NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored				
	Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood			
		GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1**: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	**NA**
		GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1**: Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2**: Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)	**Ensures internal stakeholders can be certified as low risk, high trust individuals related to insider threat risks**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	**Ex1**: Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) **Ex2**: Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information **Ex3**: Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements	**Ensures identification of potential insider risk individuals without violating legal restrictions, EEOC regulations, AI laws, etc.**
		GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	**Ex1**: Establish criteria for determining the criticality of capabilities and services as viewed by internal and external stakeholders **Ex2**: Determine (e.g., from a business impact analysis) assets and business operations that are vital to achieving mission objectives and the potential impact of a loss (or partial loss) of such operations **Ex3**: Establish and communicate resilience objectives (e.g., recovery time objectives) for delivering critical capabilities and services in various operating states (e.g., under attack, during recovery, normal operation)	**Ensures individuals have the documented soft skills needed for communications and critical capability delivery.**
		GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	**Ex1**: Create an inventory of the organization's dependencies on external resources (e.g., facilities, cloud-based hosting providers) and their relationships to organizational assets and business functions **Ex2**: Identify and document external dependencies that are potential points of failure for the organization's critical capabilities and services, and share that information with appropriate personnel	**External dependencies include remote workers that are potential points of failure for WiFi security mismanagement, RDP brute force attacks, phishing lures, password misuse, etc. Ensures potential insider risk individuals are identified and plans are in place to remediate risks.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
	Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions			
		GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	**Ex1**: Update near-term and long-term cybersecurity risk management objectives as part of annual strategic planning and when major changes occur **Ex2**: Establish measurable objectives for cybersecurity risk management (e.g., manage the quality of user training, ensure adequate risk protection for industrial control systems) **Ex3**: Senior leaders agree about cybersecurity objectives and use them for measuring and managing risk and performance	**Gartner & Forrester say traditional security awareness training is no longer effective, and Microsoft studies show only a 3% phishing incident reduction after training. Analysts say Human Risk Management (HRM) with behavioral science is now needed to manage the quality of user training. Ensures HRM is delivered with the capabilities needed.**
		GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	**Ex1**: Determine and communicate risk appetite statements that convey expectations about the appropriate level of risk for the organization **Ex2**: Translate risk appetite statements into specific, measurable, and broadly understandable risk tolerance statements **Ex3**: Refine organizational objectives and risk appetite periodically based on known risk exposure and residual risk	**Gartner, Forrester, IBM, etc. say 90% of security incident risks are related to human risk insider threats, such as phishing clicks. Risk appetitie statements should include policies and plans to address Human Risk Management. Ensures HRM capabilities are in place to reduce insider threat risks.**
		GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	**Ex1**: Aggregate and manage cybersecurity risks alongside other enterprise risks (e.g., compliance, financial, operational, regulatory, reputational, safety) **Ex2**: Include cybersecurity risk managers in enterprise risk management planning **Ex3**: Establish criteria for escalating cybersecurity risks within enterprise risk management	**Enterprise risk management should include HRM and insider threat management. Ensures HRM capabilities are in place to reduce insider threat risks.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	**Ex1**: Specify criteria for accepting and avoiding cybersecurity risk for various classifications of data **Ex2**: Determine whether to purchase cybersecurity insurance **Ex3**: Document conditions under which shared responsibility models are acceptable (e.g., outsourcing certain cybersecurity functions, having a third party perform financial transactions on behalf of the organization, using public cloud-based services)	**Human Risk Management elements should be included in policies and procedures. Ensures HRM capabilities are in place to reduce insider threat risks.**
		GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	**Ex1**: Determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals **Ex2**: Identify how all departments across the organization - such as management, operations, internal auditors, legal, acquisition, physical security, and HR - will communicate with each other about cybersecurity risks	**Ensures communication and other required soft skills for individuals responsible for executing this control are identified and improved.**
		GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	**Ex1**: Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas **Ex2**: Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership) **Ex3**: Establish criteria for risk prioritization at the appropriate levels within the enterprise **Ex4**: Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks	**Ensures quantitative approach to obtaining metrics related to insider threats and human risks are obtained and documented, which are related to 90% of security incident risks.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	**Ex1**: Define and communicate guidance and methods for identifying opportunities and including them in risk discussions (e.g., strengths, weaknesses, opportunities, and threats [SWOT] analysis) **Ex2**: Identify stretch goals and document them **Ex3**: Calculate, document, and prioritize positive risks alongside negative risks	**Ensures this includes insider risk and HRM data related to 90% of cyber risks are included in SWOT analyses.**
	Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated			
		GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	**Ex1**: Leaders (e.g., directors) agree on their roles and responsibilities in developing, implementing, and assessing the organization's cybersecurity strategy **Ex2**: Share leaders' expectations regarding a secure and ethical culture, especially when current events present the opportunity to highlight positive or negative examples of cybersecurity risk management **Ex3**: Leaders direct the CISO to maintain a comprehensive cybersecurity risk strategy and review and update it at least annually and after major events **Ex4**: Conduct reviews to ensure adequate authority and coordination among those responsible for managing cybersecurity risk	**Gartner and Forrester admonish creating a Security Behavior Culture Program to ensure a security and ethical culture. Ensures HRM is in place to meet this requirement.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	**Ex1**: Document risk management roles and responsibilities in policy **Ex2**: Document who is responsible and accountable for cybersecurity risk management activities and how those teams and individuals are to be consulted and informed **Ex3**: Include cybersecurity responsibilities and performance requirements in personnel descriptions **Ex4**: Document performance goals for personnel with cybersecurity risk management responsibilities, and periodically measure performance to identify areas for improvement **Ex5**: Clearly articulate cybersecurity responsibilities within operations, risk functions, and internal audit functions	**Ensures ten critical soft skills are scored related to relevant roles, responsibilities; documents performance goals; periodically measures performance to identify areas for improvement; provides personalized training to improve scores; allows for articulation of responsibilities based on trust and risk factors, as well as soft skills required.**
		GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	**Ex1**: Conduct periodic management reviews to ensure that those given cybersecurity risk management responsibilities have the necessary authority **Ex2**: Identify resource allocation and investment in line with risk tolerance and response **Ex3**: Provide adequate and sufficient people, process, and technical resources to support the cybersecurity strategy	**Provides metrics for periodic management review that includes trust, risk, leadership, and soft skills scores directly related to cybersecurity risks.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.RR-04: Cybersecurity is included in human resources practices	**Ex1**: Integrate cybersecurity risk management considerations into human resources processes (e.g., personnel screening, onboarding, change notification, offboarding) **Ex2**: Consider cybersecurity knowledge to be a positive factor in hiring, training, and retention decisions **Ex3**: Conduct background checks prior to onboarding new personnel for sensitive roles, and periodically repeat background checks for personnel with such roles **Ex4**: Define and enforce obligations for personnel to be aware of, adhere to, and uphold security policies as they relate to their roles	**Provides metrics for recruiting, onboarding, change notification, offboarding for trust, risk, insider threats, leadership, and soft skills. Enhances background checks related to trust factors, ensure awareness and adheration to security policies by creating a security culture based on behavioral science.**
	Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced			
		GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	**Ex1**: Create, disseminate, and maintain an understandable, usable risk management policy with statements of management intent, expectations, and direction **Ex2**: Periodically review policy and supporting processes and procedures to ensure that they align with risk management strategy objectives and priorities, as well as the high-level direction of the cybersecurity policy **Ex3**: Require approval from senior management on policy **Ex4**: Communicate cybersecurity risk management policy and supporting processes and procedures across the organization **Ex5**: Require personnel to acknowledge receipt of policy when first hired, annually, and whenever policy is updated	**Provides metrics and reports to support the creation of risk management policies and reporting, provides trending data to mesure improvements, provides new hires current and desired trust and risk scores with defined training and action plans.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	**Ex1**: Update policy based on periodic reviews of cybersecurity risk management results to ensure that policy and supporting processes and procedures adequately maintain risk at an acceptable level **Ex2**: Provide a timeline for reviewing changes to the organization's risk environment (e.g., changes in risk or in the organization's mission objectives), and communicate recommended policy updates **Ex3**: Update policy to reflect changes in legal and regulatory requirements **Ex4**: Update policy to reflect changes in technology (e.g., adoption of artificial intelligence) and changes to the business (e.g., acquisition of a new business, new contract requirements)	**Updated risk managed results must include human risk and insider threat metrics, given they are 90% of security risks. Provides scores and reports used for these metrics.**
	Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy			
		GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	**Ex1**: Measure how well the risk management strategy and risk results have helped leaders make decisions and achieve organizational objectives **Ex2**: Examine whether cybersecurity risk strategies that impede operations or innovation should be adjusted	**Provides risk and trust scores for personnel to help leaders make decisions based on validated risk data.**
		GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	**Ex1**: Review audit findings to confirm whether the existing cybersecurity strategy has ensured compliance with internal and external requirements **Ex2**: Review the performance oversight of those in cybersecurity-related roles to determine whether policy changes are necessary **Ex3**: Review strategy in light of cybersecurity incidents	**Provides metrics, data, and trending related to cybersecurity related role performance and risk/trust factors.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	**Ex1**: Review key performance indicators (KPIs) to ensure that organization-wide policies and procedures achieve objectives **Ex2**: Review key risk indicators (KRIs) to identify risks the organization faces, including likelihood and potential impact **Ex3**: Collect and communicate metrics on cybersecurity risk management with senior leadership	**Provides detailed Key Risk Indicators related to human risks, which account for 90% of security risks, provides reporting for leadership communications.**
	Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders			
		GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	**Ex1**: Establish a strategy that expresses the objectives of the cybersecurity supply chain risk management program **Ex2**: Develop the cybersecurity supply chain risk management program, including a plan (with milestones), policies, and procedures that guide implementation and improvement of the program, and share the policies and procedures with the organizational stakeholders **Ex3**: Develop and implement program processes based on the strategy, objectives, policies, and procedures that are agreed upon and performed by the organizational stakeholders **Ex4**: Establish a cross-organizational mechanism that ensures alignment between functions that contribute to cybersecurity supply chain risk management, such as cybersecurity, IT, operations, legal, human resources, and engineering	**Provides the ability to measure risk and trust factors for supply chain personnel, including MSP/MSSP personnel.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	**Ex1**: Identify one or more specific roles or positions that will be responsible and accountable for planning, resourcing, and executing cybersecurity supply chain risk management activities **Ex2**: Document cybersecurity supply chain risk management roles and responsibilities in policy **Ex3**: Create responsibility matrixes to document who will be responsible and accountable for cybersecurity supply chain risk management activities and how those teams and individuals will be consulted and informed **Ex4**: Include cybersecurity supply chain risk management responsibilities and performance requirements in personnel descriptions to ensure clarity and improve accountability **Ex5**: Document performance goals for personnel with cybersecurity risk management-specific responsibilities, and periodically measure them to demonstrate and improve performance **Ex6**: Develop roles and responsibilities for suppliers, customers, and business partners to address shared responsibilities for applicable cybersecurity risks, and integrate	**Allows for soft skill measurement to ensure proper selection of personnel for rols and responsibilities, provides training and development metrics related to performance goal measurement.**
		GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	**Ex1**: Identify areas of alignment and overlap with cybersecurity and enterprise risk management **Ex2**: Establish integrated control sets for cybersecurity risk management and cybersecurity supply chain risk management **Ex3**: Integrate cybersecurity supply chain risk management into improvement processes **Ex4**: Escalate material cybersecurity risks in supply chains to senior management, and address them at the enterprise risk management level	**Cybersecurity and enterprise risk management should include Key Risk Indicators for personnel based on validated metrics. Provides metrics and reports for KRIs.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.SC-04: Suppliers are known and prioritized by criticality	**Ex1**: Develop criteria for supplier criticality based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission **Ex2**: Keep a record of all suppliers, and prioritize suppliers based on the criticality criteria	**Allows for access rights throttling based on validated trust and risk metrics.**
		GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	**Ex1**: Establish security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised **Ex2**: Include all cybersecurity and supply chain requirements that third parties must follow and how compliance with the requirements may be verified in default contractual language **Ex3**: Define the rules and protocols for information sharing between the organization and its suppliers and sub-tier suppliers in agreements **Ex4**: Manage risk by including security requirements in agreements based on their criticality and potential impact if compromised **Ex5**: Define security requirements in service-level agreements (SLAs) for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle **Ex6**: Contractually require suppliers to disclose cybersecurity features, functions, and vulnerabilities of their products and services for the life of the product or the term of service **Ex7**: Contractually require suppliers to	**Allows for supply chain personnel assessments to measure human risks related to security performance metrics.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	**Ex1**: Perform thorough due diligence on prospective suppliers that is consistent with procurement planning and commensurate with the level of risk, criticality, and complexity of each supplier relationship **Ex2**: Assess the suitability of the technology and cybersecurity capabilities and the risk management practices of prospective suppliers **Ex3**: Conduct supplier risk assessments against business and applicable cybersecurity requirements **Ex4**: Assess the authenticity, integrity, and security of critical products prior to acquisition and use	**Due diligence and supplier risk assessments must include personnel assessments related to trust and risk factors to identify potential indicators of compromise. Provides science-based assessments to uncover potential supplier personnel risks and trust factors.**
		GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	**Ex1**: Adjust assessment formats and frequencies based on the third party's reputation and the criticality of the products or services they provide **Ex2**: Evaluate third parties' evidence of compliance with contractual cybersecurity requirements, such as self-attestations, warranties, certifications, and other artifacts **Ex3**: Monitor critical suppliers to ensure that they are fulfilling their security obligations throughout the supplier relationship lifecycle using a variety of methods and techniques, such as inspections, audits, tests, or other forms of evaluation **Ex4**: Monitor critical suppliers, services, and products for changes to their risk profiles, and reevaluate supplier criticality and risk impact accordingly **Ex5**: Plan for unexpected supplier and supply chain-related interruptions to ensure business continuity	**Allows for assessment format adjustments, risk and trust validations, tests to validate security trust, and monitoring of risk profiles related to personnel.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	**Ex1**: Define and use rules and protocols for reporting incident response and recovery activities and the status between the organization and its suppliers **Ex2**: Identify and document the roles and responsibilities of the organization and its suppliers for incident response **Ex3**: Include critical suppliers in incident response exercises and simulations **Ex4**: Define and coordinate crisis communication methods and protocols between the organization and its critical suppliers **Ex5**: Conduct collaborative lessons learned sessions with critical suppliers	**Provides the ability to measure soft skills related to supplier personnel roles and responsibilities to ensure proper alignment and capabilities to execute required functions.**
		GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	**Ex1**: Policies and procedures require provenance records for all acquired technology products and services **Ex2**: Periodically provide risk reporting to leaders about how acquired components are proven to be untampered and authentic **Ex3**: Communicate regularly among cybersecurity risk managers and operations personnel about the need to acquire software patches, updates, and upgrades only from authenticated and trustworthy software providers **Ex4**: Review policies to ensure that they require approved supplier personnel to perform maintenance on supplier products **Ex5**: Policies and procedure require checking upgrades to critical hardware for unauthorized changes	**Ensures approved supplier personnel and software providers as related to low risk and high trust factors.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	**Ex1**: Establish processes for terminating critical relationships under both normal and adverse circumstances **Ex2**: Define and implement plans for component end-of-life maintenance support and obsolescence **Ex3**: Verify that supplier access to organization resources is deactivated promptly when it is no longer needed **Ex4**: Verify that assets containing the organization's data are returned or properly disposed of in a timely, controlled, and safe manner **Ex5**: Develop and execute a plan for terminating or transitioning supplier relationships that takes supply chain security risk and resiliency into account **Ex6**: Mitigate risks to data and systems created by supplier termination **Ex7**: Manage data leakage risks associated with supplier termination	**Provides metrics related to risk and trust factors for supplier personnel to trigger reviews for potential termination or correction. Mitigates risks for disgruntled supplier personnel to cause data leaks, intellectual property theft, or security incidents.**
GOVERN (GV)				
IDENTIFY (ID): The organization's current cybersecurity risks are understood				
	Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy			
		ID.AM-01: Inventories of hardware managed by the organization are maintained	**Ex1**: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices **Ex2**: Constantly monitor networks to detect new hardware and automatically update inventories	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	**Ex1**: Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services **Ex2**: Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes **Ex3**: Maintain an inventory of the organization's systems	**NA**
		ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	**Ex1**: Maintain baselines of communication and data flows within the organization's wired and wireless networks **Ex2**: Maintain baselines of communication and data flows between the organization and third parties **Ex3**: Maintain baselines of communication and data flows for the organization's infrastructure-as-a-service (IaaS) usage **Ex4**: Maintain documentation of expected network ports, protocols, and services that are typically used among authorized systems	**Improves internal personnel and external supplier communications capabilities.**
		ID.AM-04: Inventories of services provided by suppliers are maintained	**Ex1**: Inventory all external services used by the organization, including third-party infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; APIs; and other externally hosted application services **Ex2**: Update the inventory when a new external service is going to be utilized to ensure adequate cybersecurity risk management monitoring of the organization's use of that service	**NA**
		ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	**Ex1**: Define criteria for prioritizing each class of assets **Ex2**: Apply the prioritization criteria to assets **Ex3**: Track the asset priorities and update them periodically or when significant changes to the organization occur	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		ID.AM-06: [Withdrawn: Incorporated into GV.RR-02, GV.SC-02]		
		ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	**Ex1**: Maintain a list of the designated data types of interest (e.g., personally identifiable information, protected health information, financial account numbers, organization intellectual property, operational technology data) **Ex2**: Continuously discover and analyze ad hoc data to identify new instances of designated data types **Ex3**: Assign data classifications to designated data types through tags or labels **Ex4**: Track the provenance, data owner, and geolocation of each instance of designated data types	**NA**
		ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	**Ex1**: Integrate cybersecurity considerations throughout the life cycles of systems, hardware, software, and services **Ex2**: Integrate cybersecurity considerations into product life cycles **Ex3**: Identify unofficial uses of technology to meet mission objectives (i.e., shadow IT) **Ex4**: Periodically identify redundant systems, hardware, software, and services that unnecessarily increase the organization's attack surface **Ex5**: Properly configure and secure systems, hardware, software, and services prior to their deployment in production **Ex6**: Update inventories when systems, hardware, software, and services are moved or transferred within the organization **Ex7**: Securely destroy stored data based on the organization's data retention policy using the prescribed destruction method, and keep and manage a record of the destructions **Ex8**: Securely sanitize data storage when hardware is being retired, decommissioned, reassigned, or sent for repairs or replacement **Ex9**: Offer methods for destroying paper, storage media, and other physical forms of	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
	Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization			
		ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	**Ex1**: Use vulnerability management technologies to identify unpatched and misconfigured software **Ex2**: Assess network and system architectures for design and implementation weaknesses that affect cybersecurity **Ex3**: Review, analyze, or test organization-developed software to identify design, coding, and default configuration vulnerabilities **Ex4**: Assess facilities that house critical computing assets for physical vulnerabilities and resilience issues **Ex5**: Monitor sources of cyber threat intelligence for information on new vulnerabilities in products and services **Ex6**: Review processes and procedures for weaknesses that could be exploited to affect cybersecurity	**Vulnerability should include insider threat and human risk vulnerabilites that account for 90% of potential security incidents, such as phishing vulnerabilities. Provides assessments for personnel and suppliers to predict potential human risk vulnerabilities and creates documented reports.**
		ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	**Ex1**: Configure cybersecurity tools and technologies with detection or response capabilities to securely ingest cyber threat intelligence feeds **Ex2**: Receive and review advisories from reputable third parties on current threat actors and their tactics, techniques, and procedures (TTPs) **Ex3**: Monitor sources of cyber threat intelligence for information on the types of vulnerabilities that emerging technologies may have	**Cyber threat intelligence feeds should include human risk data sources that account for 90% of potential security incidents. Provides intelligence feeds using predictive behavioral science algorithms.**
		ID.RA-03: Internal and external threats to the organization are identified and recorded	**Ex1**: Use cyber threat intelligence to maintain awareness of the types of threat actors likely to target the organization and the TTPs they are likely to use **Ex2**: Perform threat hunting to look for signs of threat actors within the environment **Ex3**: Implement processes for identifying internal threat actors	**Provides the ability to implement processes to identify internal threat actors, including unaware personnel prone to mistakes that lead to security incidents.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	**Ex1**: Business leaders and cybersecurity risk management practitioners work together to estimate the likelihood and impact of risk scenarios and record them in risk registers **Ex2**: Enumerate the potential business impacts of unauthorized access to the organization's communications, systems, and data processed in or by those systems **Ex3**: Account for the potential impacts of cascading failures for systems of systems	**Provides comprehensive human risk data to update risk registers.**
		ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	**Ex1**: Develop threat models to better understand risks to the data and identify appropriate risk responses **Ex2**: Prioritize cybersecurity resource allocations and investments based on estimated likelihoods and impacts	**Provides data and reports to better understand human risk elements and identify appropriate risk responses, such as personalized training curriculums.**
		ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	**Ex1**: Apply the vulnerability management plan's criteria for deciding whether to accept, transfer, mitigate, or avoid risk **Ex2**: Apply the vulnerability management plan's criteria for selecting compensating controls to mitigate risk **Ex3**: Track the progress of risk response implementation (e.g., plan of action and milestones [POA&M], risk register, risk detail report) **Ex4**: Use risk assessment findings to inform risk response decisions and actions **Ex5**: Communicate planned risk responses to affected stakeholders in priority order	**Provides data and reports related to human risks and insider threats, as well as documented plans to mitigate risks through training, coaching, and actions.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	**Ex1**: Implement and follow procedures for the formal documentation, review, testing, and approval of proposed changes and requested exceptions **Ex2**: Document the possible risks of making or not making each proposed change, and provide guidance on rolling back changes **Ex3**: Document the risks related to each requested exception and the plan for responding to those risks **Ex4**: Periodically review risks that were accepted based upon planned future actions or milestones	**Provides procedures, documentation, and plans to mitigate human risks and insider threats.**
		ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	**Ex1**: Conduct vulnerability information sharing between the organization and its suppliers following the rules and protocols defined in contracts **Ex2**: Assign responsibilities and verify the execution of procedures for processing, analyzing the impact of, and responding to cybersecurity threat, vulnerability, or incident disclosures by suppliers, customers, partners, and government cybersecurity organizations	**Ensures human risk vulnerability information is documented, quantified, and reported for internal and external sharing. Allows for responsibilities to be assigned based on soft skills and personnel capabilities.**
		ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	**Ex1**: Assess the authenticity and cybersecurity of critical technology products and services prior to acquisition and use	**NA**
		ID.RA-10: Critical suppliers are assessed prior to acquisition	**Ex1**: Conduct supplier risk assessments against business and applicable cybersecurity requirements, including the supply chain	**Allows for human risk assessments missed by others that can account for 90% of security incidents.**
	Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions			

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		ID.IM-01: Improvements are identified from evaluations	**Ex1**: Perform self-assessments of critical services that take current threats and TTPs into consideration **Ex2**: Invest in third-party assessments or independent audits of the effectiveness of the organization's cybersecurity program to identify areas that need improvement **Ex3**: Constantly evaluate compliance with selected cybersecurity requirements through automated means	**Sel-assessments and third-party assessments often miss human risk and insider threat elements that lead to 90% of security incidents. Provides the ability to complete comprehensive personnel and supplier assessments within nine minutes.**
		ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	**Ex1**: Identify improvements for future incident response activities based on findings from incident response assessments (e.g., tabletop exercises and simulations, tests, internal reviews, independent audits) **Ex2**: Identify improvements for future business continuity, disaster recovery, and incident response activities based on exercises performed in coordination with critical service providers and product suppliers **Ex3**: Involve internal stakeholders (e.g., senior executives, legal department, HR) in security tests and exercises as appropriate **Ex4**: Perform penetration testing to identify opportunities to improve the security posture of selected high-risk systems as approved by leadership **Ex5**: Exercise contingency plans for responding to and recovering from the discovery that products or services did not originate with the contracted supplier or partner or were altered before receipt **Ex6**: Collect and analyze performance metrics using security tools and services to inform improvements to the cybersecurity program	**Improvements should include the creation of what Gartner calls a Security Behavior Culture Program (SBCP). Identifies and offers personalized training curriculums, courses, coaching, and security exercises to drive immediate improvements.**
		ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities	**Ex1**: Conduct collaborative lessons learned sessions with suppliers **Ex2**: Annually review cybersecurity policies, processes, and procedures to take lessons learned into account **Ex3**: Use metrics to assess operational cybersecurity performance over time	**Sessions should include human risk and insider threat lessons learned. Provides metrics, reports, and trending for review and operational changes.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	**Ex1**: Establish contingency plans (e.g., incident response, business continuity, disaster recovery) for responding to and recovering from adverse events that can interfere with operations, expose confidential information, or otherwise endanger the organization's mission and viability **Ex2**: Include contact and communication information, processes for handling common scenarios, and criteria for prioritization, escalation, and elevation in all contingency plans **Ex3**: Create a vulnerability management plan to identify and assess all types of vulnerabilities and to prioritize, test, and implement risk responses **Ex4**: Communicate cybersecurity plans (including updates) to those responsible for carrying them out and to affected parties **Ex5**: Review and update all cybersecurity plans annually or when a need for significant improvements is identified	**Plans should include mitigation of human risk elements responsible for 90% of security incidents. Establishes plans to mitigate human risk and insider threat risks and responses, and facilites the ability to communicate plans internally and with suppliers.**
