**Comments on NIST CSF 2.0 Concept Paper**

Eoghan Casey, Mar 1, 2023

First and foremost, I commend NIST's impressive initiative to improve cybersecurity, and I expect the enhanced CSF 2.0 will continue to influence cybersecurity practices and regulations worldwide.

A quick introduction: Throughout my career, I have helped organizations investigate and recover from severe security breaches, including network intrusions with international scope. Until recently, I was in a Senior Executive Service (SES) strategic leadership position at the DoD Cyber Crime Center (DC3), with responsibilities for enhancing capabilities, strategic collaborations, and advancing standards and practices related to cybersecurity. Now I am VP of Cybersecurity Strategy & Product Development at OwnBackup, creating innovative solutions for cloud data security and incident response.

The recommendations below predominantly relate to NIST's encouragement for feedback about incident response and recovery outcomes that might be missing from the CSF that should be considered in CSF 2.0. When recommendations impact other areas, this is noted. The last recommendation to add a Report category could cover all cybersecurity governance reporting requirements, providing motivation for the CSF to have a new Governance function.

**Summary**

The NIST Cyber Security Framework (CSF) currently constrains incident response to rapid containment and remediation activities, which is wrong for two reasons. Firstly, incident management (see #1 below) is an integral part of the cybersecurity lifecycle and is a process of continuous improvement as detailed in NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide). Secondly, quick containment and recovery raises the risks of incomplete scope assessment such as undetected compromised machines, domain level administrator access, unknown attacker objectives, and alerting perpetrators that their activities have been noticed which allows them to take evasive action and entrench themselves more stealthily. Modern cyber attacks are carefully planned and executed to make detection and recovery difficult, targeting multiple systems simultaneously to maximize impact and taking precautions to conceal traces of exploitation and compromise. Effective incident response and recovery depends on assessing the scope of an incident to inform subsequent decisions (see #3 below).

**1. Incident Management (ID.IR, PR.IR, DE.IR, RS.IR, RC.IR)**

An integral part of a cybersecurity is being prepared to manage cybersecurity incidents, including preparing, planning, coordinating, documenting, communicating, escalating, and reporting. Effective incident management lessens the impact of an incident (downtime, cost, reputational harm), and uses lessons learned from incidents to enhance cybersecurity capability maturity. Associated preparations and processes are introduced by NIST SP 800-61 Rev. 2, but are somewhat dated by the more recent NIST publication Developing Cyber-Resilient Systems (NIST SP 800-160 Vol. 2 Rev. 1). Incident management requires work within each function of the CSF.

- **ID.IR**: Preparing to manage incidents effectively and efficiently starts with planning, including documented procedures, assigned responsibilities, necessary tools and training. Identify situations in which quick containment is likely to reduce the impact of particular incidents to avoid making hasty decisions (see #3 below). Performing incident response drills helps identify gaps in technology, personnel, training, and data sources that are necessary for effective incident management.
- **PR.IR**: Properly preserving data sources to be used for detecting, responding to, and recovering from an incident. Although NIST CSF addresses retention of data such as logs, it does not provide guidance on how to prove their integrity and provenance/lineage from the time they were generated. The integrity of data sources required for incident response is crucial because logs and backups can be targeted in cyber incidents for deletion/corruption, and may be required as proof of regulatory compliance or as evidence supporting legal action. Proper preservation and documentation of data sources hinges on maintaining the provenance/lineage of data sources. In a cyber security context, some data sources such as logs can be tracked from the moment they are generated, not just when a problem is detected and incident response operations begin.
- **DE.IR (adequately covered by DE.AE, DE.CM, and DE.DP)**: Proactive monitoring of preserved/protected data sources is an important part of incident management, to detect problems early. Documenting and communicating potential problems is essential to avoid overlooked warning signs and missed opportunities to prevent progression of an incident, which is a common mishap in serious incidents.
- **RS.IR (propose renaming RS.RP)**: Effective incident management is most critical and challenging during the response to an evolving problem, and is essentially an exercise in managing fear and frustration. Managing such an incident can be a difficult task, requiring technical personnel to be deployed and large amounts of information to be analyzed. At this stage, incident management involves planning and coordinating the overall response process, assessing risks, maintaining communication between those involved, and documenting important activities and outcomes. Continuous communication is critical to keep everyone updated on developments such as newly discovered digital artifacts (e.g., malware, stolen data) or recent security actions (e.g., system reconfiguration, data alteration). Ideally, an incident response team should function as a unit, thinking as one. Daily debriefings and status updates (preferably encrypted) can help with the necessary exchange of information among team members. Valuable time can be wasted when one uninformed person misinterprets a planned reconfiguration of a system as a part of the incident, and reacts incorrectly. Documenting all actions and findings related to an incident in a centralized location or on an email list not only helps keep everyone on the same page, but also helps avoid confusion and misunderstanding that can waste invaluable time.
- **RC.IR (propose renaming RC.RP)**: Careful planning is required before executing recovery operations to avoid exacerbating problems and to ensure successful outcomes, which include scope assessment (see #3 below). From NIST Guide for Cybersecurity Event Recovery (SP 800-184): "*Understanding that initiation of the recovery activities*

*might alert the adversary if the IR team has not fully identified the adversaries' presence within the environment, the recovery team works with the IR team to increase the level of monitoring and strengthen the isolation capabilities. This is accomplished by heightening the network defenses to look for lateral movements based on a set of indicators of compromise that have been generated by the IR team. This helps validate the adversary's presence on impacted systems.*"

Incorporating incident response management into all functions of the CSF 2.0 will facilitate alignment of international counterparts such as the UK National Cyber Security Center (NCSC) Incident Management guidance (https://www.ncsc.gov.uk/collection/incident-management).

