# Industry Cybersecurity Processes & Profile Mappings

## **D-1 Energy Sector Cybersecurity Efforts and the DOE C2M2 Program**

### **Energy Sector Cybersecurity**

In the last decade NIST has interacted with industry as energy networks become more than mere power delivery systems. As part of the development of the Smart Grid, NIST has worked with industry to develop a series of documents supporting the secure and reliable delivery of Smart Grid services with appropriate security and privacy.[[1]](#footnote-1) It has established a standing Smart Grid Advisory Committee and works with the Smart Grid Interoperability Panel.

During the last several years, research has also focused on the impact of cybersecurity risks on physical systems beyond SCADA, ICS and Smart Grid. Research in this area has been given the term Cyber-Physical Systems, CPS. NIST held a workshop on CPS in August of 2014[[2]](#footnote-2) and again in April 2015.[[3]](#footnote-3) Related to the workshops, a set of work groups were established to support development of use cases, manage security and privacy issues, and to deal with issues specific to timing controls. This Cyber*‑*Physical Systems Public Working Group released a draft CPS Framework to evaluate CPS systems and the risks they face.[[4]](#footnote-4) The Industrial Internet Consortium has also had an active discussion regarding CPS security[[5]](#footnote-5), and has released a reference architecture.

### **DOE Cybersecurity**

The Department of Energy has worked with industry to develop the *Energy Sector Cybersecurity Framework Implementation Guidance[[6]](#footnote-6)* document. Additionally, the DOE has developed the Cybersecurity Capability Maturity Model (C2M2). It describes the C2M2 program as:

“The Cybersecurity Capability Maturity Model (C2M2) program is a public-private partnership effort that was established as a result of the Administration’s efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the grid. The C2M2 helps organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity capabilities.

The model focuses on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology assets and the environments in which they operate.”*[[7]](#footnote-7)*

Further, DOE has adapted the C2M2 program for the oil and natural gas subsector. It describes the additional benefit of the ONG-C2M2:

“The ONG-C2M2 includes the core C2M2 as well as additional reference material and implementation guidance specifically tailored for the oil and natural gas subsector.”*[[8]](#footnote-8)*

This MBLT Profile has used both the Implementation Guidance and the ONG-C2M2. By leveraging this existing body of work, the MBLT Profile utilizes existing industry capability and cross-reference tables to allow organizations who have already leveraged the DOE program to utilize that work here.

This Profile has also utilized its seven-step process for Cybersecurity Framework implementation as described in the Implementation Guidance. The following is a copy of the Implementation Guidance’s Appendix B.