	Business Environment (ID.BE): [Withdrawn: Incorporated into GV.OC]			
		ID.BE-01: [Withdrawn: Incorporated into GV.OC-05]		
		ID.BE-02: [Withdrawn: Incorporated into GV.OC-01]		
		ID.BE-03: [Withdrawn: Incorporated into GV.OC-01]		
		ID.BE-04: [Withdrawn: Incorporated into GV.OC-04, GV.OC-05]		
		ID.BE-05: [Withdrawn: Incorporated into GV.OC-04]		
	Governance (ID.GV): [Withdrawn: Incorporated into GV]			
		ID.GV-01: [Withdrawn: Incorporated into GV.PO, GV.PO-01, GV.PO-02]		
		ID.GV-02: [Withdrawn: Incorporated into GV.OC-02, GV.RR, GV.RR-02]		
		ID.GV-03: [Withdrawn: Moved to GV.OC-03]		

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		ID.GV-04: [Withdrawn: Moved to GV.RM-04]		
	Risk Management Strategy (ID.RM): [Withdrawn: Incorporated into GV.RM]			
		ID.RM-01: [Withdrawn: Incorporated into GV.RM-01, GV.RM-06, GV.RR-03]		
		ID.RM-02: [Withdrawn: Incorporated into GV.RM-02, GV.RM-04]		
		ID.RM-03: [Withdrawn: Moved into GV.RM-02]		
	Supply Chain Risk Management (ID.SC): [Withdrawn: Incorporated into GV.SC]			
		ID.SC-01: [Withdrawn: Incorporated into GV.RM-05, GV.SC-01, GV.SC-06, GV.SC-09, GV.SC-10]		
		ID.SC-02: [Withdrawn: Incorporated into GV.OC-02, GV.SC-03, GV.SC-04, GV.SC-07, ID.RA-10]		
		ID.SC-03: [Withdrawn: Moved to GV.SC-05]		
		ID.SC-04: [Withdrawn: Incorporated into GV.SC-07, ID.RA-10]		
		ID.SC-05: [Withdrawn: Incorporated into GV.SC-08, ID.IM-02]		
IDENTIFY (ID)				
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used				
	Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access			

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	**Ex1**: Initiate requests for new access or additional access for employees, contractors, and others, and track, review, and fulfill the requests, with permission from system or data owners when needed **Ex2**: Issue, manage, and revoke cryptographic certificates and identity tokens, cryptographic keys (i.e., key management), and other credentials **Ex3**: Select a unique identifier for each device from immutable hardware characteristics or an identifier securely provisioned to the device **Ex4**: Physically label authorized hardware with an identifier for inventory and servicing purposes	**Access rights should be dynamically related to personnel and supplier trust and risk metrics. Provides initial and ongoing trust and risk scores to inform Identity Access Management (IAM) and badge access systems to throttle access where appropriate.**
		PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	**Ex1**: Verify a person's claimed identity at enrollment time using government-issued identity credentials (e.g., passport, visa, driver's license) **Ex2**: Issue a different credential for each person (i.e., no credential sharing)	**Identifies potential trust and risk issues with personnel and suppliers proir to allowing access to sensitive information and systems.**
		PR.AA-03: Users, services, and hardware are authenticated	**Ex1**: Require multifactor authentication **Ex2**: Enforce policies for the minimum strength of passwords, PINs, and similar authenticators **Ex3**: Periodically reauthenticate users, services, and hardware based on risk (e.g., in zero trust architectures) **Ex4**: Ensure that authorized personnel can access accounts essential for protecting safety under emergency conditions	**Predictive algorithms help identify individuals at risk for password mismanagement to allow for personalized email filtering, password change requirements, and training.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.AA-04: Identity assertions are protected, conveyed, and verified	**Ex1**: Protect identity assertions that are used to convey authentication and user information through single sign-on systems **Ex2**: Protect identity assertions that are used to convey authentication and user information between federated systems **Ex3**: Implement standards-based approaches for identity assertions in all contexts, and follow all guidance for the generation (e.g., data models, metadata), protection (e.g., digital signing, encryption), and verification (e.g., signature validation) of identity assertions	**NA**
		PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	**Ex1**: Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, and promptly rescind privileges that are no longer needed **Ex2**: Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation, day/time, requester endpoint's cyber health) **Ex3**: Restrict access and privileges to the minimum necessary (e.g., zero trust architecture) **Ex4**: Periodically review the privileges associated with critical business functions to confirm proper separation of duties	**Ensures personnel and supplier Zero Trust by quantifying trust and risk factors, as well as potential disengagement or disgruntled actions to allow for restricted digital and physical access until training and actions can mitigate the risks.**
		PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	**Ex1**: Use security guards, security cameras, locked entrances, alarm systems, and other physical controls to monitor facilities and restrict access **Ex2**: Employ additional physical security controls for areas that contain high-risk assets **Ex3**: Escort guests, vendors, and other third parties within areas that contain business-critical assets	**Allows for personalized physical and badge access rights based on measured trust and risk factors that are non-intrusive.**
	Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks			

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	**Ex1**: Provide basic cybersecurity awareness and training to employees, contractors, partners, suppliers, and all other users of the organization's non-public resources **Ex2**: Train personnel to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials) **Ex3**: Explain the consequences of cybersecurity policy violations, both to individual users and the organization as a whole **Ex4**: Periodically assess or test users on their understanding of basic cybersecurity practices **Ex5**: Require annual refreshers to reinforce existing practices and introduce new practices	**Microsoft reports show only a 3% phishing click reduction after security awareness training (SAT) . Gartner and Forrester agree that traditional one-size-fits-all SAT is obsolete and admonish adopting Human Risk Management (HRM) based on behavioral science. NIH studies show workloads, stress, and trust and primary reasons for phish clicks. Provides HRM assessments and allows for personalized SAT combined with training for trust, stress, leadership, engagement, and more to use HRM to create a Gartner SBCP.**
		PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	**Ex1**: Identify the specialized roles within the organization that require additional cybersecurity training, such as physical and cybersecurity personnel, finance personnel, senior leadership, and anyone with access to business-critical data **Ex2**: Provide role-based cybersecurity awareness and training to all those in specialized roles, including contractors, partners, suppliers, and other third parties **Ex3**: Periodically assess or test users on their understanding of cybersecurity practices for their specialized roles **Ex4**: Require annual refreshers to reinforce existing practices and introduce new practices	**As noted, Microsoft reports show only a 3% phishing click reduction after security awareness training (SAT) . Gartner and Forrester agree that traditional one-size-fits-all SAT is obsolete and admonish adopting Human Risk Management (HRM) based on behavioral science. Training should be personalized based on roles related to soft skills, as well as trust and risk metrics. Provides personalized training that goes beyond only SAT to include factors such as trust, stress, workload balance, hybrid work habits, and more that NIH studies account for most phishing and other incidents.**
		PR.AT-03: [Withdrawn: Incorporated into PR.AT-01, PR.AT-02]		
		PR.AT-04: [Withdrawn: Incorporated into PR.AT-02]		
		PR.AT-05: [Withdrawn: Incorporated into PR.AT-02]		

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
	Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information			
		PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	**Ex1**: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources **Ex2**: Use full disk encryption to protect data stored on user endpoints **Ex3**: Confirm the integrity of software by validating signatures **Ex4**: Restrict the use of removable media to prevent data exfiltration **Ex5**: Physically secure removable media containing unencrypted sensitive information, such as within locked offices or file cabinets	**NA**
		PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	**Ex1**: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of network communications **Ex2**: Automatically encrypt or block outbound emails and other communications that contain sensitive data, depending on the data classification **Ex3**: Block access to personal email, file sharing, file storage services, and other personal communications applications and services from organizational systems and networks **Ex4**: Prevent reuse of sensitive data from production environments (e.g., customer records) in development, testing, and other non-production environments	**NA**
		PR.DS-03: [Withdrawn: Incorporated into ID.AM-08, PR.PS-03]		
		PR.DS-04: [Withdrawn: Moved to PR.IR-04]		
		PR.DS-05: [Withdrawn: Incorporated into PR.DS-01, PR.DS-02, PR.DS-10]		
		PR.DS-06: [Withdrawn: Incorporated into PR.DS-01, DE.CM-09]		

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.DS-07: [Withdrawn: Incorporated into PR.IR-01]		
		PR.DS-08: [Withdrawn: Incorporated into ID.RA-09, DE.CM-09]		
		PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	**Ex1**: Remove data that must remain confidential (e.g., from processors and memory) as soon as it is no longer needed **Ex2**: Protect data in use from access by other users and processes of the same platform	**Helps protect data in use from access by individuals based on low risk or trust factors.**
		PR.DS-11: Backups of data are created, protected, maintained, and tested	**Ex1**: Continuously back up critical data in near-real-time, and back up other data frequently at agreed-upon schedules **Ex2**: Test backups and restores for all types of data sources at least annually **Ex3**: Securely store some backups offline and offsite so that an incident or disaster will not damage them **Ex4**: Enforce geographic separation and geolocation restrictions for data backup storage	**NA**
	Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability			
		PR.PS-01: Configuration management practices are established and applied	**Ex1**: Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality) **Ex2**: Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software **Ex3**: Monitor implemented software for deviations from approved baselines	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	**Ex1**: Perform routine and emergency patching within the timeframes specified in the vulnerability management plan **Ex2**: Update container images, and deploy new container instances to replace rather than update existing instances **Ex3**: Replace end-of-life software and service versions with supported, maintained versions **Ex4**: Uninstall and remove unauthorized software and services that pose undue risks **Ex5**: Uninstall and remove any unnecessary software components (e.g., operating system utilities) that attackers might misuse **Ex6**: Define and implement plans for software and service end-of-life maintenance support and obsolescence	**NA**
		PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	**Ex1**: Replace hardware when it lacks needed security capabilities or when it cannot support software with needed security capabilities **Ex2**: Define and implement plans for hardware end-of-life maintenance support and obsolescence **Ex3**: Perform hardware disposal in a secure, responsible, and auditable manner	**NA**
		PR.PS-04: Log records are generated and made available for continuous monitoring	**Ex1**: Configure all operating systems, applications, and services (including cloud-based services) to generate log records **Ex2**: Configure log generators to securely share their logs with the organization's logging infrastructure systems and services **Ex3**: Configure log generators to record the data needed by zero-trust architectures	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.PS-05: Installation and execution of unauthorized software are prevented	**Ex1**: When risk warrants it, restrict software execution to permitted products only or deny the execution of prohibited and unauthorized software **Ex2**: Verify the source of new software and the software's integrity before installing it **Ex3**: Configure platforms to use only approved DNS services that block access to known malicious domains **Ex4**: Configure platforms to allow the installation of organization-approved software only	**Helps reduce the use of non-authorized software by measuring potential human risks that can lead to misuse, and personalizing training related to misuse.**
		PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	**Ex1**: Protect all components of organization-developed software from tampering and unauthorized access **Ex2**: Secure all software produced by the organization, with minimal vulnerabilities in their releases **Ex3**: Maintain the software used in production environments, and securely dispose of software once it is no longer needed	**NA**
	Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience			

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	**Ex1**: Logically segment organization networks and cloud-based platforms according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests), and permit required communications only between segments **Ex2**: Logically segment organization networks from external networks, and permit only necessary communications to enter the organization's networks from the external networks **Ex3**: Implement zero trust architectures to restrict network access to each resource to the minimum necessary **Ex4**: Check the cyber health of endpoints before allowing them to access and use production resources	**Segmentation and Zero Trust architectures should include and restrict access based on human risks and insider threat metrics. Provides documented trust and risk scores for personnel and suppliers to establish segmentation and access rights.**
		PR.IR-02: The organization's technology assets are protected from environmental threats	**Ex1**: Protect organizational equipment from known environmental threats, such as flooding, fire, wind, and excessive heat and humidity **Ex2**: Include protection from environmental threats and provisions for adequate operating infrastructure in requirements for service providers that operate systems on the organization's behalf	**NA**
		PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	**Ex1**: Avoid single points of failure in systems and infrastructure **Ex2**: Use load balancing to increase capacity and improve reliability **Ex3**: Use high-availability components like redundant storage and power supplies to improve system reliability	**NA**
		PR.IR-04: Adequate resource capacity to ensure availability is maintained	**Ex1**: Monitor usage of storage, power, compute, network bandwidth, and other resources **Ex2**: Forecast future needs, and scale resources accordingly	**NA**
	Identity Management, Authentication and Access Control (PR.AC): [Withdrawn: Moved to PR.AA]			
		PR.AC-01: [Withdrawn: Incorporated into PR.AA-01, PR.AA-05]		

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.AC-02: [Withdrawn: Moved to PR.AA-06]		
		PR.AC-03: [Withdrawn: Incorporated into PR.AA-03, PR.AA-05, PR.IR-01]		
		PR.AC-04: [Withdrawn: Moved to PR.AA-05]		
		PR.AC-05: [Withdrawn: Incorporated into PR.IR-01]		
		PR.AC-06: [Withdrawn: Moved to PR.AA-02]		
		PR.AC-07: [Withdrawn: Moved to PR.AA-03]		
	Information Protection Processes and Procedures (PR.IP): [Withdrawn: Incorporated into other Categories and Functions]			
		PR.IP-01: [Withdrawn: Incorporated into PR.PS-01]		
		PR.IP-02: [Withdrawn: Incorporated into ID.AM-08, PR.PS-06]		
		PR.IP-03: [Withdrawn: Incorporated into PR.PS-01, ID.RA-07]		
		PR.IP-04: [Withdrawn: Moved to PR.DS-11]		
		PR.IP-05: [Withdrawn: Moved to PR.IR-02]		
		PR.IP-06: [Withdrawn: Incorporated into ID.AM-08]		
		PR.IP-07: [Withdrawn: Incorporated into ID.IM, ID.IM-03]		
		PR.IP-08: [Withdrawn: Moved to ID.IM-03]		
		PR.IP-09: [Withdrawn: Moved to ID.IM-04]		
		PR.IP-10: [Withdrawn: Incorporated into ID.IM-02, ID.IM-04]		
		PR.IP-11: [Withdrawn: Moved to GV.RR-04]		
		PR.IP-12: [Withdrawn: Incorporated into ID.RA-01, PR.PS-02]		
	Maintenance (PR.MA): [Withdrawn: Incorporated into ID.AM-08]			
		PR.MA-01: [Withdrawn: Incorporated into ID.AM-08, PR.PS-03]		
		PR.MA-02: [Withdrawn: Incorporated into ID.AM-08, PR.PS-02]		
	Protective Technology (PR.PT): [Withdrawn: Incorporated into other Protect Categories]			
		PR.PT-01: [Withdrawn: Incorporated into PR.PS-04]		

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		PR.PT-02: [Withdrawn: Incorporated into PR.DS-01, PR.PS-01]		
		PR.PT-03: [Withdrawn: Incorporated into PR.PS-01]		
		PR.PT-04: [Withdrawn: Incorporated into PR.AA-06, PR.IR-01]		
		PR.PT-05: [Withdrawn: Moved to PR.IR-03]		
PROTECT (PR)				
DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed				
	Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events			