**2. Rename and Reinforce Analysis (RS.AN -> RS.IV)**

The term Investigate would better describe the process and outcomes covered under the current Analysis category (RS.AN). Analysis is actually a subcategory of Investigate, which is evident from the subcategories, which includes performing forensic analysis and scope assessment (see #3 below). This category can be reinforced using the incident analysis and documentation aspects of the incident handling analysis guidance in NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide) and NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response).

Recommend renaming the Analysis (RS.AN) category to Investigate RS.IV, and describe this as "Investigation is conducted to ensure effective response and support recovery activities."

**3. Respond and Scope Assessment (RS.IV-5)**

The typical reaction to a cyber security incident is to return to normal operations immediately. This is an understandable and intuitive response. Continued business disruption costs revenue, raises risks and liability, and increases total damages. Unfortunately, a hasty response can be counterproductive, potentially creating more problems than it solves. For this reason, before rushing to recovery, it is essential to conduct some scope assessment to inform decisions.

The objective of scope assessment is to see if the cyber security incident is still occurring, and to determine the scale and impact of the incident. NIST SP 800-61 Rev. 2 (Section 3.2.4), states that "*the [incident response] team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.*"

Scope of time is particularly important because the incident could have started well before it was detected. Therefore, it is advisable to reconstruct a detailed timeline of the incident to understand the sequence of events before, during, and after the incident. Documenting the timeline of an incident helps identify areas that require additional investigation. Organizations that are not prepared to handle an incident that began long ago find it very difficult to determine

when an incident started and to fix the root cause to prevent future problems. To avoid such difficulties, the continuous monitoring measures of the NIST CSF (DE.CM and DE.DP) can be bolstered by incident handling practices to ensure that these data sources are properly preserved.

Recommend adding scope assessment subcategory under Respond as a subcategory of Investigate (RS.IV-5), assuming adoption of proposed renaming in #2 above.

**4. Recover (Tactical): Timely, Precise, and Reliable (RC.TC)**
Executing recovery operations has a number of challenges that need to be addressed in NIST CSF 2.0:

a. **Timely**: It is important to be able to recover systems/data in a timely manner. Cyberinsurers have been reported to have paid the ransom in situations where the victim organization had backups but the time and cost of recovery would exceed the ransom amount.
b. **Precise**: It is only necessary to restore what was impacted by an incident. Rather than having an all-or-nothing restoration process, organizations need technical solutions that can restore specific data, files, or systems precisely. An organization that lacks precision restoration capabilities will waste resources restoring data, files, and systems unnecessarily. The ability to ascertain specifically what was impacted by an incident relates back to scope assessment.
c. **Reliable (pre-recovery)**: It is essential to be able to verify the integrity of a data source that is being used to restore normal operations. If the cyber security incident began before the data source was preserved, then it could already have been compromised, rendering it untrustworthy for recovery purposes. The ability to determine whether or not a specific data source was impacted by an incident relates back to scope assessment, and is addressed by the Data Integrity practice guide (NIST CP 1800-25: https://www.nccoe.nist.gov/publication/1800-25/): "*the information produced by integrity monitoring systems can be used to inform a recovery process; they provide information about what changes happened, when changes began to take place, as well as what programs were involved in the changes.*"
d. **Reliable (post-recovery)**: It is important to be able to validate that recovery operations completed successfully, restoring data, files, or systems to their correct state.

NIST CSF 2.0 could align with risk management practices by emphasizing the importance of setting a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for mission-critical systems and data sources.

**5. Prevent Future Incidents by Remediating Root Cause (RC.RC)**
In addition to continuous improvement of response (RS.IM) and recovery activities (RC.IM), the NIST CSF needs to explicitly list "ameliorating the security weakness(es) that enabled the cyber incident" as an outcome. This is dependent on the ability to ascertain root cause, which relates back to incident investigation and scope assessment.

**6. Reporting and Legal Requirements (expand RS.CO-2 or extend in new GV function)**
There are multiple reasons that reports are required during and after an incident, and the current coverage of this in RS.CO-2 is weak. Reporting includes keeping stakeholders updated on progress and outcomes, consolidating incident resolution and lessons learned, and using after action review to improve organizational capability maturity levels for incident management specifically, and cybersecurity generally. Depending on the situation, reporting may be required by organizational policy, regulatory compliance, and law enforcement. Reporting is the final phase of the forensic process described in NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response).

There are multiple reasons that reports are required during and after an incident. These include keeping stakeholders updated on progress and outcomes, consolidating incident resolution and lessons learned, and using after action review to improve organizational capability maturity levels for incident management specifically, and cybersecurity generally. Depending on the situation, reporting may be required by organizational policy or regulatory compliance.

Cyber security incidents are becoming more damaging and costly, and regulatory penalties are rising. As the stakes/impact increases, organizations need to be prepared for regulatory reporting and legal action which requires trustworthy information of probative value, highlighting the aforementioned need for proper preservation and documentation of data sources (data provenance/lineage).

