EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Risk Management in Practice

A Guide for the Electric Sector

3002003333

Risk Management in Practice

A Guide for the Electric Sector

3002003333

Technical Update, December 2014

EPRI Project Manager

A. Lee

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT.

THIS REPORT WAS PREPARED AS AN ACCOUNT OF WORK SPONSORED BY AN AGENCY OF THE UNITED STATES GOVERNMENT. NEITHER THE UNITED STATES GOVERNMENT NOR ANY AGENCY THEREOF, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OR IMPLIED, OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS. REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF. THE VIEWS AND OPINIONS OF AUTHORS EXPRESSED HEREIN DO NOT NECESSARILY STATE OR REFLECT THOSE OF THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF.

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigator
A. Lee

This report describes research sponsored by EPRI.

The following organizations and individuals participated in the development of this report:

Maurice Martin, Craig Miller, George Walker: National Rural Electric Cooperative Association (NRECA)

Jason Christopher: Department of Energy

John Fry, Fowad Muneer, Sean Storer: ICF International

James Stevens: Software Engineering Institute, Carnegie Mellon University

In addition, several individuals provided feedback and recommendations on the development of the document. The dedication and commitment of all the participants was significant and the technical content could not have been developed without their contributions.

Some of the material included in this technical update is based on several documents, for example, the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, September 2014; the U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Risk Management Process*, May 2012; the U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1*, February 2014, and the *NIST Framework for Improving Critical Infrastructure Security*, February 2014. The authors acknowledge the dedication and technical expertise of all the individuals who participated in the development of these documents.

This publication is a corporate document that should be cited in the literature in the following manner:

Risk Management in Practice: A Guide for the Electric Sector. EPRI, Palo Alto, CA: 2014. 3002003333.

ABSTRACT

A cyber security risk management process provides the basis for determining the type, nature, and severity of cyber security risks facing a utility and provides the basis for all subsequent cyber security risk management decision making. Risk management includes identifying the threat agents, the vulnerabilities, as well as the impacts of cyber security events. The organization includes this information in making risk mitigation decisions based on the cyber security risk tolerance of the organization. Risk management considers both malicious and non-malicious events because the impact on the system may be the same.

This Technical Update provides guidance for risk management in practice in the electric sector. This present work builds upon the technical update, *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology*, 3002001181 that was published in 2013; the DOE *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2); the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, the National Rural Electric Cooperative Association (NRECA) Guidance, and other documents.

The focus of this document is to provide guidance on applying the diverse existing cyber security guidance that is applicable to the electric sector. The goal of this document is to provide a framework and comparative analyses of existing guidance that may be used by cyber security practitioners in addressing cyber security.

This document was developed jointly by several organizations, including EPRI, DOE, NRECA, Carnegie Mellon University, and several utilities. This document is a companion document to the EPRI technical update, *Security Posture Using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),* Technical Update 3002003332, also published in 2014.

Keywords
Cyber Security
Cyber Security Risk Assessment
Cyber Security Risk Management
Failure Scenarios

EXECUTIVE SUMMARY

Currently, the nation's power system consists of both legacy and next generation technologies. This increased digital functionality provides a larger attack surface for any potential adversary, such as nation-states, terrorists, malicious contractors, and disgruntled employees.

The federal government has responded to all of these changes in technology and the threat environment by developing and updating cyber security guidance. Currently, utilities are assessing all this guidance for applicability and what must be implemented. In addition, utilities are trying to analyze all this guidance because it is at different levels of specificity and focus. The goal of this document is to provide guidance on applying this diverse existing cyber security guidance that is applicable to the electric sector. The goal of this document is to provide a framework and comparative analyses of existing guidance that may be used by cyber security practitioners in addressing cyber security.

This document was developed jointly by several organizations, including EPRI, DOE, NRECA, Carnegie Mellon University, and several utilities. This document is a companion document to the EPRI technical update, *Security Posture Using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),* Technical Update 3002003332, also published in 2014.

ACRONYMS

BES	Bulk Electric System
CIP	Critical Infrastructure Protection
COP	Common Operating Picture
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
DOE	Department of Energy
EO	Executive Order
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
GRC	Governance, Risk, and Compliance
ICS	Industrial Control Systems
IT	Information Technology
MIL	Maturity Indicator Level
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NRECA	National Rural Electric Cooperative Association
OT	Operations Technology
PUC	Public Utility Commission
RMP	Risk Management Process

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
BACKGROUND

Currently, the nation's power system consists of both legacy and next generation technologies. New grid technologies are introducing millions of novel, intelligent components to the electric grid that communicate in much more advanced ways (two-way communications, dynamic optimization, and wired and wireless communications) than in the past. These new components will operate in conjunction with legacy equipment that may be several decades old, and provide little to no cyber security controls. In addition, with alternative energy sources such as solar power and wind, there is increased interconnection across organizations and systems. With the increase in the use of digital devices and more advanced communications, the overall cyber risk has increased. For example, as substations are modernized, the new equipment is digital, rather than analog. These new devices include commercially available operating systems, protocols, and applications rather than proprietary solutions. This increased digital functionality provides a larger attack surface for any potential adversary, such as nation-states, terrorists, malicious contractors, and disgruntled employees.