Table D‑1. Summary of Framework Use Steps

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | Step 1: Prioritize and Scope | | | | Inputs | Activities | Outputs | | 1. Risk management strategy  2. Organizational objectives and priorities  3. Threat information | 1. Organization determines where it wants to apply the Framework to evaluate and potentially guide the improvement of the organization’s cybersecurity capabilities | 1. Framework usage scope | | Step 2: Orient | | | | Inputs | Activities | Outputs | | 1. Framework usage scope  2. Risk management strategy | 1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and Informative References (e.g., cybersecurity and risk management standards, tools, methods, and guidelines) | 1. In-scope systems and assets  2. In-scope requirements (i.e., regulatory, company, organizational)  3. In-scope cybersecurity and risk management standards, tools, methods, and guidelines  4. Evaluation approach | | Step 3: Create a Current Profile | | | | Inputs | Activities | Outputs | | 1. Evaluation approach  2. In-scope systems and assets  3. In-scope regulatory requirements  4. In-scope cybersecurity and risk management standards, tools, methods, and guidelines | 1. Organization identifies its current cybersecurity and risk management state | 1. Current Profile  2. Current Implementation Tier | | Step 4: Conduct a Risk Assessment | | | | Inputs | Activities | Outputs | | 1. Framework usage scope  2. Risk management strategy  3. Organization-defined risk assessment approach  4. In-scope regulatory requirements  5. In-scope cybersecurity and risk management standards, tools, methods, and guidelines | 1. Perform risk assessment for in-scope portion of the organization | 1. Risk assessment reports | | Step 5: Create a Target Profile | | | | Inputs | Activities | Outputs | | 1. Current Profile  2. Current Tier  3. Organizational objectives  4. Risk management strategy  5. Risk assessment reports | 1. Organization identifies goals that will mitigate risk commensurate with the risk to organizational and critical infrastructure objectives | 1. Target Profile  2. Target Tier | | Step 6: Determine, Analyze, and Prioritize Gaps | | | | Inputs | Activities | Outputs | | 1. Current Profile  2. Current Tier  3. Target Profile  4. Target Tier  5. Organizational objectives  6. Impact to critical infrastructure  7. Gaps and potential consequences  8. Organizational constraints  9. Risk management strategy  10. Risk assessment reports | 1. Analyze gaps between current state and Target Profile in organization’s context  2. Evaluate potential consequences from gaps  3. Determine which gaps need attention  4. Identify actions to address gaps  5. Perform cost-benefit analysis (CBA) on actions  6. Prioritize actions (CBA and consequences)  7. Plan to implement prioritized actions | 1. Prioritized gaps and potential consequences  2. Prioritized implementation plan | | Step 7: Implement Action Plan | | | | Inputs | Activities | Outputs | | 1. Prioritized implementation plan | 1. Implement actions by priority  2. Track progress against plan  3. Monitor and evaluate progress against key risks, metrics, and performance indicators  4. Report progress | 1. Project tracking data  2. New security measures implemented | |

## **D-2 Cybersecurity Framework Informative References**

Other critical infrastructure organizations have also developed Cybersecurity Framework Profiles. Examples include the electric power industry, the public water industry, the aviation industry, and the transportation industry. Some of the Profile work predates the development of the Cybersecurity Framework. Others have incorporated the Cybersecurity Framework into their Profile work. We review some of this work in our related *How To Guide*.

## **D-3 Mapping of Optional Resources**

The Cybersecurity Framework appendix describing the Framework Core includes informative references from other security standards. They are replicated here.