Cyber security regulations have routine reporting requirements to ensure compliance. Therefore, an organization's cyber security program should be setup to produce documentation routinely that shows proof of compliance.

Some incidents can lead to legal action (e.g., termination, prosecution). Attorneys need concrete evidence of a policy violation or crime and its apparent source to pursue legal action. It is critical that the information provided to attorneys is complete and accurate, since the actions they take can have broad consequences, potentially terminating employment of suspected individuals. For example, mistyping an IP address or failing to adjust for time zone differences can result in the wrong person being subjected to the attention of legal action.

Managed security service providers are assisting customers with security incidents without adhering to well established digital forensic principles and processes. They have insufficiently trained personnel preserving data sources without documenting provenance/lineage details for authentication purposes. In addition, these personnel search network level data for specific information, but do not preserve the original data source properly for future authentication and analysis. The manner in which data sources were (and were not) preserved can create challenges when a security incident leads to litigation.

Reporting could be treated more generally than a category of Response (RS.RP), and could be a category of a new Governance function (GV.RP) to include regulatory reporting requirements.

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| | **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 organizational objectives and the organization's risk strategy. | **ID.AM-1:** Physical devices and systems within the organization are inventoried | · **CIS CSC** 1<br>· **COBIT 5** BAI09.01, BAI09.02<br>· **ISA 62443-2-1:2009** 4.2.3.4<br>· **ISA 62443-3-3:2013** SR 7.8<br>· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>· **NIST SP 800-53 Rev. 4** CM-8, PM-5 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | · **CIS CSC** 2<br>· **COBIT 5** BAI09.01, BAI09.02, BAI09.05<br>· **ISA 62443-2-1:2009** 4.2.3.4<br>· **ISA 62443-3-3:2013** SR 7.8<br>· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1<br>· **NIST SP 800-53 Rev. 4** CM-8, PM-5 |
| | | **ID.AM-3:** Organizational communication and data flows are mapped | · **CIS CSC** 12<br>· **COBIT 5** DSS05.02<br>· **ISA 62443-2-1:2009** 4.2.3.4<br>· **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2<br>· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 |
| | | **ID.AM-4:** External information systems are catalogued | · **CIS CSC** 12<br>· **COBIT 5** APO02.02, APO10.04, DSS01.02<br>· **ISO/IEC 27001:2013** A.11.2.6<br>· **NIST SP 800-53 Rev. 4** AC-20, SA-9 |
| | | **ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | · **CIS CSC** 13, 14<br>· **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02<br>· **ISA 62443-2-1:2009** 4.2.3.6<br>· **ISO/IEC 27001:2013** A.8.2.1<br>· **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6 |
| | | **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<br>· **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03<br>· **ISA 62443-2-1:2009** 4.3.2.3.3<br>· **ISO/IEC 27001:2013** A.6.1.1<br>· **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11 |
| | **Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk | **ID.BE-1:** The organization's role in the supply chain is identified and communicated | · **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>· **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2<br>· **NIST SP 800-53 Rev. 4** CP-2, SA-12 |
| | | **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | · **COBIT 5** APO02.06, APO03.01<br>· **ISO/IEC 27001:2013** Clause 4.1<br>· **NIST SP 800-53 Rev. 4** PM-8 |
| | | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | · **COBIT 5** APO02.01, APO02.06, APO03.01<br>· **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6<br>· **NIST SP 800-53 Rev. 4** PM-11, SA-14 |

| | | | |
|---|---|---|---|
| IDENTIFY (ID) | management decisions. | **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established | · **COBIT 5** APO10.01, BAI04.02, BAI09.02<br>· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3<br>· **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14 |
| | | **ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | · **COBIT 5** BAI03.02, DSS04.02<br>· **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>· **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14 |
| | **Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | **ID.GV-1:** Organizational cybersecurity policy is established and communicated | · **CIS CSC** 19<br>· **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02<br>· **ISA 62443-2-1:2009** 4.3.2.6<br>· **ISO/IEC 27001:2013** A.5.1.1<br>· **NIST SP 800-53 Rev. 4** -1 controls from all security control families |
| | | **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners | · **CIS CSC** 19<br>· **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04<br>· **ISA 62443-2-1:2009** 4.3.2.3.3<br>· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1<br>· **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2 |
| | | **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | · **CIS CSC** 19<br>· **COBIT 5** BAI02.01, MEA03.01, MEA03.04<br>· **ISA 62443-2-1:2009** 4.4.3.7<br>· **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5<br>· **NIST SP 800-53 Rev. 4** -1 controls from all security control families |
| | | **ID.GV-4:** Governance and risk management processes address cybersecurity risks | · **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02<br>· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3<br>· **ISO/IEC 27001:2013** Clause 6<br>· **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 |
| | **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | **ID.RA-1:** Asset vulnerabilities are identified and documented | · **CIS CSC** 4<br>· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02<br>· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12<br>· **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3<br>· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 |
| | | **ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources | · **CIS CSC** 4<br>· **COBIT 5** BAI08.01<br>· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12<br>· **ISO/IEC 27001:2013** A.6.1.4<br>· **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16 |
| | | **ID.RA-3:** Threats, both internal and external, are identified and documented | · **CIS CSC** 4<br>· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04<br>· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12<br>· **ISO/IEC 27001:2013** Clause 6.1.2<br>· **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16 |
| | | | · **CIS CSC** 4 |