This new technology increases the complexity of addressing cyber risks. Many of the commercially available solutions have known vulnerabilities that could be exploited when the solutions are installed in control system components. Potential impacts from a cyber-event include: billing errors, brownouts/blackouts, personal injury or loss of life, operational strain during a disaster recovery situation, or physical damage to power equipment.

Another change is the convergence of Information Technology (IT) and Operations Technology (OT). Historically IT has included computer systems, applications, communications technology and software to store, retrieve, transmit and process data typically for a business or enterprise. OT has historically focused on physical-equipment-oriented technology that is commonly used to operate the energy sector. Currently, multiple groups and operators often independently gather and analyze information from isolated and "stove-piped" systems that have been developed to provide security monitoring for physical, enterprise, and control system environments. As the threat landscape has evolved, there is a greater need to have a coordinated view of all aspects of an organization's security posture (situational awareness), events (both unintentional, such as a component failure; and malicious) that may impact an organization's security posture, and responses to those events.

The federal government has responded to all of these changes in technology and the threat environment by developing and updating cyber security guidance. The various documents are described below.

1.1 Federal Government Cyber Security Risk Guidance

To address cyber security risks, the President issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, on February 12, 2013, which states:

> *It is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency,*

innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

The EO requires the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The Framework focuses on using business drivers to guide cyber security activities and considering cyber security risks as part of the organization's risk management processes. In response, the National Institute of Standards and Technology (NIST) released a *Framework for Improving Critical Infrastructure Cybersecurity*[1] [hereafter referred to as the NIST Cybersecurity Framework or the NIST CSF] that provides a structure for creating, guiding, assessing, and improving cyber security programs.

Both of these documents are at a high level and address all sixteen critical infrastructures, including the energy sector and the electricity subsector. The U.S. Department of Energy (DOE) developed the *Energy Sector Cybersecurity Framework Implementation Guidance* specifically for energy sector owners and operators. It is tailored to the energy sector and provides guidance on implementing the NIST CSF.

1.2 Department of Energy Risk Management Process

(The following material is extracted from the DOE/EPRI report: *Cyber Security Risk Assessment and Continuous Monitoring Methodology*, 2013. The material is included in this document for completeness.)

> The Department of Energy (DOE) developed the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) document to address cyber security risk. The RMP provides a scalable risk management process that is specific to the risks inherent in operating information technology (IT) and industrial control systems (ICS). The term *risk management* refers to the program and supporting processes used to manage cyber security risk to an organization's operations, its assets, and individuals.
>
> The risk management cycle includes four phases. These phases require utilities to (1) *frame* risk (i.e., establish the context for risk-based decisions), (2) *assess* risk, (3) *respond* to risk once determined, and (4) *monitor* risk on an ongoing basis, using an iterative feedback loop for continuous improvement in the risk-related activities of organizations. The risk management cycle and the four phases are illustrated in Figure 1-1 and further defined below. Although the discussion below focuses on cyber security risk, the four phases are applicable to all types of enterprise risk.

[1] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

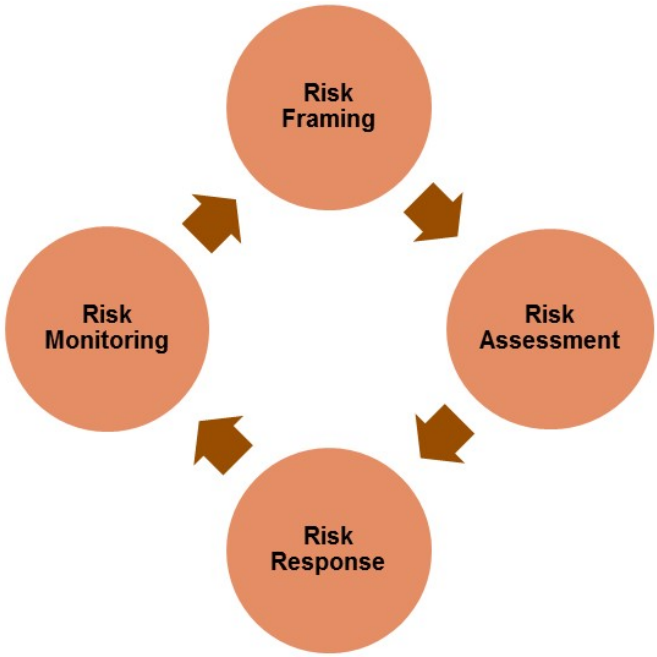

Figure 1-1
Risk Management Cycle

1.2.1 Risk Framing

The risk-framing phase includes the description of the environment in which risk-based decisions are made. The environment for control systems is often distinct from that for IT systems. For example, many control system components are located in physically unprotected areas (e.g., pole tops, sides of buildings) and are expected to operate 24/7 without interruption. Establishing a realistic risk frame requires utilities to specify the following for the control systems:

