Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
Identify	AM	Asset Management	Operational Security: Asset Management	**5.7**	**5.4**					1, 2	DI, DM
			ID.AM-1: Physical devices and systems within the organization are inventoried.	4	5	All Physical Devices and System are documented as of 09/08/2022.	Very Low	Low	Low	1	CM-8
			ID.AM-2: Software platforms and applications within the organization are inventoried.	8	5	Software platforms and Applications are not documented as of 09/08/2022. This needs to be addressed ASAP	Low	Moderate	Moderate	2	CM-8
			PR.SE-1: Inventory of Sensitive Data – Personally Identifiable Information (PII)	8	5	PII is stored internally in the clients backend systems	Low	High	High		SE-1
			ID.AM-3: Organizational communication and data flows are mapped.	3	5	As of 09/08/2022, organizational communication is not mapped	Low	Moderate	Moderate	1	AC-20, SA-9
			ID.AM-4: External information systems are catalogued.	5	5	As of 09/08/2022, all external information systems are catalogued	Very Low	Low	Low	1	AC-4, CA-3, CA-9, PL-8
			ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	9	8	As of 09/08/2022, organization resources that are inventoried, are prioritized. However, due to ID.AM-2 all	Moderate	High	High		CP-2, RA-2, SA-14
			ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	3	5	Proper internal structure of cybersecurity roles and responsibilities has been established	Low	Low	Low		CP-2, PS-7, PM-11
	GV	Governance	Strategic Security: Governance and Compliance	**7.5**	**5.0**						AU, PL, PM
			ID.GV-1: Organizational cybersecurity policy is established and communicated.	8	5	The company has established and communicated its organizational cybersecurity policy. Employees are aware of and familiar with the contents of the policy. This indicates a proactive approach to cybersecurity governance	Low	High	High		controls from all families
			ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	8	5	The company has processes in place to ensure that cybersecurity roles and responsibilities are well-coordinated and	Low	High	High		PM-1, PS-7
			ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	9	5	The company has processes in place to ensure that legal and regulatory requirements related to cybersecurity,	Low	High	High		controls from all families
			ID.GV-4: Governance and risk management processes address cybersecurity risks.	5	5	The company has established governance and risk management processes that specifically address	Low	Moderate	Moderate		PM-9, PM-11
	RA	Risk Assessment	Strategic Security: Risk Assessments	**7.2**	**5.3**					3, 20	RA

Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
			ID.RA-1: Asset vulnerabilities are identified and documented.	8	5	The company has processes in place to identify and document vulnerabilities associated with its assets. This indicates a proactive approach to understanding and managing potential security weaknesses, which is essential for maintaining a secure environment.	Low	High	High	3	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
			ID.RA-2: Cyberthreat intelligence is received from information sharing forums and sources.	5	7	While the company does receive cyberthreat intelligence from information sharing forums and sources,	Low	Moderate	Moderate	3	PM-15, PM-16, SI-5
			ID.RA-3: Threats, both internal and external, are identified and documented.	7	5	The company has established processes to identify and document threats, encompassing both internal and external	Low	Moderate	Moderate	3, 20	RA-3, SI-5, PM-12, PM-16
			ID.RA-4: Potential business impacts and likelihoods are identified.	5	5	The company has processes in place to identify potential business impacts and likelihoods associated with cybersecurity	Low	Moderate	Moderate		RA-2, RA-3, PM-9, PM-11,
			ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	9	5	The company utilizes information on threats, vulnerabilities, likelihoods, and impacts to assess and determine risks.	Low	High	High		RA-2, RA-3, PM-16
			ID.RA-6: Risk responses are identified and prioritized.	9	5	The company has established processes to identify and prioritize risk responses. This indicates a structured approach to	Low	High	High		PM-4, PM-9
	RM	Risk Management	Strategic Security: Risk Management	**5.3**	**4.3**						RA, PM
			ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	8	5	The company has established and managed risk management processes. These processes are agreed upon by	Low	High	High		PM-9
			ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	5	5	The company has determined and clearly expressed its organizational risk tolerance. This indicates a clear	Low	Low	Low		PM-9
			ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	3	3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific	Low	Low	Low		PM-9
	AC	Identity Management and Access Control	Operational Security: Access Control	**8.1**	**6.3**					4, 11-14, 16, 18	AC, IA
			PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.	8	8	While the organization has processes in place for issuing, managing, verifying, and auditing identities and credentials for authorized devices, users, and processes, there might be room for improvement. Consideration could be given to further enhancing the verification and auditing processes to ensure even greater security and compliance.	High	High	Very High	18	AC-2, IA Family