| | | | |
|---|---|---|---|
| | | **ID.RA-4:** Potential business impacts and likelihoods are identified | · **COBIT 5** DSS04.02<br>· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12<br>· **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2<br>· **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11 |
| | | **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | · **CIS CSC** 4<br>· **COBIT 5** APO12.02<br>· **ISO/IEC 27001:2013** A.12.6.1<br>· **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16 |
| | | **ID.RA-6:** Risk responses are identified and prioritized | · **CIS CSC** 4<br>· **COBIT 5** APO12.05, APO13.02<br>· **ISO/IEC 27001:2013** Clause 6.1.3<br>· **NIST SP 800-53 Rev. 4** PM-4, PM-9 |
| | **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | · **CIS CSC** 4<br>· **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02<br>· **ISA 62443-2-1:2009** 4.3.4.2<br>· **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3<br>· **NIST SP 800-53 Rev. 4** PM-9 |
| | | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | · **COBIT 5** APO12.06<br>· **ISA 62443-2-1:2009** 4.3.2.6.5<br>· **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3<br>· **NIST SP 800-53 Rev. 4** PM-9 |
| | | **ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | · **COBIT 5** APO12.02<br>· **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3<br>· **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11 |
| | **Incident Response Management (ID.IR):** The organization's policies, priorities, and processes are established and used to support incident response decisions.<br><br>**Change Note:** Net new category to incorporate requirements for incident resposne management**.** | **ID.IR-1:** Incident response policies, plans, and procedures are established, including documented procedures, assigned responsibilities, necessary tools and training. | · **ISO/IEC 27041:2015**<br>· **NIST SP 800-61 Rev. 2** |
| | | **ID.IR-2:** The organization identifies situations in which quick containment is likely to reduce the impact of particular incidents to avoid making hasty decisions. | |
| | **Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk | **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders | · **CIS CSC** 4<br>· **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03,<br>· **ISA 62443-2-1:2009** 4.3.4.2<br>· **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2<br>· **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9 |
| | | **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process | · **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03,<br>· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10,<br>· **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2<br>· **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 |
| | | **ID.SC-3:** Contracts with suppliers and third-party partners are | · **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 |

| | | | |
|---|---|---|---|
| | The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. | **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. | · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7<br>· **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3<br>· **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9 |
| | | **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | · **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03,<br>· **ISA 62443-2-1:2009** 4.3.2.6.7<br>· **ISA 62443-3-3:2013** SR 6.1<br>· **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2<br>· **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12 |
| | | **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers | · **CIS CSC** 19, 20<br>· **COBIT 5** DSS04.04<br>· **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11<br>· **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4<br>· **ISO/IEC 27001:2013** A.17.1.3<br>· **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9 |
| | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | **PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | · **CIS CSC** 1, 5, 15, 16<br>· **COBIT 5** DSS05.04, DSS06.03<br>· **ISA 62443-2-1:2009** 4.3.3.5.1<br>· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9<br>· **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3<br>· **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, |
| | | **PR.AC-2:** Physical access to assets is managed and protected | · **COBIT 5** DSS01.04, DSS05.05<br>· **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8<br>· **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.<br>· **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 |
| | | **PR.AC-3:** Remote access is managed | · **CIS CSC** 12<br>· **COBIT 5** APO13.01, DSS01.04, DSS05.03<br>· **ISA 62443-2-1:2009** 4.3.3.6.6<br>· **ISA 62443-3-3:2013** SR 1.13, SR 2.6<br>· **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1<br>· **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15 |
| | | **PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | · **CIS CSC** 3, 5, 12, 14, 15, 16, 18<br>· **COBIT 5** DSS05.04<br>· **ISA 62443-2-1:2009** 4.3.3.7.3<br>· **ISA 62443-3-3:2013** SR 2.1<br>· **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5<br>· **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 |
| | | **PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation) | · **CIS CSC** 9, 14, 15, 18<br>· **COBIT 5** DSS01.05, DSS05.02<br>· **ISA 62443-2-1:2009** 4.3.3.4<br>· **ISA 62443-3-3:2013** SR 3.1, SR 3.8<br>· **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 |

| | | | |
|---|---|---|---|
| | | | · **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7 |
| | | **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions | · **CIS CSC**, 16<br>· **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03<br>· **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4<br>· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1<br>· **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1<br>· **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, |
| | | **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) | · **CIS CSC** 1, 12, 15, 16<br>· **COBIT 5** DSS05.04, DSS05.10, DSS06.10<br>· **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, [illegible]<br>· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10<br>· **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4<br>· **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, |
| | **Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. | **PR.AT-1:** All users are informed and trained | · **CIS CSC** 17, 18<br>· **COBIT 5** APO07.03, BAI05.07<br>· **ISA 62443-2-1:2009** 4.3.2.4.2<br>· **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1<br>· **NIST SP 800-53 Rev. 4** AT-2, PM-13 |
| | | **PR.AT-2:** Privileged users understand their roles and responsibilities | · **CIS CSC** 5, 17, 18<br>· **COBIT 5** APO07.02, DSS05.04, DSS06.03<br>· **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3<br>· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2<br>· **NIST SP 800-53 Rev. 4** AT-3, PM-13 |
| | | **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities | · **CIS CSC** 17<br>· **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05<br>· **ISA 62443-2-1:2009** 4.3.2.4.2<br>· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2<br>· **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16 |
| | | **PR.AT-4:** Senior executives understand their roles and responsibilities | · **CIS CSC** 17, 19<br>· **COBIT 5** EDM01.01, APO01.02, APO07.03<br>· **ISA 62443-2-1:2009** 4.3.2.4.2<br>· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2<br>· **NIST SP 800-53 Rev. 4** AT-3, PM-13 |
| | | **PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities | · **CIS CSC** 17<br>· **COBIT 5** APO07.03<br>· **ISA 62443-2-1:2009** 4.3.2.4.2<br>· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2<br>· **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13 |
| | | **PR.DS-1:** Data-at-rest is protected | · **CIS CSC** 13, 14<br>· **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06<br>· **ISA 62443-3-3:2013** SR 3.4, SR 4.1 |

