Niveluri de implementare

FOCUS AREA	TIER 1 PARTIAL	TIER 2 RISK INFORMED	TIER 3 REPEATABLE	TIER 4 ADAPTIVE
Risk Management Process	• Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. • Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	• Risk management practices are approved by management but may not be established as organizational-wide policy. • Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	• The organization's risk management practices are formally approved and expressed as policy. • Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.	• The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. • Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
Integrated Risk Management Program	• There is limited awareness of cybersecurity risk at the organizational level. • The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. • The organization may not have processes that enable cybersecurity information to be shared within the organization.	• There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. • Cybersecurity information is shared within the organization on an informal basis. • Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. • Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.	• There is an organization-wide approach to manage cybersecurity risk. • Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. • Consistent methods are in place to respond effectively to changes in risk. • Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. • The organization consistently and accurately monitors cybersecurity risk of organizational assets. • Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. • Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.	• There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. • The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. • Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. • The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. • Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. • The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.
External Participation	• The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. • The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. • The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.	• Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. • The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. • Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.	• The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. • It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. • The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. • Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.	• The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. • It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. • The organization shares that information internally and externally with other collaborators. • The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. • Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.
People	• CybersecurRy • professionals (staff) and the general employee population have had little to no cybersecurtty¬related training. • The staff has a limited or nonexistent training • Security awareness is limited. • Employees have little or no awareness of company security resources and escalation paths.	• The staff and employees have received cybersecurity¬related training. • The staff has a training pipeline. • There man awareness of cybersecurity risk at the organizational level. • Employees have a general awareness of security and company security resources and escalation paths.	• The staff possesses the knowledge and skills to perform their appointed roles and responsibilities. • Employees should receive regular cybersecurity¬related training and briefings. • The staff has a robust training pipeline, including Internal and external security conferences or training opportunities. • Organization and business units have a security champion or dedicated security staff.	• The staffs knowledge and skills are regularly reviewed for currency and applicability and new skills, and knowledge needs are identified and addressed. • Employees receive regular cybersecunty-related training and briefings on relevant and emerging security topics. • The staff has a robust training pipeline and routinely attend internal and external security conferences or training opportunities.
Technology	• Tools to help manage cybersecurity risk are not deployed, not supported, or insufficient to address risks. • Tools may be in place but are not adequately tuned or maintained. • Technology deployed lags current threats. • Tool deployment may not adequately cover risk areas.	• Tools are deployed and supported to address identified risks. • The tools in deployment are tuned and maintained when resources are available. • The technology deployed, for the most part, keeps pace with current threats. • Tool coverage of the risk area is complete when deployed.	• Tools are deployed and supported to address identified risks. • The tools in deployment are tuned and maintained when resources are available. • The technology deployed, for the most part, keeps pace with current threats. • Tool coverage of the risk area is complete when deployed.	• The tools deployed In the environment are regularly reviewed for effectiveness and coverage against changes in the threat environment and internal ecosystem. • The tools and technology deployed anticipate emerging threats.