Cybersecurity Risk-Aligned Framework											
Function	Category Unique Identifier	Category	Cybersecurity Framework Control	Priority	Compliance	Notes	Likelihood	Impact	Risk	CSC Top Twenty	NIST Policy Family
			PR.AC-2: Physical access to assets is managed and protected.	6	6	The organization has established processes to manage and protect physical access to assets. This indicates a	Moderate	High	High		PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
			PR.AC-3: Remote access is managed.	8	5	The organization has established processes to manage remote access. This indicates a structured approach to	Low	High	High	12	AC-17, AC-19, AC-20
			PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	9	8	While the organization does have processes in place for managing access permissions and authorizations, there	High	High	Very High	4, 14, 16, 18	AC-2, AC-3, AC-5, AC-6, AC-
			PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	10	6	The organization has implemented measures to protect network integrity, including practices such as network	Moderate	Very High	Very High	11, 12, 13, 14	AC-4, SC-7
			PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	8	6	The organization has established processes to ensure that identities are proofed and securely bound to	Low	High	High		AC-2, IA Family
			PR.AC-7: Users, devices, and other assets are authenticated (e.g., single factor and multi-factor) commensurate with the risk of the transaction (individuals' security and privacy risks and other organizational risks).	8	5	The organization has implemented authentication measures for users, devices, and other assets. Authentication methods, including both single-factor and multi-factor, are applied in a manner commensurate with the risk associated with specific transactions. This indicates a thoughtful approach to balancing security and privacy concerns, ensuring that the level of authentication matches the potential risks involved.	Low	High	High		AC-2, IA Family
	AT	Awareness and Training	Strategic Security: Awareness and Training	**6.5**	**6.5**					4, 17	AT, PS
			PR.AT-1: All users are informed and trained.	8	8	While there are efforts in place to inform and train users, there may be room for improvement. Consideration	High	High	Very High	17	AT-2, PM-13
			PR.AT-2: Privileged users understand their roles and responsibilities.	7	6	Privileged users within the organization understand their roles and responsibilities. This indicates that there	Low	Moderate	Moderate	4, 17	AT-3, PM-13
			PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	5	7	While efforts have been made to inform third-party stakeholders of their roles and responsibilities, there may be room for improvement. Consideration could be given to enhancing the communication and training processes to ensure that all relevant parties have a clear understanding of their respective roles and responsibilities in relation to cybersecurity. This will contribute to a more secure collaborative environment.	Moderate	High	High	17	PS-7, SA-9
			PR.AT-4: Senior executives understand their roles and responsibilities.	6	5	Senior executives within the organization understand their roles and responsibilities. This indicates that there	Low	Low	Low	17	AT-3, PM-13