| | | | |
|---|---|---|---|
| PROTECT (PR) | **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | | · **ISO/IEC 27001:2013** A.8.2.3<br>· **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28 |
| | | **PR.DS-2:** Data-in-transit is protected | · **CIS CSC** 13, 14<br>· **COBIT 5** APO01.06, DSS05.02, DSS06.06<br>· **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2<br>· **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3<br>· **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12 |
| | | **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition | · **CIS CSC** 1<br>· **COBIT 5** BAI09.03<br>· **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1<br>· **ISA 62443-3-3:2013** SR 4.2<br>· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7<br>· **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16 |
| | | **PR.DS-4:** Adequate capacity to ensure availability is maintained | · **CIS CSC** 1, 2, 13<br>· **COBIT 5** APO13.01, BAI04.04<br>· **ISA 62443-3-3:2013** SR 7.1, SR 7.2<br>· **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1<br>· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5 |
| | | **PR.DS-5:** Protections against data leaks are implemented | · **CIS CSC** 13<br>· **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02<br>· **ISA 62443-3-3:2013** SR 5.2<br>· **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.<br>· **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, |
| | | **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity | · **CIS CSC** 2, 3<br>· **COBIT 5** APO01.06, BAI06.01, DSS06.02<br>· **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8<br>· **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4<br>· **NIST SP 800-53 Rev. 4** SC-16, SI-7 |
| | | **PR.DS-7:** The development and testing environment(s) are separate from the production environment | · **CIS CSC** 18, 20<br>· **COBIT 5** BAI03.08, BAI07.04<br>· **ISO/IEC 27001:2013** A.12.1.4<br>· **NIST SP 800-53 Rev. 4** CM-2 |
| | | **PR.DS-8:** Integrity checking mechanisms are used to verify hardware integrity | · **COBIT 5** BAI03.05<br>· **ISA 62443-2-1:2009** 4.3.4.4.4<br>· **ISO/IEC 27001:2013** A.11.2.4<br>· **NIST SP 800-53 Rev. 4** SA-10, SI-7 |
| | | **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) | · **CIS CSC** 3, 9, 11<br>· **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05<br>· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3<br>· **ISA 62443-3-3:2013** SR 7.6<br>· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 |

| | | |
|---|---|---|
| | | · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 |
| | **PR.IP-2:** A System Development Life Cycle to manage systems is implemented | · **CIS CSC** 18<br>· **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03<br>· **ISA 62443-2-1:2009** 4.3.4.3.3<br>· **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5<br>· **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI- |
| | **PR.IP-3:** Configuration change control processes are in place | · **CIS CSC** 3, 11<br>· **COBIT 5** BAI01.06, BAI06.01<br>· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3<br>· **ISA 62443-3-3:2013** SR 7.6<br>· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4<br>· **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10 |
| | **PR.IP-4:** Backups of information are conducted, maintained, and tested | · **CIS CSC** 10<br>· **COBIT 5** APO13.01, DSS01.01, DSS04.07<br>· **ISA 62443-2-1:2009** 4.3.4.3.9<br>· **ISA 62443-3-3:2013** SR 7.3, SR 7.4<br>· **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3<br>· **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9 |
| | **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met | · **COBIT 5** DSS01.04, DSS05.05<br>· **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6<br>· **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3<br>· **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 |
| **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. | **PR.IP-6:** Data is destroyed according to policy | · **COBIT 5** BAI09.03, DSS05.06<br>· **ISA 62443-2-1:2009** 4.3.4.4.4<br>· **ISA 62443-3-3:2013** SR 4.2<br>· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7<br>· **NIST SP 800-53 Rev. 4** MP-6 |
| | **PR.IP-7:** Protection processes are improved | · **COBIT 5** APO11.06, APO12.06, DSS04.05<br>· **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8<br>· **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10<br>· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 |
| | **PR.IP-8:** Effectiveness of protection technologies is shared | · **COBIT 5** BAI08.04, DSS03.04<br>· **ISO/IEC 27001:2013** A.16.1.6<br>· **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4 |
| | **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | · **CIS CSC** 19<br>· **COBIT 5** APO12.06, DSS04.03<br>· **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1<br>· **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3<br>· **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 |
| | | · **CIS CSC** 19, 20<br>· **COBIT 5** DSS04.04 |