- Assumptions about threats, vulnerabilities, impacts, and likelihood of occurrence;
- Constraints imposed by legislation, regulation, and resources (time, money, and people);
- Risk tolerance/level of acceptable risk;
- System priorities and criticality within mission/functional areas, and trade-offs between different types of risk; and
- Trust relationships with third parties and vendors and physical interconnections with external organizations.

1.2.2 Risk Assessment

Risk assessment involves the integration of threat, vulnerability, and consequence/impact information. In the risk assessment phase, the utility identifies, prioritizes, and estimates risk to operations, assets, and individuals. Risk determination is used in prioritizing and allocating resources to reduce those risks. The first step in the process is to identify the assets – the control systems or groups of control systems. Once this task has been completed, the utility:

- Identifies, characterizes, and assess threats;
- Assesses critical assets (control system) vulnerabilities;
- Determines the impact (the expected consequences of cyber security events); and

- Specifies the likelihood of the cyber security event (including the skills and capabilities of the attacker and the availability of attack tools and malware).

1.2.3 Risk Response

The risk response phase addresses how a utility responds to risk associated with control systems once that risk is assessed. In this phase, a utility:

- Develops alternative courses of action for responding to risk (accept, avoid, mitigate, share, or transfer risk);
- Evaluates the alternative courses of action;
- Prioritizes the risk mitigation measures based on the overall risk management strategy,
- Determines appropriate courses of action consistent with the utility's risk tolerance level; and
- Implements the courses of action.

A utility may determine that certain response actions are not feasible to implement, are cost prohibitive, or are not relevant to the utility's control system operations. If the mitigation controls are cost prohibitive, require excessive utility resources to implement, or are not feasible to implement, a utility may implement compensating controls[2] to manage the risk in an acceptable way and meet the cyber security requirements. The risk response element is the point where utilities make choices on how best to address risk.

1.2.4 Risk Monitoring

The risk-monitoring phase addresses how risks are monitored over time in a utility. During the risk monitoring phase, utilities:
Evaluate the ongoing effectiveness of risk response measures;

- Identify changes that may impact risk to a utility's control systems and the operational environments; and
- Identify changes (technology, vulnerabilities, threat agents) that may impact the effectiveness of risk responses.

1.3 Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2[3]) provides guidance on measures to identify, assess, and manage cyber risk and enable utilities to evaluate their cyber security capabilities and make improvements in their cyber security programs. The ES-C2M2 provides descriptive rather than prescriptive industry focused guidance. The model content is presented at a high level of abstraction so that it can be interpreted and applied by subsector organizations of various types, structures, and sizes including, for example, large independently owned utilities (IOUs), rural cooperatives, and public power utilities. The ES-C2M2 may be used by the electric sector to implement the NIST CSF.

---

[2]A compensating control is a cyber security control implemented as an alternative to a recommended control that provides equivalent or comparable control.

[3] http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

The approach for using the ES-C2M2 is illustrated in Figure 1-2 below and is extracted from the ES-C2M2 document. As stated in the ES-C2M2, "An organization performs an evaluation against the model, uses that evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated." The ES-C2M2 should be executed in each phase of the risk management cycle illustrated in Figure 1-1 above. The focus may be different in each phase, for example, in the risk framing phase the ES-C2M2 focus should be on defining and documenting the utility's cyber security strategy. In the risk assessment phase, the ES-C2M2 focus should be on assessing the implemented cyber security strategy.

