NIST-Based Cybersecurity GAP Assessment

PROJECT SUMMARY

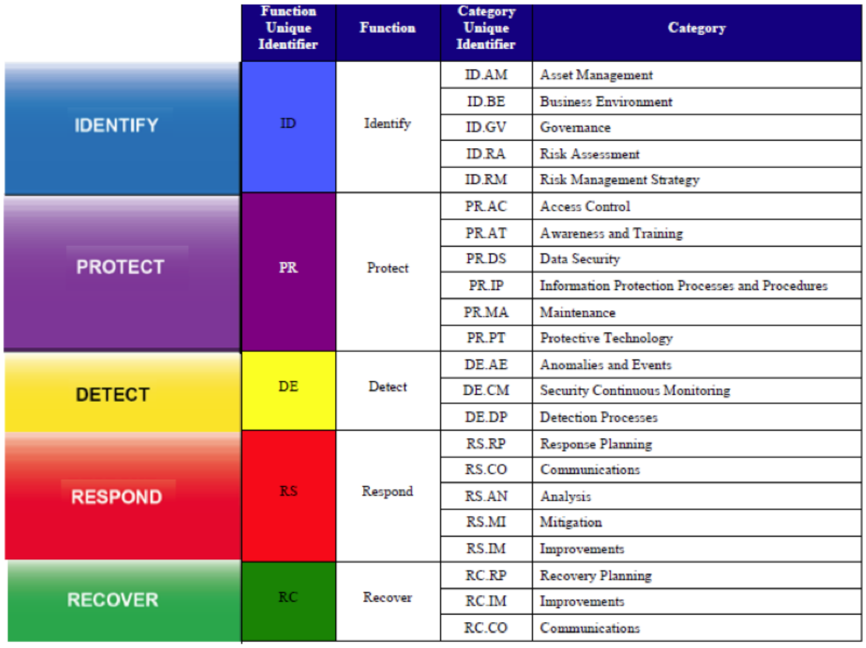
exida is a leader in Industrial Control Systems (ICS) Cybersecurity and specializes in the Process Control Network (PCN), in terms of performing Risk Assessments, Vulnerability Assessments, and Gap Assessments. As part of this service, exida offers a low-cost gap assessment based upon the National Institute of Standards Technology (NIST) Cybersecurity framework that will determine a company's general cybersecurity posture.

BACKGROUND

Process control systems have long been known to be critical to the health, safety, welfare, and economic stability of the public at large. Recognizing this fact in 2013, the president issued Presidential executive order 13636 "Improving Critical Infrastructure Cybersecurity." The policy calls for the development of a voluntary risk-based Cybersecurity Framework. Based on sets of existing industry standards, policies, and guidelines, developed to be technology neutral, and designed to be used as a template to guide an organization in its cybersecurity activities and focus, the resulting framework is now known as the NIST Cybersecurity Framework.

This framework is not a prescriptive document as are other published standards and regulations. Instead this document allows the organization to determine where they currently stand against a number of categories and at the same time determine where they would like to stand.

The determination of how the company stands up against a predefined matrix determines the Tier for each category. The aggregation of the Tiers determines the Profile for each of the Functions. The exercise identifies the gap between the Current Profile and the Target Profile. The framework does not give prescriptive solutions on how to achieve the desired Target Profile, but it does lay out a roadmap to guide where activities and energies should be most effectively applied