| | | | |
|---|---|---|---|
| | | **PR.IP-10:** Response and recovery plans are tested | · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11<br>· **ISA 62443-3-3:2013** SR 3.3<br>· **ISO/IEC 27001:2013** A.17.1.3<br>· **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14 |
| | | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | · **CIS CSC** 5, 16<br>· **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05<br>· **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3<br>· **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4<br>· **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 |
| | | **PR.IP-12:** A vulnerability management plan is developed and implemented | · **CIS CSC** 4, 18, 20<br>· **COBIT 5** BAI03.10, DSS05.01, DSS05.02<br>· **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3<br>· **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2 |
| | **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. | **PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools | · **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05<br>· **ISA 62443-2-1:2009** 4.3.3.3.7<br>· **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6<br>· **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6 |
| | | **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | · **CIS CSC** 3, 5<br>· **COBIT 5** DSS05.04<br>· **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8<br>· **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1<br>· **NIST SP 800-53 Rev. 4** MA-4 |
| | **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | · **CIS CSC** 1, 3, 5, 6, 14, 15, 16<br>· **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01<br>· **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4<br>· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12<br>· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1<br>· **NIST SP 800-53 Rev. 4** AU Family |
| | | **PR.PT-2:** Removable media is protected and its use restricted according to policy | · **CIS CSC** 8, 13<br>· **COBIT 5** APO13.01, DSS05.02, DSS05.06<br>· **ISA 62443-3-3:2013** SR 2.3<br>· **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9<br>· **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 |
| | | **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | · **CIS CSC** 3, 11, 14<br>· **COBIT 5** DSS05.02, DSS05.05, DSS06.06<br>· **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7,<br>· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9,<br>· **ISO/IEC 27001:2013** A.9.1.2<br>· **NIST SP 800-53 Rev. 4** AC-3, CM-7 |
| | | | · **CIS CSC** 8, 12, 15<br>· **COBIT 5** DSS05.02, APO13.01 |

| | | | |
|---|---|---|---|
| | | **PR.PT-4:** Communications and control networks are protected | · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1,<br>· **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3<br>· **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC- |
| | | **PR.PT-5:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | · **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05<br>· **ISA 62443-2-1:2009** 4.3.2.5.2<br>· **ISA 62443-3-3:2013** SR 7.1, SR 7.2<br>· **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1<br>· **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 |
| | **Incident Management (PR.IR):** Data sources necessary for incident response are properly preserved to guarantee their integrity and provenance. | **PR.IR-1:** Protect the integrity of data sources required for incident response in a manner that is verifiable and provable | · **NIST SP 800-61 Rev. 2**<br>· **ISO/IEC 27037:2012** |
| | | **PR.PR-2:** Track the provenance/lineage of data sources required for incident response in a manner that is producible and provable for reliability and legal purposes. | · **NIST SP 800-61 Rev. 2**<br>· **ISO/IEC 27037:2012** |
| | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed | · **CIS CSC** 1, 4, 6, 12, 13, 15, 16<br>· **COBIT 5** DSS03.01<br>· **ISA 62443-2-1:2009** 4.4.3.3<br>· **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2<br>· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4 |
| | | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | · **CIS CSC** 3, 6, 13, 15<br>· **COBIT 5** DSS05.07<br>· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2<br>· **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4<br>· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4 |
| | | **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors | · **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16<br>· **COBIT 5** BAI08.02<br>· **ISA 62443-3-3:2013** SR 6.1<br>· **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7<br>· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 |
| | | **DE.AE-4:** Impact of events is determined | · **CIS CSC** 4, 6<br>· **COBIT 5** APO12.06, DSS03.01<br>· **ISO/IEC 27001:2013** A.16.1.4<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4 |
| | | | · **CIS CSC** 6, 19<br>· **COBIT 5** APO12.06, DSS03.01 |

| | | | |
|---|---|---|---|
| **DETECT (DE)** | | **DE.AE-5:** Incident alert thresholds are established | · **ISA 62443-2-1:2009** 4.2.3.10<br>· **ISO/IEC 27001:2013** A.16.1.4<br>· **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 |
| | **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | **DE.CM-1:** The network is monitored to detect potential cybersecurity events | · **CIS CSC** 1, 7, 8, 12, 13, 15, 16<br>· **COBIT 5** DSS01.03, DSS03.05, DSS05.07<br>· **ISA 62443-3-3:2013** SR 6.2<br>· **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 |
| | | **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events | · **COBIT 5** DSS01.04, DSS01.05<br>· **ISA 62443-2-1:2009** 4.3.3.3.8<br>· **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2<br>· **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20 |
| | | **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events | · **CIS CSC** 5, 7, 14, 16<br>· **COBIT 5** DSS05.07<br>· **ISA 62443-3-3:2013** SR 6.2<br>· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3<br>· **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 |
| | | **DE.CM-4:** Malicious code is detected | · **CIS CSC** 4, 7, 8, 12<br>· **COBIT 5** DSS05.01<br>· **ISA 62443-2-1:2009** 4.3.4.3.8<br>· **ISA 62443-3-3:2013** SR 3.2<br>· **ISO/IEC 27001:2013** A.12.2.1<br>· **NIST SP 800-53 Rev. 4** SI-3, SI-8 |
| | | **DE.CM-5:** Unauthorized mobile code is detected | · **CIS CSC** 7, 8<br>· **COBIT 5** DSS05.01<br>· **ISA 62443-3-3:2013** SR 2.4<br>· **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2<br>· **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44 |
| | | **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events | · **COBIT 5** APO07.06, APO10.05<br>· **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1<br>· **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4 |
| | | **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed | · **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16<br>· **COBIT 5** DSS05.02, DSS05.05<br>· **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1<br>· **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 |
| | | **DE.CM-8:** Vulnerability scans are performed | · **CIS CSC** 4, 20<br>· **COBIT 5** BAI03.10, DSS05.01<br>· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7<br>· **ISO/IEC 27001:2013** A.12.6.1<br>· **NIST SP 800-53 Rev. 4** RA-5 |
| | | **DE.DP-1:** Roles and responsibilities for detection are well defined | · **CIS CSC** 19<br>· **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 |