| **Subcategory** | **Informative References from Cybersecurity Framework** |
| --- | --- |
| **ID.AM-1**: Physical devices and systems within the organization are inventoried | · **CCS CSC** 1 |
| · **COBIT 5** BAI09.01, BAI09.02 |
| · **ISA 62443-2-1:2009** 4.2.3.4 |
| · **ISA 62443-3-3:2013** SR 7.8 |
| · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 |
| · **NIST SP 800-53** **Rev. 4** CM-8 |
| **ID.AM-2:** Software platforms and applications within the organization are inventoried | · **CCS CSC** 2 |
| · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 |
| · **ISA 62443-2-1:2009** 4.2.3.4 |
| · **ISA 62443-3-3:2013** SR 7.8 |
| · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 |
| · **NIST SP 800-53** **Rev. 4** CM-8 |
| **ID.AM-3:** Organizational communication and data flows are mapped | · **CCS CSC** 1 |
| · **COBIT 5** DSS05.02 |
| · **ISA 62443-2-1:2009** 4.2.3.4 |
| · **ISO/IEC 27001:2013** A.13.2.1 |
| · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 |
| **ID.AM-4:** External information systems are catalogued | · **COBIT 5** APO02.02 |
| · **ISO/IEC 27001:2013** A.11.2.6 |
| · **NIST SP 800-53** **Rev. 4** AC-20, SA-9 |
| **ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | · **COBIT 5** APO03.03, APO03.04, BAI09.02 |
| · **ISA 62443-2-1:2009** 4.2.3.6 |
| · **ISO/IEC 27001:2013** A.8.2.1 |
| · **NIST SP 800-53** **Rev. 4** CP-2, RA-2, SA-14 |
| **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | · **COBIT 5** APO01.02, DSS06.03 |
| · **ISA 62443-2-1:2009** 4.3.2.3.3 |
| · **ISO/IEC 27001:2013** A.6.1.1 |
| · **NIST SP 800-53** **Rev. 4** CP-2, PS-7, PM-11 |
| **ID.BE-1:** The organization’s role in the supply chain is identified and communicated | · **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 |
| · **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 |
| · **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 |
| · **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 |
| · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 |
| · **NIST SP 800-53** **Rev. 4** PM-11, SA-14 |
| **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established | · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 |
| · **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 | · **COBIT 5** DSS04.02 |
| · **ISO/IEC 27001:2013** A.11.1.4,A.17.1.1,A.17.1.2, A.17.2.1 |
| · **NIST SP 800-53** **Rev. 4** CP-2, CP-11, SA-14 |
| **ID.GV-1:** Organizational information security policy is established | · **COBIT 5** APO01.03, EDM01.01, EDM01.02 |
| · **ISA 62443-2-1:2009** 4.3.2.6 |
| · **ISO/IEC 27001:2013** A.5.1.1 |
| · **NIST SP 800-53** **Rev. 4** -1 controls from all families |
| **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | · **COBIT 5** APO13.12 |
| · **ISA 62443-2-1:2009** 4.3.2.3.3 |
| · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 |
| · **NIST SP 800-53** **Rev. 4** PM-1, PS-7 |
| **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | · **COBIT 5** MEA03.01, MEA03.04 |
| · **ISA 62443-2-1:2009** 4.4.3.7 |
| · **ISO/IEC 27001:2013** A.18.1 |
| · **NIST SP 800-53** **Rev. 4** -1 controls from all families (except PM-1) |
| **ID.GV-4**: Governance and risk management processes address cybersecurity risks | · **COBIT 5** DSS04.02 |
| · **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 |
| · **NIST SP 800-53 Rev. 4** PM-9, PM-11 |
| **ID.RA-1:** Asset vulnerabilities are identified and documented | · **CCS CSC** 4 |
| · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 |
| · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 |
| · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 |
| · **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:** Threat and vulnerability information is received from information sharing forums and sources | · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 |
| · **ISO/IEC 27001:2013** A.6.1.4 |
| · **NIST SP 800-53** **Rev. 4** PM-15, PM-16, SI-5 |
| **ID.RA-3:** Threats, both internal and external, are identified and documented | · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 |
| · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 |
| · **NIST SP 800-53** **Rev. 4** RA-3, SI-5, PM-12, PM-16 |
| **ID.RA-4:** Potential business impacts and likelihoods are identified | · **COBIT 5** DSS04.02 |
| · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 |
| · **NIST SP 800-53** **Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14 |
