor Management
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Incident Management: Incident Handling Process: Detection Policies: • IT Asset Management • Network Monitoring and Log Management • Physical Security of Sensitive Information • Security Testing
Detect Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	Incident Management: Roles & Responsibilities Policies: • Incident Management • Intrusion Detection and Prevention

NIST Category	NIST Subcategory	Tandem References
ensure awareness of anomalous events.	**DE.DP-2:** Detection activities comply with all applicable requirements	Incident Management: Incident Handling Process: Detection Policies: Intrusion Detection and Prevention
	DE.DP-3: Detection processes are tested	Incident Management: Exercises & Tests Policies: Security Testing
	DE.DP-4: Event detection information is communicated	Incident Management: Additional Documentation: Internal Communication Policies: • Incident Management • Intrusion Detection and Prevention • Security Committee
	DE.DP-5: Detection processes are continuously improved	Incident Management: Incident Handling Process: Postmortem Policies: • Security Committee • Intrusion Detection and Prevention
Respond Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an incident	Incident Management Policies: Incident Management

NIST Category	NIST Subcategory	Tandem References
Respond Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	Incident Management • Roles & Responsibilities • Incident Handlers • Action Plans Policies: Incident Management
	RS.CO-2: Incidents are reported consistent with established criteria	Incident Management: • Categories • Severity Levels • Additional Documentation: Internal Communication Policies: Incident Management
	RS.CO-3: Information is shared consistent with response plans	Incident Management: Additional Documentation • Customer / Member Communication • Internal Communication • Third-Party Communication Policies: • Incident Management • Information Sharing and Regulatory Monitoring

	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Incident Management:
		• Roles & Responsibilities
		• Additional Documentation
		  ○ Internal Communication
		  ○ Third-Party Communication
		Policies: Incident Management

NIST Category	NIST Subcategory	Tandem References
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Incident Management: Additional Documentation: Third-Party Communication Policies: Information Sharing and Regulatory Monitoring
Respond Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	Incident Management: Incident Handling Process: Detection Policies • Incident Management • Intrusion Detection and Prevention
	RS.AN-2: The impact of the incident is understood	Incident Management: • Incident Handling Process: Analysis • Severity Levels Policies: Incident Management
	RS.AN-3: Forensics are performed	Incident Management • Incident Handling Process: Analysis • Additional Documentation: Evidence Policies: Incident Management
	RS.AN-4: Incidents are categorized consistent with response plans	Incident Management: Categories Policies: Incident Management
Respond Mitigation (RS.MI): Activities are performed to prevent expansion of an event,	**RS.MI-1:** Incidents are contained	Incident Management: Incident Handling Process: Containment Policies: Incident Management
	RS.MI-2: Incidents are mitigated	Incident Management: Incident Handling Process: Eradication and Recovery Policies: Incident Management

NIST Category	NIST Subcategory	Tandem References
mitigate its effects, and resolve the incident.	**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks	Incident Management: Incident Handling Process: Postmortem Risk Assessment
Respond Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	Incident Management: Incident Handling Process: Postmortem Policies: Incident Management
	RS.IM-2: Response strategies are updated	Incident Management: • Incident Handling Process: Postmortem • Action Plans Policies: • Incident Management • Security Committee
Recover Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	Incident Management: Incident Handling Process: Recovery Business Continuity Plan Policies: Incident Management
Recover Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	Incident Management: Incident Handling Process: Postmortem Business Continuity Plan: Exercises & Tests Policies: Incident Management
	RC.IM-2: Recovery strategies are updated	Incident Management: Incident Handling Process: Postmortem Business Continuity Plan Policies: Security Committee

NIST Category	NIST Subcategory	Tandem References
Recover Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	Incident Management: Additional Documentation: • Customer / Member Communication • Internal Communication • Third-Party Communication Business Continuity Plan: • Emergency Checklist: Customer Communication • Preparedness Control: Customer Communication Plan
	RC.CO-2: Reputation is repaired after an incident	Incident Management: Additional Documentation: • Customer / Member Communication • Internal Communication • Third-Party Communication Business Continuity Plan: Preparedness Controls: • Customer Communication Plan • Employee Communication Plan
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	Incident Management: Additional Documentation: • Customer / Member Communication • Internal Communication • Third-Party Communication Business Continuity Plan: • Call Trees • Employee Alerts Tool • Preparedness Control: Employee Communication Plan