| | | | |
|---|---|---|---|
| | **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. | **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability | · **ISA 62443-2-1:2009** 4.4.3.1<br>· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2<br>· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14 |
| | | **DE.DP-2:** Detection activities comply with all applicable requirements | · **COBIT 5** DSS06.01, MEA03.03, MEA03.04<br>· **ISA 62443-2-1:2009** 4.4.3.2<br>· **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3<br>· **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14 |
| | | **DE.DP-3:** Detection processes are tested | · **COBIT 5** APO13.02, DSS05.02<br>· **ISA 62443-2-1:2009** 4.4.3.2<br>· **ISA 62443-3-3:2013** SR 3.3<br>· **ISO/IEC 27001:2013** A.14.2.8<br>· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14 |
| | | **DE.DP-4:** Event detection information is communicated | · **CIS CSC** 19<br>· **COBIT 5** APO08.04, APO12.06, DSS02.05<br>· **ISA 62443-2-1:2009** 4.3.4.5.9<br>· **ISA 62443-3-3:2013** SR 6.1<br>· **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3<br>· **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4 |
| | | **DE.DP-5:** Detection processes are continuously improved | · **COBIT 5** APO11.06, APO12.06, DSS04.05<br>· **ISA 62443-2-1:2009** 4.4.3.4<br>· **ISO/IEC 27001:2013** A.16.1.6<br>· **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 |
| | **~~Response Planning (RS.RP):~~** ~~Response processes and procedures are executed...~~<br>**Incident Management (RS.IR):** Incident is managed according to response plan & legal requirements, to ensure effective and efficient response to detected cyber security incident<br>**Change Note:** Name change to account for the scope of activities that occur under this Category. "Management" is more appropriate than "Planning". | **RS.IR-1:** Response plan is executed during or after an incident<br><br>**Change Note:** Subcat letter designation changed to reflect Category name change. | · **CIS CSC** 19<br>· **COBIT 5** APO12.06, BAI01.10<br>· **ISA 62443-2-1:2009** 4.3.4.5.1<br>· **ISO/IEC 27001:2013** A.16.1.5<br>· **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 |
| | | **RS.IR-2:** Incident is properly managed, including coordinating, documenting, communicating, escalating, and reporting<br><br>**Change Note:** Net new subcategory. See accompanying document for justification | · **NIST SP 800-61 Rev. 2**<br>· **ISO/IEC 27043:2015** |
| | | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | · **CIS CSC** 19<br>· **COBIT 5** EDM03.02, APO01.02, APO12.03<br>· **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4<br>· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1<br>· **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 |
| | | **RS.CO-2:** Incidents are reported consistent with established criteria | · **CIS CSC** 19<br>· **COBIT 5** DSS01.03<br>· **ISA 62443-2-1:2009** 4.3.4.5.5<br>· **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2<br>· **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8 |

| | | | |
|---|---|---|---|
| **RESPOND (RS)** | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | **RS.CO-3:** Information is shared consistent with response plans | · **CIS CSC** 19<br>· **COBIT 5** DSS03.04<br>· **ISA 62443-2-1:2009** 4.3.4.5.2<br>· **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2<br>· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 |
| | | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans | · **CIS CSC** 19<br>· **COBIT 5** DSS03.04<br>· **ISA 62443-2-1:2009** 4.3.4.5.5<br>· **ISO/IEC 27001:2013** Clause 7.4<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| | | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | · **CIS CSC** 19<br>· **COBIT 5** BAI08.04<br>· **ISO/IEC 27001:2013** A.6.1.4<br>· **NIST SP 800-53 Rev. 4** SI-5, PM-15 |
| | ~~**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.~~<br><br>**Investigation (RS.IV):** Investigation is conducted to ensure effective response and support recovery activities.<br><br>**Change Note:** Name change to account for the scope of activities that occur under this Category. "Investigation" is more appropriate than "Analysis". | ~~**RS.AN-1:** **RS.IV-1:** Notifications from detection systems are investigated.~~<br><br>**Change Note:** Subcat letter designation changed to reflect Category name change. | · **CIS CSC** 4, 6, 8, 19<br>· **COBIT 5** DSS02.04, DSS02.07<br>· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>· **ISA 62443-3-3:2013** SR 6.1<br>· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5<br>· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 |
| | | ~~**RS.AN-5:** **RS.IV-2:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)~~<br><br>**Change Notes:**<br>- Subcat letter designation changed to reflect Category name change.<br>- Moved to an earlier position in list of subcats. | · **CIS CSC** 4, 19<br><br>· **COBIT 5** EDM03.02, DSS05.07<br><br>· **NIST SP 800-53 Rev. 4** SI-5, PM-15 |
| | | ~~**RS.AN-3:** **RS.IV-3:** Forensics are performed~~<br><br>**Change Notes:** Subcat letter designation changed to reflect Category name change. | · **COBIT 5** APO12.06, DSS03.02, DSS05.07<br>· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1<br>· **ISO/IEC 27001:2013** A.16.1.7<br>· **NIST SP 800-53 Rev. 4** AU-7, IR-4 |
| | | ~~**RS.AN-4:** **RS.IV-4:** Incidents are categorized consistent with response plans~~<br><br>**Change Notes:** Subcat letter designation changed to reflect Category name change. | · **CIS CSC** 19<br>· **COBIT 5** DSS02.02<br>· **ISA 62443-2-1:2009** 4.3.4.5.6<br>· **ISO/IEC 27001:2013** A.16.1.4<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8 |
| | | **RS.IV-5:** The scope of the incident is fully assessed, optimally including root cause(s) and timeline of the incident<br>**Change Note:** Net new subcategory. See accompanying document for justification | · **NIST SP 800-61 Rev. 2**<br>· **ISO/IEC 27042:2015**<br>· **NIST SP 800-86** |