| **ID.RA-5**: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | · **COBIT 5** APO12.02 |
| · **ISO/IEC 27001:2013** A.12.6.1 |
| · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16 |
| **ID.RA-6:** Risk responses are identified and prioritized | · **COBIT 5** APO12.05, APO13.02 |
| · **NIST SP 800-53 Rev. 4** PM-4, PM-9 |
| **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 |
| · **ISA 62443-2-1:2009** 4.3.4.2 |
| · **NIST SP 800-53** **Rev. 4** PM-9 |
| **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | · **COBIT 5** APO12.06 |
| · **ISA 62443-2-1:2009** 4.3.2.6.5 |
| · **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 | · **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14 |
| **PR.AC-1:** Identities and credentials are managed for authorized devices and users | · **CCS** **CSC** 16 |
| · **COBIT 5** DSS05.04, DSS06.03 |
| · **ISA 62443-2-1:2009** 4.3.3.5.1 |
| · **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 |
| · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 |
| · **NIST SP 800-53** **Rev. 4** AC-2, IA Family |
| **PR.AC-2:** Physical access to assets is managed and protected | · **COBIT 5** DSS01.04, DSS05.05 |
| · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 |
| · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 |
| · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 |
| **PR.AC-3:** Remote access is managed | · **COBIT 5** APO13.01, DSS01.04, DSS05.03 |
| · **ISA 62443-2-1:2009** 4.3.3.6.6 |
| · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 |
| · **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 |
| · **NIST SP 800-53 Rev. 4** AC‑17, AC-19, AC-20 |
| **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties | · **CCS** **CSC** 12, 15 |
| · **ISA 62443-2-1:2009** 4.3.3.7.3 |
| · **ISA 62443-3-3:2013** SR 2.1 |
| · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 |
| · **NIST SP 800-53** **Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16 |
| **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate | · **ISA 62443-2-1:2009** 4.3.3.4 |
| · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 |
| · **ISO/IEC 27001:2013** A.13.1.1,A.13.1.3, A.13.2.1 |
| · **NIST SP 800-53 Rev. 4** AC-4, SC-7 |
| **PR.AT-1:** All users are informed and trained | · **CCS CSC** 9 |
| · **COBIT 5** APO07.03, BAI05.07 |
| · **ISA 62443-2-1:2009** 4.3.2.4.2 |
| · **ISO/IEC 27001:2013** A.7.2.2 |
| · **NIST SP 800-53** **Rev. 4** AT-2, PM-13 |
| **PR.AT-2:** Privileged users understand roles & responsibilities | · **CCS CSC** 9 |
| · **COBIT 5** APO07.02, DSS06.03 |
| · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 |
| · **ISO/IEC 27001:2013** A.6.1.1,A.7.2.2 |
| · **NIST SP 800-53** **Rev. 4** AT-3, PM-13 |
| **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | · **CCS** **CSC** 9 |
| · **COBIT 5** APO07.03, APO10.04, APO10.05 |
| · **ISA 62443-2-1:2009** 4.3.2.4.2 |
| · **ISO/IEC 27001:2013** A.6.1.1,A.7.2.2 |
| · **NIST SP 800-53** **Rev. 4** PS-7, SA-9 |
| **PR.AT-4:** Senior executives understand roles & responsibilities | · **CCS** **CSC** 9 |
| · **COBIT 5** APO07.03 |
| · **ISA 62443-2-1:2009** 4.3.2.4.2 |
| · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, |
| · **NIST SP 800-53** **Rev. 4** AT-3, PM-13 |
| **PR.AT-5:** Physical and information security personnel understand roles & responsibilities | · **CCS** **CSC** 9 |
| · **COBIT 5** APO07.03 |
| · **ISA 62443-2-1:2009** 4.3.2.4.2 |
| · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, |
| · **NIST SP 800-53** **Rev. 4** AT-3, PM-13 |
| **PR.DS-1:** Data-at-rest is protected | · **CCS** **CSC** 17 |
| · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 |
| · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 |
| · **ISO/IEC 27001:2013** A.8.2.3 |
| · **NIST SP 800-53 Rev. 4** SC-28 |
| **PR.DS-2:** Data-in-transit is protected | · **CCS** **CSC** 17 |
| · **COBIT 5** APO01.06, DSS06.06 |
| · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 |
| · **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 |
| · **NIST SP 800-53** **Rev. 4** SC-8 |
| **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition | · **COBIT 5** BAI09.03 |
| · **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 |
| · **ISA 62443-3-3:2013** SR 4.2 |
| · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 |
| · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16 |
| **PR.DS-4:** Adequate capacity to ensure availability is maintained | · **COBIT 5** APO13.01 |
| · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 |
| · **ISO/IEC 27001:2013** A.12.3.1 |
| · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5 |
| **PR.DS-5:** Protections against data leaks are implemented | · **CCS CSC** 17 |
| · **COBIT 5** APO01.06 |
| · **ISA 62443-3-3:2013** SR 5.2 |
| · **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.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 |
| · **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, SI-4 |
| **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity | · **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 |
| · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 |
| · **NIST SP 800-53** **Rev. 4** SI-7 |
| **PR.DS-7:** The development and testing environment(s) are separate from the production environment | · **COBIT 5** BAI07.04 |
| · **ISO/IEC 27001:2013** A.12.1.4 |
| · **NIST SP 800-53 Rev. 4** CM-2 |
| **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained | · **CCS** **CSC** 3, 10 |
| · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 |
| · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 |
| · **ISA 62443-3-3:2013** SR 7.6 |
| · **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 | · **COBIT 5** APO13.01 |
| · **ISA 62443-2-1:2009** 4.3.4.3.3 |
| · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 |
| · **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8 |
| **PR.IP-3:** Configuration change control processes are in place | · **COBIT 5** BAI06.01, BAI01.06 |
| · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 |
| · **ISA 62443-3-3:2013** SR 7.6 |
| · **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-3, CM-4, SA-10 |
| **PR.IP-4:** Backups of information are conducted, maintained, and tested periodically | · **COBIT 5** APO13.01 |
| · **ISA 62443-2-1:2009** 4.3.4.3.9 |
| · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 |
| · **ISO/IEC 27001:2013** A.12.3.1,A.17.1.2A.17.1.3, A.18.1.3 |
| · **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 |
| · **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 |
| · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 |
| · **NIST SP 800-53** **Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 |
| **PR.IP-6:** Data is destroyed according to policy | · **COBIT 5** BAI09.03 |
| · **ISA 62443-2-1:2009** 4.3.4.4.4 |
| · **ISA 62443-3-3:2013** SR 4.2 |
| · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 |
| · **NIST SP 800-53 Rev. 4** MP-6 |
| **PR.IP-7:** Protection processes are continuously improved | · **COBIT 5** APO11.06, DSS04.05 |
| · **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 |
| · **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 with appropriate parties | · **ISO/IEC 27001:2013** A.16.1.6 |
| · **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 | · **COBIT 5** DSS04.03 |
| · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 |
| · **ISO/IEC 27001:2013** A.16.1.1,A.17.1.1, A.17.1.2 |
| · **NIST SP 800-53** **Rev. 4** CP-2, IR-8 |
| **PR.IP-10:** Response and recovery plans are tested | · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 |
| · **ISA 62443-3-3:2013** SR 3.3 |
| · **ISO/IEC 27001:2013** A.17.1.3 |
| · **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) | · **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 |
| · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 |
| · **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 |
| · **NIST SP 800-53 Rev. 4** PS Family |
| **PR.IP-12:** Avulnerability management plan is developed and implemented | · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 |
| · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2 |
| **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | · **COBIT 5** BAI09.03 |
| · **ISA 62443-2-1:2009** 4.3.3.3.7 |
| · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 |
| · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5 |
| **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | · **COBIT 5** DSS05.04 |
| · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 |
| · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 |
| · **NIST SP 800-53 Rev. 4** MA-4 |
| **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | · **CCS CSC** 14 |
| · **COBIT 5** APO11.04 |
| · **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 |
| · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 |
| · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 |
| · **NIST SP 800-53** **Rev. 4** AU Family |
| **PR.PT-2:** Removable media is protected and its use restricted according to policy | · **COBIT 5** DSS05.02, APO13.01 |
| · **ISA 62443-3-3:2013** SR 2.3 |
| · **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 |
| · **NIST SP 800-53** **Rev. 4** MP-2, MP-4, MP-5, MP-7 |
| **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality | · **COBIT 5** DSS05.02 |
| · **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, 4.3.3.5.8, 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, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 |
| · **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, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 |
| · **ISO/IEC 27001:2013** A.9.1.2 |
| · **NIST SP 800-53 Rev. 4** AC-3, CM-7 |
| **PR.PT-4:** Communications and control networks are protected | · **CCS CSC** 7 |
| · **COBIT 5** DSS05.02, APO13.01 |
| · **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, SR 7.6 |
| · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 |
| · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7 |
| **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed | · **COBIT 5** DSS03.01 |
| · **ISA 62443-2-1:2009** 4.4.3.3 |
| · **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 | · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 |
| · **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 |
| · **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 |
| · **NIST SP 800-53** **Rev. 4** AU-6, CA-7, IR-4, SI-4 |
| **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | · **ISA 62443-3-3:2013** SR 6.1 |
| · **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 | · **COBIT 5** APO12.06 |
| · **NIST SP 800-53** **Rev. 4** CP-2, IR-4, RA-3, SI -4 |
| **DE.AE-5:** Incident alert thresholds are established | · **COBIT 5** APO12.06 |
| · **ISA 62443-2-1:2009** 4.2.3.10 |
| · **NIST SP 800-53** **Rev. 4** IR-4, IR-5, IR-8 |
| **DE.CM-1:** The network ismonitored to detect potential cybersecurity events | · **CCS CSC** 14, 16 |
| · **COBIT 5** DSS05.07 |
| · **ISA 62443-3-3:2013** SR 6.2 |
| · **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 | · **ISA 62443-2-1:2009** 4.3.3.3.8 |
| · **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 | · **ISA 62443-3-3:2013** SR 6.2 |
| · **ISO/IEC 27001:2013** A.12.4.1 |
| · **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 | · **CCS CSC** 5 |
| · **COBIT 5** DSS05.01 |
| · **ISA 62443-2-1:2009** 4.3.4.3.8 |
| · **ISA 62443-3-3:2013** SR 3.2 |
| · **ISO/IEC 27001:2013** A.12.2.1 |
| · **NIST SP 800-53 Rev. 4** SI-3 |
| **DE.CM-5:** Unauthorized mobile code is detected | · **ISA 62443-3-3:2013** SR 2.4 |
| · **ISO/IEC 27001:2013** A.12.5.1 |
| · **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 |
| · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 |
| · **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 | · **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 | · **COBIT 5** BAI03.10 |
| · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 |
| · **ISO/IEC 27001:2013** A.12.6.1 |
| · **NIST SP 800-53** **Rev. 4** RA-5 |
| **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability | · **CCS CSC** 5 |
| · **COBIT 5** DSS05.01 |
| · **ISA 62443-2-1:2009** 4.4.3.1 |
| · **ISO/IEC 27001:2013** A.6.1.1 |
| · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14 |
| **DE.DP-2:** Detection activities comply with all applicable requirements | · **ISA 62443-2-1:2009** 4.4.3.2 |
| · **ISO/IEC 27001:2013** A.18.1.4 |
| · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4 |
| **DE.DP-3:** Detection processes are tested | · **COBIT 5** APO13.02 |
| · **ISA 62443-2-1:2009** 4.4.3.2 |
| · **ISA 62443-3-3:2013** SR 3.3 |
| · **ISO/IEC 27001:2013** A.14.2.8 |
| · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 |
| **DE.DP-4:** Event detection information is communicated to appropriate parties | · **COBIT 5** APO12.06 |
| · **ISA 62443-2-1:2009** 4.3.4.5.9 |
| · **ISA 62443-3-3:2013** SR 6.1 |
| · **ISO/IEC 27001:2013** A.16.1.2 |
| · **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, DSS04.05 |
| · **ISA 62443-2-1:2009** 4.4.3.4 |
| · **ISO/IEC 27001:2013** A.16.1.6 |
| · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 |
| **RS.RP-1:** Response plan is executed during or after an event | · **COBIT 5** BAI01.10 |
| · **CCS** **CSC** 18 |
