CPRIM Artifacts - Detailed risks identified by NCSF, with the respective subcategories.

Category	Subcategory	Normative reference	Risk identified	Impacts ModBus TCP?	Impacts Inverter?
Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 ISO/IEC 27001:2013 A.8.1.1, A. 8.1.2	The absence of asset inventory and responsible definitions can compromise asset management, access authorization, and identification of accountable parties.	Yes	Yes
	ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 ISO/IEC 27001:2013 A.8.1.1, A. 8.1.2, A.12.5.1	The absence of software inventory can compromise software management and owners' identification.	Yes	Yes
	ID.AM-3: Organizational communication and data flows are mapped	CIS CSC 12 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2	The absence of organizational communication mapping and data flow can hinder comprehensive device management and attacks against network services.	Yes	Yes
	ID.AM-4: External information systems are catalogued	CIS CSC 12 ISO/IEC 27001:2013 A.11.2.6	It does not apply, out of scope.	No	No
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their ratings, criticality, and business value	CIS CSC 13, 14 ISO/IEC 27001:2013 A.8.2.1	The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of network security threats and effective information management.	Yes	Yes
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CIS CSC 17, 19 ISO/IEC 27001:2013 A.6.1.1	It does not apply, out of scope.	No	No
Business Context (ID.BE)	D.BE-1: The organization's role in the supply chain is identified and communicated	ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A. 15.2.2	It does not apply, out of scope.	No	No
	ID.BE-2: The organization's place in critical infrastructure and its industrial sector is identified and communicated	ISO/IEC 27001:2013 Item 4.1	It does not apply, out of scope.	No	No
	D.BE-3: Priorities for organizational mission, objectives and activities are established and communicated	ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6	It does not apply, out of scope.	No	No
	D.BE-4: Dependencies and functions critical to the delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3	It does not apply, out of scope.	No	No
	ID.BE-5: Resilience requirements to support the delivery of critical services are established for all operational conditions (e.g., under coercion/attack, during recovery, normal operations)	ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1	The absence of security requirements and controls for management can hinder the management and control of information security.	Yes	Yes
Governance (ID.GV)	ID. GV-1: Organizational cybersecurity policy is established and communicated	CIS CSC 19	The absence of standards for reporting incidents and response procedures can compromise incident response and management.	Yes	Yes
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal functions and external partners	CIS CSC 19	The absence of defined roles and responsibilities can hinder the mapping, documentation, and handling of cybersecurity incidents.	Yes	Yes
	ID.GV-3: Legal and regulatory requirements relating to cybersecurity, including privacy and civil liberties obligations, are understood and managed	CIS CSC 19	It does not apply, out of scope.	No	No
	ID.GV-4: Governance and risk management processes address cybersecurity risks	ID.GV-4: Governance and risk	The absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersecurity risks.	Yes	Yes
Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	CIS CSC 4 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3	The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management and compliance analysis.	Yes	Yes
	ID.RA-2: Information about cyber threats is received from forums and information sharing sources	CIS CSC 4	The absence of specialized forums for mapping cyber threats can hinder the management of such threats.	Yes	Yes
	ID.RA-3: Internal and external threats are identified and documented	CIS CSC 4 ISO/IEC 27001:2013 Cláusula 6.1.2	The absence of identification and documentation of internal threats can compromise asset integrity.	Yes	Yes
	ID.RA-4: Potential business impacts and probabilities are identified in the organization	CIS CSC 4 ISO/IEC 27001:2013 A.16.1.6, Cláusula 6.1.2	It does not apply, out of scope.	No	No

	ID.RA-5: Threats, vulnerabilities, probabilities and impacts are used to determine risks	CIS CSC 4 ISO/IEC 27001:2013 A.12.6.1	The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information about these vulnerabilities and impede the definition of criteria for software installation.	Yes	Yes
	ID.RA-6: Risk responses are identified and prioritized	CIS CSC 4 ISO/IEC 27001:2013 Cláusula 6.1.3	The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information security risks.	Yes	Yes
Risk Management Strategy (ID. RM)	ID.RM-1: Risk management processes are established, managed, and approved by organizational stakeholders	CIS CSC 4 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001: 2013 Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3	It does not apply, out of scope.	No	No
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	CIS CSC 4 ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3	It does not apply, out of scope.	No	No
	ID.RM-3: The organization's risk tolerance determination is permeated by its role in critical infrastructure and industry-specific risk analysis	CIS CSC 4 ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3	It does not apply, out of scope.	No	No
Supply Chain Risk Management (ID.SC)	ID.SC-1: Cyber supply chain risk management processes are identified, established, evaluated, managed, and agreed upon by the organization's stakeholders.	CIS CSC 4 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A. 15.2.2	It does not apply, out of scope.	No	No
	ID.SC-1: Cyber supply chain risk management processes are identified, established, evaluated, managed, and agreed upon by the organization's stakeholders.	ISO/IEC 27001:2013 A.15.2.1, A.15.2.2	It does not apply, out of scope.	No	No
	ID.SC-3: Contracts with third-party suppliers and partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and the Cyber Supply Chain Risk Management Plan	ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3	It does not apply, out of scope.	No	No
	ID.SC-4: Suppliers and third-party partners are systematically evaluated through audits, test results, or other forms of assessments to confirm that they are meeting their contractual obligations	ISO/IEC 27001:2013 A.15.2.1, A.15.2.2	It does not apply, out of scope.	No	No
	ID.SC-5: Response and recovery planning and testing is performed with third-party service providers and providers	ISO/IEC 27001:2013 A.17.1.3	It does not apply, out of scope.	No	No