		DE.CM-01: Networks and network services are monitored to find potentially adverse events	**Ex1**: Monitor DNS, BGP, and other network services for adverse events **Ex2**: Monitor wired and wireless networks for connections from unauthorized endpoints **Ex3**: Monitor facilities for unauthorized or rogue wireless networks **Ex4**: Compare actual network flows against baselines to detect deviations **Ex5**: Monitor network communications to identify changes in security postures for zero trust purposes	**NA**
		DE.CM-02: The physical environment is monitored to find potentially adverse events	**Ex1**: Monitor logs from physical access control systems (e.g., badge readers) to find unusual access patterns (e.g., deviations from the norm) and failed access attempts **Ex2**: Review and monitor physical access records (e.g., from visitor registration, sign-in sheets) **Ex3**: Monitor physical access controls (e.g., locks, latches, hinge pins, alarms) for signs of tampering **Ex4**: Monitor the physical environment using alarm systems, cameras, and security guards	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	**Ex1**: Use behavior analytics software to detect anomalous user activity to mitigate insider threats **Ex2**: Monitor logs from logical access control systems to find unusual access patterns and failed access attempts **Ex3**: Continuously monitor deception technology, including user accounts, for any usage	**Provides the behavior analytics software to detect potential anomalous activity and mitigate insider threats.**
		DE.CM-04: [Withdrawn: Incorporated into DE.CM-01, DE.CM-09]		
		DE.CM-05: [Withdrawn: Incorporated into DE.CM-01, DE.CM-09]		
		DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	**Ex1**: Monitor remote and onsite administration and maintenance activities that external providers perform on organizational systems **Ex2**: Monitor activity from cloud-based services, internet service providers, and other service providers for deviations from expected behavior	**Provides predictive metrics to mitigate deviations from expected behaviors by personnel and suppliers.**
		DE.CM-07: [Withdrawn: Incorporated into DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09]		
		DE.CM-08: [Withdrawn: Incorporated into ID.RA-01]		
		DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	**Ex1**: Monitor email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks and exfiltration, and other adverse events **Ex2**: Monitor authentication attempts to identify attacks against credentials and unauthorized credential reuse **Ex3**: Monitor software configurations for deviations from security baselines **Ex4**: Monitor hardware and software for signs of tampering **Ex5**: Use technologies with a presence on endpoints to detect cyber health issues (e.g., missing patches, malware infections, unauthorized software), and redirect the endpoints to a remediation environment before access is authorized	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
	Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents			
		DE.AE-01: [Withdrawn: Incorporated into ID.AM-03]		
		DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	**Ex1**: Use security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity **Ex2**: Utilize up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise **Ex3**: Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation **Ex4**: Use log analysis tools to generate reports on their findings	**Cyber threat intelligence feeds should include human risk data sources that account for 90% of potential security incidents. Provides intelligence feeds using predictive behavioral science algorithms.**
		DE.AE-03: Information is correlated from multiple sources	**Ex1**: Constantly transfer log data generated by other sources to a relatively small number of log servers **Ex2**: Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources **Ex3**: Utilize cyber threat intelligence to help correlate events among log sources	**Cyber threat intelligence feeds should include human risk data sources that account for 90% of potential security incidents. Provides intelligence feeds using predictive behavioral science algorithms.**
		DE.AE-04: The estimated impact and scope of adverse events are understood	**Ex1**: Use SIEMs or other tools to estimate impact and scope, and review and refine the estimates **Ex2**: A person creates their own estimates of impact and scope	**NA**
		DE.AE-05: [Withdrawn: Moved to DE.AE-08]		

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		DE.AE-06: Information on adverse events is provided to authorized staff and tools	**Ex1**: Use cybersecurity software to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools **Ex2**: Incident responders and other authorized personnel can access log analysis findings at all times **Ex3**: Automatically create and assign tickets in the organization's ticketing system when certain types of alerts occur **Ex4**: Manually create and assign tickets in the organization's ticketing system when technical staff discover indicators of compromise	
		DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	**Ex1**: Securely provide cyber threat intelligence feeds to detection technologies, processes, and personnel **Ex2**: Securely provide information from asset inventories to detection technologies, processes, and personnel **Ex3**: Rapidly acquire and analyze vulnerability disclosures for the organization's technologies from suppliers, vendors, and third-party security advisories	**NA**
		DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	**Ex1**: Apply incident criteria to known and assumed characteristics of activity in order to determine whether an incident should be declared **Ex2**: Take known false positives into account when applying incident criteria	**Provides predictive incident criteria related to human risk and insider threat elements.**
	Detection Processes (DE.DP): [Withdrawn: Incorporated into other Categories and Functions]			
		DE.DP-01: [Withdrawn: Incorporated into GV.RR-02]		
		DE.DP-02: [Withdrawn: Incorporated into DE.AE]		
		DE.DP-03: [Withdrawn: Incorporated into ID.IM-02]		
		DE.DP-04: [Withdrawn: Incorporated into DE.AE-06]		

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		DE.DP-05: [Withdrawn: Incorporated into ID.IM, ID.IM-03]		
DETECT (DE)				
RESPOND (RS): Actions regarding a detected cybersecurity incident are taken				
	Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed			
		RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	**Ex1**: Detection technologies automatically report confirmed incidents **Ex2**: Request incident response assistance from the organization's incident response outsourcer **Ex3**: Designate an incident lead for each incident **Ex4**: Initiate execution of additional cybersecurity plans as needed to support incident response (for example, business continuity and disaster recovery)	**Allows for soft skill and capability metrics to determine appropriate incident leads for each type of incident.**
		RS.MA-02: Incident reports are triaged and validated	**Ex1**: Preliminarily review incident reports to confirm that they are cybersecurity-related and necessitate incident response activities **Ex2**: Apply criteria to estimate the severity of an incident	**NA**
		RS.MA-03: Incidents are categorized and prioritized	**Ex1**: Further review and categorize incidents based on the type of incident (e.g., data breach, ransomware, DDoS, account compromise) **Ex2**: Prioritize incidents based on their scope, likely impact, and time-critical nature **Ex3**: Select incident response strategies for active incidents by balancing the need to quickly recover from an incident with the need to observe the attacker or conduct a more thorough investigation	**Should include insider incidents. Provides metrics to categorize and prioritize incidents. Ensures appropriate insider incident response including personalized training.**
		RS.MA-04: Incidents are escalated or elevated as needed	**Ex1**: Track and validate the status of all ongoing incidents **Ex2**: Coordinate incident escalation or elevation with designated internal and external stakeholders	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		RS.MA-05: The criteria for initiating incident recovery are applied	**Ex1**: Apply incident recovery criteria to known and assumed characteristics of the incident to determine whether incident recovery processes should be initiated **Ex2**: Take the possible operational disruption of incident recovery activities into account	**Should include insider incidents. Provides metrics to categorize and prioritize incidents. Ensures appropriate insider incident response including personalized training.**
	Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities			
		RS.AN-01: [Withdrawn: Incorporated into RS.MA-02]		
		RS.AN-02: [Withdrawn: Incorporated into RS.MA-02, RS.MA-03, RS.MA-04]		
		RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	**Ex1**: Determine the sequence of events that occurred during the incident and which assets and resources were involved in each event **Ex2**: Attempt to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident **Ex3**: Analyze the incident to find the underlying, systemic root causes **Ex4**: Check any cyber deception technology for additional information on attacker behavior	**Provides insider threat actor vulnerabilities metrics and analyzing underlying, systemic root causes related to human factors such as stress, workloads, leadership, training, etc.**
		RS.AN-04: [Withdrawn: Moved to RS.MA-03]		
		RS.AN-05: [Withdrawn: Moved to ID.RA-08]		
		RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	**Ex1**: Require each incident responder and others (e.g., system administrators, cybersecurity engineers) who perform incident response tasks to record their actions and make the record immutable **Ex2**: Require the incident lead to document the incident in detail and be responsible for preserving the integrity of the documentation and the sources of all information being reported	**Provides details related to incident response based on insider threats, including personalized training completion and scores related to underlying root causes.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	**Ex1**: Collect, preserve, and safeguard the integrity of all pertinent incident data and metadata (e.g., data source, date/time of collection) based on evidence preservation and chain-of-custody procedures	**NA**
		RS.AN-08: An incident's magnitude is estimated and validated	**Ex1**: Review other potential targets of the incident to search for indicators of compromise and evidence of persistence **Ex2**: Automatically run tools on targets to look for indicators of compromise and evidence of persistence	**NA**
	Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies			
		RS.CO-01: [Withdrawn: Incorporated into PR.AT-01]		
		RS.CO-02: Internal and external stakeholders are notified of incidents	**Ex1**: Follow the organization's breach notification procedures after discovering a data breach incident, including notifying affected customers **Ex2**: Notify business partners and customers of incidents in accordance with contractual requirements **Ex3**: Notify law enforcement agencies and regulatory bodies of incidents based on criteria in the incident response plan and management approval	**NA**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		RS.CO-03: Information is shared with designated internal and external stakeholders	**Ex1**: Securely share information consistent with response plans and information sharing agreements **Ex2**: Voluntarily share information about an attacker's observed TTPs, with all sensitive data removed, with an Information Sharing and Analysis Center (ISAC) **Ex3**: Notify HR when malicious insider activity occurs **Ex4**: Regularly update senior leadership on the status of major incidents **Ex5**: Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers **Ex6**: Coordinate crisis communication methods between the organization and its critical suppliers	**Provides detailed information and metrics related to insider threats and human risks to notify HR. Offers reports and metrics for senior leadership related to human risks. Facilitates crisis communications within the organization and with suppliers.**
		RS.CO-04: [Withdrawn: Incorporated into RS.MA-01, RS.MA-04]		
		RS.CO-05: [Withdrawn: Incorporated into RS.CO-03]		
	Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects			
		RS.MI-01: Incidents are contained	**Ex1**: Cybersecurity technologies (e.g., antivirus software) and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform containment actions **Ex2**: Allow incident responders to manually select and perform containment actions **Ex3**: Allow a third party (e.g., internet service provider, managed security service provider) to perform containment actions on behalf of the organization **Ex4**: Automatically transfer compromised endpoints to a remediation virtual local area network (VLAN)	**Provides metrics and reports for incident responders and third parties related to human risk and insider threat elements. Allows containment actions to include personalized training, coaching, and actions to mitigate future incidents.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		RS.MI-02: Incidents are eradicated	**Ex1**: Cybersecurity technologies and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform eradication actions **Ex2**: Allow incident responders to manually select and perform eradication actions **Ex3**: Allow a third party (e.g., managed security service provider) to perform eradication actions on behalf of the organization	**NA**
		RS.MI-03: [Withdrawn: Incorporated into ID.RA-06]		
	Response Planning (RS.RP): [Withdrawn: Incorporated into RS.MA]			
		RS.RP-01: [Withdrawn: Incorporated into RS.MA-01]		
	Improvements (RS.IM): [Withdrawn: Incorporated into ID.IM]			
		RS.IM-01: [Withdrawn: Incorporated into ID.IM-03, ID.IM-04]		
		RS.IM-02: [Withdrawn: Incorporated into ID.IM-03]		
RESPOND (RS)				
RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored				
	Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents			
		RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	**Ex1**: Begin recovery procedures during or after incident response processes **Ex2**: Make all individuals with recovery responsibilities aware of the plans for recovery and the authorizations required to implement each aspect of the plans	**Recovery should include proper mitigation of future human risk and insider threat incidents, such as personalized training, coaching, and assessments. Provides for this.**
		RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	**Ex1**: Select recovery actions based on the criteria defined in the incident response plan and available resources **Ex2**: Change planned recovery actions based on a reassessment of organizational needs and resources	**Recovery should include proper mitigation of future human risk and insider threat incidents, such as personalized training, coaching, and assessments. Provides for this.**

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	**Ex1**: Check restoration assets for indicators of compromise, file corruption, and other integrity issues before use	**NA**
		RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	**Ex1**: Use business impact and system categorization records (including service delivery objectives) to validate that essential services are restored in the appropriate order **Ex2**: Work with system owners to confirm the successful restoration of systems and the return to normal operations **Ex3**: Monitor the performance of restored systems to verify the adequacy of the restoration	**NA**
		RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	**Ex1**: Check restored assets for indicators of compromise and remediation of root causes of the incident before production use **Ex2**: Verify the correctness and adequacy of the restoration actions taken before putting a restored system online	**NA**
		RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	**Ex1**: Prepare an after-action report that documents the incident itself, the response and recovery actions taken, and lessons learned **Ex2**: Declare the end of incident recovery once the criteria are met	**Provides metrics and reports related to human-related incidents, such as stress, work, leadership, and disengagement factors, to create comprehensive after-action reports.**
	Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties			
		RC.CO-01: [Withdrawn: Incorporated into RC.CO-04]		
		RC.CO-02: [Withdrawn: Incorporated into RC.CO-04]		

Function	Category	Subcategory	Implementation Examples	HermanCyber Solutions & Services Relevant to Requirements
		RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	**Ex1**: Securely share recovery information, including restoration progress, consistent with response plans and information sharing agreements **Ex2**: Regularly update senior leadership on recovery status and restoration progress for major incidents **Ex3**: Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers **Ex4**: Coordinate crisis communication between the organization and its critical suppliers	**Provides metrics and reports related to human-related incidents, such as stress, work, leadership, and disengagement factors, to update senior leadership.**
		RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	**Ex1**: Follow the organization's breach notification procedures for recovering from a data breach incident **Ex2**: Explain the steps being taken to recover from the incident and to prevent a recurrence	**Offers the ability to provide detailed plans and steps being taken, such as personalized training, to prevent recurrances based on human risk elements.**
	Improvements (RC.IM): [Withdrawn: Incorporated into ID.IM]			
		RC.IM-01: [Withdrawn: Incorporated into ID.IM-03, ID.IM-04]		
		RC.IM-02: [Withdrawn: Incorporated into ID.IM-03]		
RECOVER (RC)				