| · **ISA 62443-2-1:2009** 4.3.4.5.1 |
| · **ISO/IEC 27001:2013** A.16.1.5 |
| · **NIST SP 800-53** **Rev. 4** CP-2, CP-10, IR-4, IR-8 |
| **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 |
| · **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 |
| · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 |
| **RS.CO-2:** Events are reported consistent with established criteria | · **ISA 62443-2-1:2009** 4.3.4.5.5 |
| · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 |
| · **NIST SP 800-53 Rev. 4** AU-6,IR-6, IR-8 |
| **RS.CO-3:** Information is shared consistent with response plans | · **ISA 62443-2-1:2009** 4.3.4.5.2 |
| · **ISO/IEC 27001:2013** A.16.1.2 |
| · **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 | · **ISA 62443-2-1:2009** 4.3.4.5.5 |
| · **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 | · **NIST SP 800-53 Rev. 4** PM-15, SI-5 |
| **RS.AN-1:** Notifications from detection systems are investigated | · **COBIT 5** DSS02.07 |
| · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 |
| · **ISA 62443-3-3:2013** SR 6.1 |
| · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 |
| · **NIST SP 800-53** **Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 |
| **RS.AN-2:** The impact of the incident is understood | · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 |
| · **ISO/IEC 27001:2013** A.16.1.6 |
| · **NIST SP 800-53** **Rev. 4** CP-2, IR-4 |
| **RS.AN-3:** Forensics are performed | · **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 |
| · **ISO/IEC 27001:2013** A.16.1.7 |
| · **NIST SP 800-53** **Rev. 4** AU-7, IR-4 |
| **RS.AN-4:** Incidents are categorized consistent with response plans | · **ISA 62443-2-1:2009** 4.3.4.5.6 |
| · **ISO/IEC 27001:2013** A.16.1.4 |
| · **NIST SP 800-53** **Rev. 4** CP-2, IR-4, IR-5, IR-8 |
| **RS.MI-1:** Incidents are contained | · **ISA 62443-2-1:2009** 4.3.4.5.6 |
| · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 |
| · **ISO/IEC 27001:2013** A.16.1.5 |
| · **NIST SP 800-53** **Rev. 4** IR-4 |
| **RS.MI-2:** Incidents are mitigated | · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 |
| · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 |
| · **NIST SP 800-53** **Rev. 4** IR-4 |
| **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks | · **ISO/IEC 27001:2013** A.12.6.1 |
| · **NIST SP 800-53** **Rev. 4** CA-7,RA-3, RA-5 |
| **RS.IM-1:** Responseplans incorporate lessons learned | · **COBIT 5** BAI01.13 |
| · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 |
| · **ISO/IEC 27001:2013** A.16.1.6 |
| · **NIST SP 800-53** **Rev. 4** CP-2, IR-4, IR-8 |
| **RS.IM-2:** Response strategies are updated | · **NIST SP 800-53** **Rev. 4** CP-2, IR-4, IR-8 |
| **RC.RP-1:** Recovery plan is executed during or after an event | · **CCS** **CSC** 8 |
| · **COBIT 5** DSS02.05, DSS03.04 |
| · **ISO/IEC 27001:2013** A.16.1.5 |
| · **NIST SP 800-53** **Rev. 4** CP-10, IR-4, IR-8 |
| **RC.IM-1:** Recovery plans incorporate lessons learned | · **COBIT 5** BAI05.07 |
| · **ISA 62443-2-1** 4.4.3.4 |
| · **NIST SP 800-53** **Rev. 4** CP-2, IR-4, IR-8 |
| **RC.IM-2:** Recovery strategies are updated | · **COBIT 5** BAI07.08 |
| · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| **RC.CO-1:** Public relations are managed | · **COBIT 5** EDM03.02 |
| **RC.CO-2:** Reputation after an event is repaired | · **COBIT 5** MEA03.02 |
| **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | · **NIST SP 800-53 Rev. 4** CP-2, IR-4 |

1. NIST, Smart Grid landing page <http://www.nist.gov/smartgrid/> [↑](#footnote-ref-1)
2. NIST, Cyber-Physical Systems Public Working Group Workshop, <http://www.nist.gov/cps/cps-pwg-workshop.cfm> [↑](#footnote-ref-2)
3. NIST, Cyber-Physical Systems Public Working Group (CPS-PWG) Workshop – April 2015, <http://nist.gov/cps/cps-pwg-workshop-april-2015.cfm> [↑](#footnote-ref-3)
4. Cyber‑Physical Systems Public Working Group, draft *Cyber-Physical Systems Framework*, September 2015, <https://pages.nist.gov/cpspwg> [↑](#footnote-ref-4)
5. Industrial Internet Consortium Security Working Group, <http://www.iiconsortium.org/wc-security.htm> [↑](#footnote-ref-5)
6. <http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf> [↑](#footnote-ref-6)
7. <http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program> [↑](#footnote-ref-7)
8. <http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/oil-and-natural-gas-subsector-cybersecurity> [↑](#footnote-ref-8)