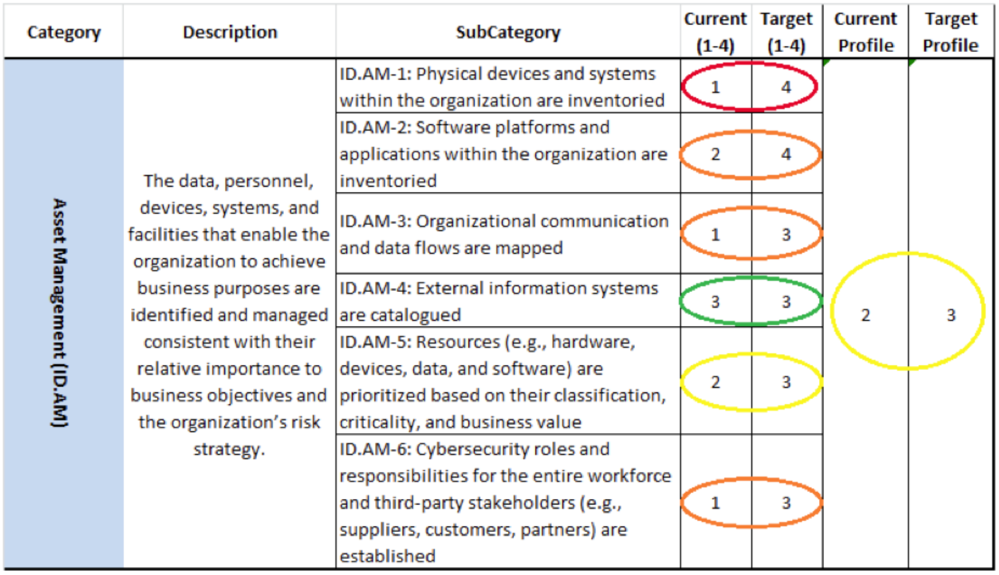


	Function Unique Identifier	Function	Category Unique Identifier	Category
IDENTIFY	ID	Identify	ID.AM	Asset Management
			ID.BE	Business Environment
			ID.GV	Governance
			ID.RA	Risk Assessment
			ID.RM	Risk Management Strategy
PROTECT	PR	Protect	PR.AC	Access Control
			PR.AT	Awareness and Training
			PR.DS	Data Security
			PR.IP	Information Protection Processes and Procedures
			PR.MA	Maintenance
			PR.PT	Protective Technology
DETECT	DE	Detect	DE.AE	Anomalies and Events
			DE.CM	Security Continuous Monitoring
			DE.DP	Detection Processes
RESPOND	RS	Respond	RS.RP	Response Planning
			RS.CO	Communications
			RS.AN	Analysis
			RS.MI	Mitigation
			RS.IM	Improvements
RECOVER	RC	Recover	RC.RP	Recovery Planning
			RC.IM	Improvements
			RC.CO	Communications

Using the Functions, Categories, and Subcategories as detailed in the NIST Cybersecurity Framework as a guide, let exida work with you. We will spend 3 to 4 hours determining your Current and Target profiles, giving you valuable insight into where you are doing well and where some more effort should be applied.

(continued)

Based on the results of the exercise, exida will provide recommendations and suggestions specific to your organization on how to proceed, where you can accomplish tasks yourself, and where outside expertise would be beneficial.



Category	Description	SubCategory	Current (1-4)	Target (1-4)	Current Profile	Target Profile
Asset Management (ID.AM)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	1	4	2	3
		ID.AM-2: Software platforms and applications within the organization are inventoried	2	4		
		ID.AM-3: Organizational communication and data flows are mapped	1	3		
		ID.AM-4: External information systems are catalogued	3	3		
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	2	3		
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	1	3		

BASIC **SERVICE** & **BENEFITS**

WHAT WE OFFER

- Quick non-time or personnel intrusive method of gauging current cybersecurity posture as compared against a target of where the company wants to be
- Based on NIST Cybersecurity Framework
- Low cost as compared to full assessment
- Does not require invasive discovery in and around the control system

WHY IT IS WORTH IT

- Easy gauge to determine if further detailed review is necessary
- Does not entail intrusion in to ICS systems and the facility
- ½ day approx. vs multiple day engagement

WHAT WE WILL DO

- Provide the Tier descriptions and a short training on the process
- Spend a small period of time interviewing those knowledgeable about your control system asking standardized questions and applying a 4 level response.
- Produce a summary of the findings and recommendations