ect

Cybersecurity Risk-Aligned Framework											
Function	Category Unique Identifier	Category	Cybersecurity Framework Control	Priority	Compliance	Notes	Likelihood	Impact	Risk	CSC Top Twenty	NIST Policy Family
Proje	DS	Data Security	Operational Security: Encryption and Data Integrity	**6.3**	**5.0**					1, 2, 13, 14	SC
			PR.DS-1: Data-at-rest is protected.	9	5	The organization has implemented measures to protect data-at-rest. This indicates that there are security	Low	High	High	14	SC-28
			PR.DS-2: Data-in-transit is protected.	9	5	The organization has established measures to protect data-in-transit. This indicates that there are security	Low	High	High	13, 14	SC-8
			PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	4	4	The organization has established formal processes to manage assets throughout their lifecycle, including removal,	Low	Moderate	Moderate	1	CM-8, MP-6, PE-16
			PR.DS-4: Adequate capacity to ensure availability is maintained.	7	5	The organization has measures in place to ensure that adequate capacity is maintained to guarantee availability.	Low	High	High		AU-4, CP-2, SC-5
			PR.DS-5: Protections against data leaks are implemented.	5	5	The organization has implemented measures to protect against data leaks. This indicates that there are security controls in place to prevent unauthorized disclosure or leakage of sensitive information. These protections are crucial for maintaining the	Low	Low	Low	13	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
			PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	5	5	The organization utilizes integrity checking mechanisms to verify the integrity of software, firmware, and	Low	Low	Low	2	SI-7
			PR.DS-7: The development and testing environment(s) are separate from the production environment.	7	7	The organization maintains separate development and testing environments from the production environment. This	Low	Moderate	Moderate		CM-2
			PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	4	4	The organization employs integrity checking mechanisms to verify the integrity of hardware components. This	Low	Low	Low		
	IP	Information Protection Processes and Procedures	Operational Security: Processes and Procedures	**6.3**	**4.8**					5, 3, 7, 11, 19	MP, PE, SA, SC
			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).	7	5	The organization has established and maintains a baseline configuration for its information technology and industrial control systems. This configuration incorporates security principles,	Low	High	High	5, 7, 11	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-
			PR.IP-2: A System Development Life Cycle to manage systems is implemented.	4	4	The organization has implemented a System Development Life Cycle (SDLC) to manage systems. This indicates a	Low	Low	Low		SA-3, SA-4, SA-8, SA-10, SA-

Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
			PR.IP-3: Configuration change control processes are in place.	8	5	The organization has established processes for configuration change control. This indicates a structured approach to managing changes to configurations, which is crucial for maintaining the integrity and security of systems and networks. It ensures that changes are carefully planned, tested, and approved before being implemented.	Low	High	High		CM-3, CM-4, SA-10
			PR.IP-4: Backups of information are conducted, maintained, and tested.	8	5	The organization conducts, maintains, and tests backups of information. This indicates a proactive approach to	Low	High	High		CP-4, CP-6, CP-9
			PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	3	3	The organization complies with policies and regulations concerning the physical operating environment for its assets. This indicates a structured approach to ensuring that the physical environment in which organizational assets operate meets the required standards and safeguards. This compliance helps to mitigate physical risks that could impact the security and availability of assets.	Very Low	Low	Low		PE
			PR.IP-6: Data is destroyed according to policy.	6	5	The organization has established policies and procedures for the proper destruction of data. This indicates a	Low	Moderate	Moderate		MP-6
			PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	9	5	The organization has established and actively manages response plans, including Incident Response and	Low	High	High		CP, IR families
			PR.IP-10: Response and recovery plans are tested.	7	7	While there are efforts in place to test response and recovery plans, there may be room for improvement.	High	High	Very High	19	CP, IR families
			PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	4	4	Cybersecurity is integrated into human resources practices within the organization. This includes	Low	Low	Low		PS Family
			Application development	5	5						SI-2, SI-3
			PR.IP-12: A vulnerability management plan is developed and implemented.	8	5	The organization has developed and implemented a vulnerability management plan. This indicates a structured approach to identifying, assessing, and mitigating vulnerabilities within the organization's systems and networks. Having a formal plan in place is crucial for maintaining a secure posture and proactively addressing potential security weaknesses.	Low	High	High	3	RA-3, RA-5, SI-2

Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
	MA	Maintenance	Operational Security: Asset Maintenance	**5.0**	**3.5**					4, 12	MA
			PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	4	4	The organization conducts maintenance and repair of its assets using approved and controlled tools. Additionally, these	Low	Low	Low		MA Family
			PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	6	3	The organization has established processes to approve, log, and conduct remote maintenance of its assets in a	Low	Moderate	Moderate	4, 12	MA-4
	PT	Protective Technology	Operational Security: Protect Assets	**7.8**	**4.6**					4, 6, 8, 11, 13, 14, 18	CM, AU
			PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	9	5	The organization has established and follows processes for determining, documenting, implementing, and reviewing audit/log records in accordance with policy. This indicates a structured approach to logging and auditing activities, which is crucial for monitoring and analyzing security events. It also helps to ensure compliance with organizational policies and regulatory requirements related to logging and auditing.	Low	Very High	Very High	6	AU Family
			PR.PT-2: Removable media is protected and its use restricted according to policy.	5	5	The organization has established measures to protect removable media and has policies in place to restrict its	Low	Low	Low	8, 13, 14	MP Family
			PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	8	5	The organization has incorporated the principle of least functionality by configuring systems to provide only	Low	High	High	4, 14, 18	AC-3, CM-7
			PR.PT-4: Communications and control networks are protected.	9	4	The organization has implemented measures to protect communications and control networks. This indicates a structured approach to securing the networks used for communication and control purposes. This is crucial for safeguarding sensitive information, ensuring secure operations, and preventing unauthorized access or interference in these critical systems.	Low	Very High	Very High	11	AC-4, AC-17, AC-18, CP-8, SC-7
			PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	8	4	The organization has implemented mechanisms such as failsafe, load balancing, and hot swap to achieve	Low	High	High	11	
	AE	Anomalies and Events	Operational Security: Monitor, Analyze, and Detect Events	**6.2**	**5.2**					6, 12, 19	IR

Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
Detect			DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	5	5	The organization has established and actively manages a baseline of network operations and expected data flows for	Low	Low	Low	12	AC-4, CA-3, CM-2, SI-4
			DE.AE-2: Detected events are analyzed to understand attack targets and methods.	6	6	The organization actively analyzes detected events to gain an understanding of attack targets and	Moderate	Moderate	Moderate	19	AU-6, CA-7, IR-4, SI-4
			DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	7	5	The organization collects and correlates event data from multiple sources and sensors. This indicates a structured approach to aggregating information from various points within the environment. Correlating data from multiple sources allows for a more comprehensive view of events, which is crucial for effective threat detection and incident response.	Low	Moderate	Moderate	6	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
			DE.AE-4: Impact of events is determined.	8	5	The organization actively determines the impact of events. This indicates a structured approach to assessing the	Low	High	High	19	CP-2, IR-4, RA-3, SI -4
			DE.AE-5: Incident alert thresholds are established.	5	5	The organization has established incident alert thresholds. This indicates a proactive approach to setting	Low	Low	Low	19	IR-4, IR-5, IR-8
	CM	Security Continuous Monitoring	Operational Security: Security Continuous Monitoring	**7.0**	**4.5**					5, 8, 19	
			DE.CM-1: The network is monitored to detect potential cybersecurity events.	10	5	The organization actively monitors the network to detect potential cybersecurity events. This indicates a	Low	Very High	Very High	19	AC-2, AU-12, CA-7, CM-3, SC-
			DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	5	5	The organization actively monitors the physical environment to detect potential cybersecurity events. This indicates a	Low	Low	Low	19	CA-7, PE-3, PE-6, PE-20
			DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	5	3	The organization actively monitors personnel activity to detect potential cybersecurity events. This indicates a	Low	Low	Low	19	AC-2, AU-12, AU-13, CA-7, CM-
			DE.CM-4: Malicious code is detected.	8	5	The organization actively detects malicious code. This indicates a structured approach to identifying and	Low	High	High	8, 19	SI-3
			DE.CM-5: Unauthorized mobile code is detected.	5	5	The organization actively detects unauthorized mobile code. This indicates a structured approach to identifying and	Low	Low	Low	8, 19	SC-18, SI-4. SC-44
			DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	6	4	The organization actively monitors external service provider activity to detect potential cybersecurity events.	Low	Moderate	Moderate	19	CA-7, PS-7, SA-4, SA-9, SI-4

Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	9	4	The organization actively monitors for unauthorized personnel, connections, devices, and software. This indicates a structured approach to continuously checking for any unauthorized entities or activities within the environment. Proactive monitoring for unauthorized elements is crucial for early detection and response to potential security breaches, helping to safeguard against unauthorized access and activities that could pose a risk to the organization.	Low	Very High	Very High	19	CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
			DE.CM-8: Vulnerability scans are performed.	8	5	The organization conducts vulnerability scans. This indicates a structured approach to regularly assessing systems	Low	High	High	3	RA-5
	DP	Detection Processes	Operational Security: Detection Processes	**5.2**	**4.8**					6	
			DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	6	6	The organization has well-defined roles and responsibilities for detection, ensuring clear accountability. This	Moderate	Moderate	Moderate	6	CA-2, CA-7, PM-14
			DE.DP-2: Detection activities comply with all applicable requirements.	8	4	Detection activities within the organization are conducted in compliance with all applicable	Low	High	High	6	CA-2, CA-7, PM-14, SI-4
			DE.DP-3: Detection processes are tested.	4	6	While there are efforts in place to test detection processes, there may be room for improvement. Consideration could	Moderate	Low	Moderate	6	CA-2, CA-7, PE-3, PM-14, SI-
			DE.DP-4: Event detection information is communicated.	4	4	The organization effectively communicates event detection information. This indicates a structured	Low	Low	Low	6	AU-6, CA-2, CA-7, RA-5, SI-4
			DE.DP-5: Detection processes are continuously improved.	4	4	The organization actively engages in continuous improvement of its detection processes. This indicates a	Low	Low	Low	6	CA-2, CA-7, PL-2, RA-5, SI-4,
	RP	Response Planning	Operational Security: Response Planning	**8.0**	**5.0**					19	
			RS.RP-1: Response plan is executed during or after an incident.	8	5	The organization executes the response plan during or after an incident. This indicates a structured approach to activating and implementing the planned response measures when a security incident occurs. Executing the response plan in a timely and effective manner is crucial for minimizing the impact of incidents and facilitating a coordinated and controlled response. This control supports a proactive and organized approach to incident response.	Low	High	High	19	CP-2, CP-10, IR-4, IR-8

Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
Respond	CO	Communications	Operational Security: Communications	**4.8**	**4.2**					19	
			RS.CO-1: Personnel know their roles and order of operations when a response is needed.	5	5	Personnel within the organization are aware of their roles and the established order of operations when a response is needed. This indicates a structured approach to ensuring that individuals understand their responsibilities and the sequence of actions to take in the event of a security incident. Clarity regarding roles and procedures is crucial for a coordinated and effective incident response effort. This control supports a proactive and organized approach to incident management.	Low	Low	Low	19	CP-2, CP-3, IR-3, IR-8
			RS.CO-2: Events and Incidents are reported consistent with established criteria.	8	5	Events and incidents within the organization are reported in accordance with established criteria. This indicates a	Low	High	High	19	AU-6, IR-6, IR-8
			RS.CO-3: Information is shared consistent with response plans.	3	3	The organization shares information in alignment with its response plans. This indicates a structured approach to	Low	Low	Low	19	CA-2, CA-7, CP-2, IR-4, IR-8,
			RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	5	5	The organization coordinates with stakeholders in accordance with its response plans. This indicates a	Low	Moderate	Moderate	19	CP-2, IR-4, IR-8
			RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	3	3	The organization actively engages in voluntary information sharing with external stakeholders to enhance	Low	Low	Low	19	PM-15, SI-5
	AN	Analysis	Operational Security: Analysis	**6.6**	**5.2**					19	
			RS.AN-1: Notifications from detection systems are investigated.	9	5	Notifications from detection systems are actively investigated. This indicates a structured approach to examining and	Low	High	High	19	AU-6, CA-7, IR-4, IR-5, PE-6, SI-
			RS.AN-2: The impact of the incident is understood.	5	5	The organization actively works to understand the impact of security incidents. This indicates a structured	Low	Low	High	19	CP-2, IR-4
			RS.AN-3: Forensics are performed.	5	5	The organization conducts forensic analysis as part of incident response efforts. This indicates a structured	Low	Low	High	19	AU-7, IR-4

Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
			RS.AN-4: Incidents are categorized consistent with response plans.	6	6	Incidents within the organization are categorized in alignment with established response plans. This indicates a structured approach to classifying incidents based on predefined criteria outlined in response plans. Consistent categorization is crucial for organizing incidents by severity or type, which in turn helps in prioritizing response efforts and allocating resources effectively. This control supports a proactive and organized approach to incident management.	Low	Moderate	Moderate	19	CP-2, IR-4, IR-5, IR-8
			RS.AN-5: 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).	8	5	The organization has established processes to receive, analyze, and respond to vulnerabilities disclosed from both internal and external sources. This indicates a structured approach to handling reports of vulnerabilities, whether they come from internal testing, security bulletins, or external security researchers. Having established processes for vulnerability disclosure and response is crucial for promptly addressing potential security weaknesses and minimizing associated risks. This control supports a proactive and organized approach to vulnerability management.	Low	High	High	19	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
	MI	Mitigation	Operational Security: Mitigation	**6.7**	**4.3**					3, 19	IR
			RS.MI-1: Incidents are contained.	8	5	The organization effectively contains incidents as part of its incident response process. This indicates a structured	Low	High	High	19	IR-4
			RS.MI-2: Incidents are mitigated.	6	4	The organization effectively mitigates incidents as part of its incident response process. This indicates a structured	Low	Moderate	Moderate	19	IR-4
			RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	6	4	The organization actively addresses newly identified vulnerabilities by either mitigating them or documenting them	Low	Moderate	Moderate	3	CA-7, RA-3, RA-5
	IM-D	Improvements	Operational Security: Improvements	**6.0**	**4.0**					19	
			RS.IM-1: Response plans incorporate lessons learned.	4	4	The organization's response plans include a process for incorporating lessons learned from previous incidents.	Low	Low	Low	19	CP-2, IR-4, IR-8

Cybersecurity Risk-Aligned Framework											
Function	**Category Unique Identifier**	**Category**	**Cybersecurity Framework Control**	**Priority**	**Compliance**	**Notes**	**Likelihood**	**Impact**	**Risk**	**CSC Top Twenty**	**NIST Policy Family**
			RS.IM-2: Response strategies are updated.	8	4	The organization regularly updates its response strategies based on evolving threat landscapes and lessons learned	Low	High	High	19	CP-2, IR-4, IR-8
Recover	RP	Recovery Planning	Operational Security: Recovery Planning	**5.0**	**5.0**					19	CP
			RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.	5	5	The organization executes the recovery plan during or after a cybersecurity incident. This indicates a structured	Low	Low	Low	19	CP-10, IR-4, IR-8
	IM-R	Improvements	Operational Security: Improvements	**4.0**	**4.0**					19	
			RC.IM-1: Recovery plans incorporate lessons learned.	4	4	The organization's recovery plans include a process for incorporating lessons learned from previous incidents.	Low	Low	Low	19	CP-2, IR-4, IR-8
			RC.IM-2: Recovery strategies are updated.	4	4	The organization regularly updates its recovery strategies based on evolving threat landscapes and lessons learned	Low	Low	Low	19	CP-2, IR-4, IR-8
	CO	Communications	Operational Security: Communications	**4.0**	**4.0**					19	
			RC.CO-1: Public relations are managed.	4	4	The organization has established processes to manage public relations in	Low	Moderate	Moderate	19	
			RC.CO-2: Reputation is repaired after an incident.	4	4	The organization has established processes to repair its reputation	Low	Moderate	Moderate	19	
			RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	4	4	The organization has established processes to communicate recovery activities to both internal and external stakeholders, including executive and management teams. This indicates a structured approach to ensuring that relevant parties are informed of the progress and status of recovery efforts following a cybersecurity incident. Effective communication of recovery activities is crucial for maintaining transparency, managing expectations, and demonstrating the organization's commitment to resolving the incident. This control supports a proactive and communicative approach to incident recovery.	Low	Moderate	Moderate	19	CP-2, IR-4

Cybersecurity Risk-Aligned Framework											
Function	Category Unique Identifier	Category	Cybersecurity Framework Control	Priority	Compliance	Notes	Likelihood	Impact	Risk	CSC Top Twenty	NIST Policy Family