| | | | |
|---|---|---|---|
| | | for justification. | |
| | | **~~RS.AN-2:~~ RS.IV-6:** The impact of the incident is understood<br><br>**Change Notes:**<br>- Subcat letter designation changed to reflect Category name change.<br>- Moved to a later position in list of subcats. | · **COBIT 5** DSS02.02<br><br>· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>· **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4 |
| | **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. | **RS.MI-1:** Incidents are contained | · **CIS CSC** 19<br>· **COBIT 5** APO12.06<br>· **ISA 62443-2-1:2009** 4.3.4.5.6<br>· **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4<br>· **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5<br>· **NIST SP 800-53 Rev. 4** IR-4 |
| | | **RS.MI-2:** Incidents are mitigated | · **CIS CSC** 4, 19<br>· **COBIT 5** APO12.06<br>· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10<br>· **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5<br>· **NIST SP 800-53 Rev. 4** IR-4 |
| | | **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks | · **CIS CSC** 4<br>· **COBIT 5** APO12.06<br>· **ISO/IEC 27001:2013** A.12.6.1<br>· **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5 |
| | **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | **RS.IM-1:** Response plans incorporate lessons learned | · **COBIT 5** BAI01.13<br>· **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4<br>· **ISO/IEC 27001:2013** A.16.1.6, Clause 10<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| | | **RS.IM-2:** Response strategies are updated | · **COBIT 5** BAI01.13, DSS04.08<br>· **ISO/IEC 27001:2013** A.16.1.6, Clause 10<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| | **~~Recovery Planning~~ Incident Management (RC.IRRP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. | **RC.IRRP-1:** Recovery plan is executed during or after a cybersecurity incident<br><br>**Change Note:** Subcat letter designation changed to reflect Category name change from "Planning" to "Management" | · **CIS CSC** 10<br>· **COBIT 5** APO12.06, DSS02.05, DSS03.04<br>· **ISO/IEC 27001:2013** A.16.1.5<br>· **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 |
| | **Tactical (RC.TC):** Tactical measures to ensure timely, precise, reliable recovery.<br><br>**Change Note:** Net new category. See accompanying document for justification. | **RC.TC-1:** Verify reliability of data both before recovery operations (clean), and after recovery operations (successful)<br><br>**Change Note:** Net new subcategory. See accompanying document for justification. | · **NIST SP 800-184** |
| | | **RC.TC-1:** Ensure that recovery operations are performed in a timely and precise manner.<br>**Change Note:** Net new subcategory. See accompanying document for justification. | · **NIST SP 800-184** |
| | | **RC.IM-1:** Recovery plans incorporate lessons learned | · **COBIT 5** APO12.06, BAI05.07, DSS04.08<br>· **ISA 62443-2-1:2009** 4.4.3.4 |

| | | | |
|---|---|---|---|
| **RECOVER (RC)** | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-1:** Recovery plans incorporate lessons learned | · **ISO/IEC 27001:2013** A.16.1.6, Clause 10<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| | | **RC.IM-2:** Recovery strategies are updated | · **COBIT 5** APO12.06, BAI07.08<br>· **ISO/IEC 27001:2013** A.16.1.6, Clause 10<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). | **RC.CO-1:** Public relations are managed | · **COBIT 5** EDM03.02<br>· **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4 |
| | | **RC.CO-2:** Reputation is repaired after an incident | · **COBIT 5** MEA03.02<br>· **ISO/IEC 27001:2013** Clause 7.4 |
| | | **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams | · **COBIT 5** APO12.06<br>· **ISO/IEC 27001:2013** Clause 7.4<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4 |
| | **Root Cause (RC.RC):** Ameliorate the security weakness(es) that enabled the cyber incident.<br><br>**Change Note:** Net new category. See accompanying document for justification. | **RC.RC-1:** Post-incident verification to confirm root cause(s) | · **NIST SP 800-86** |
| | | **RC.RC-2:** Plan remediation of root cause(s) | |
| | | **RC.RC-3: R**emediation of root cause(s) | |