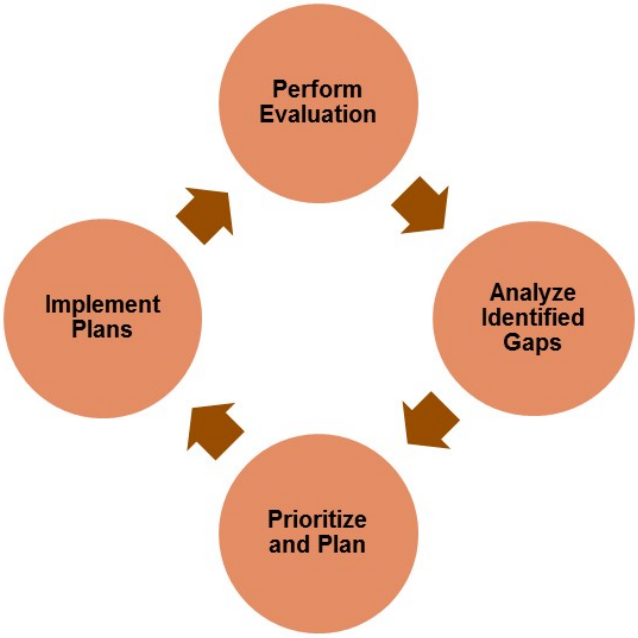

Figure 1-2
Recommended Approach for Using the ES-C2M2

1.4 North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards

Another risk management approach is compliance based using the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. These mandatory reliability standards are applicable to the bulk electric system (BES), only. As stated in each standard, "The standards include requirements in support of protecting BES cyber systems from compromise that could lead to misoperation or instability in the BES."

1.5 Control-Based Security Assessment Documents

For the control-based approach, the National Electric Sector Cybersecurity Organization Resource (NESCOR) risk assessment methodology may be used. An overview of risk assessment and the NESCOR methodology are documented in the jointly published DOE and EPRI document: Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology.

There are several different security control standards/requirements documents that may be used in the control-based approach. Some of these documents are: the NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, the NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, NRECA Guidance, the Nuclear Regulatory Commission (NRC) Regulatory Guideline (RG) 5.71, Cyber Security Programs for Nuclear Facilities, and the Nuclear Energy Institute (NEI) document 08-09 Revision 6, Cyber Security Plan for Nuclear Power Reactors.

1.6 Other Guidance Documents

Finally, guidance documents have been developed by several organizations such as the National Association of Regulatory Utility Commissioners (NARUC) and the Department of Homeland Security (DHS) to assist in addressing cyber security risk.

1.7 Content of This Technical Update

All of the documents described above are at different levels of specificity and may be used for different purposes related to managing cyber security risk. For example, the ES-C2M2 may be used to determine the maturity level of an organization and the NISTIR 7628 security requirements may be used as part of a cyber security risk assessment of specific control systems.

Some utilities have the technical expertise to assess and use the various documents as part of an overall cyber security risk management program. However, not all utilities have in-house expertise and must rely on external organizations and guidance. Also, some utilities are being asked by management and by regulatory organizations, such as state public utility commissions (PUCs), to demonstrate how they meet the requirements and/or content of these various documents.

This technical update has two objectives to assist utilities in using and assessing the various cyber security documents. The first objective is to provide an overview diagram of the cyber security documents that are referenced above and their use in the different areas of an enterprise risk management process. This document may be used by utilities that do not have cyber security technical expertise as a roadmap on moving forward. The second objective is to provide a comparative analysis of the referenced documents. Currently, there are many versions of the comparative analysis – developed by utilities and contractors. The goal is to have a common baseline set that may be used by everyone. This first version is not intended to be final – and the goal is to have people use the comparative analysis tables included in this technical update and the companion documents and provide comments for future versions.

Chapter 2 includes the overview diagram with a description of the diagram components and how to use the various documents, chapter 3 contains one of the comparative analysis tables with explanations, chapter 4 includes a gap analysis, and chapter 5 includes a summary and next steps.

2
CYBER SECURITY RISK MANAGEMENT

Cyber security is a priority for critical infrastructures, especially electric utilities. However, cyber security threats and concerns are constantly evolving and present complex, multifaceted challenges. Staying current with best practices requires constant attention to the changing technical landscape and a commitment to continuous improvement. There have been many efforts to support utilities in this endeavor and while they are each individually valuable, the number and diversity of guidance can create confusion since many address the same subject from different perspectives and use different nomenclature.

This document is NOT an attempt to develop new guidance but rather assist in navigating the diverse existing guidance that is applicable to the electric sector. Therefore, the goal of this document is to provide a framework and comparative analyses of existing guidance that will assist cyber security practitioners in the electric sector to define the appropriate roles for each document and make use of them in a coordinated approach to addressing cyber security.

Ideally, users of this material will be working toward an Enterprise Risk Management Process and Strategy that can be divided into multiple parts, and three are included here:

- Financial Risk Strategy – This assesses the financial implications of adverse events, including cyber security events.
- Mission Risk Strategy –This looks at the risk that any failure will render a utility unable to safely deliver power.
- Cyber Security Risk Strategy – This looks at the impacts of cyber security compromises.

These three are related – the risk of physical compromise of the information, business, and operational systems (commonly call IT and OT) clearly drives financial and mission risk, and the utility's strategy related to financial and missions risk should be a factor in setting targets and requirements for the cyber security risk. While all three risk categories are important, the scope of this document is limited to the Cyber Security Risk Strategy.

In this analysis, the cyber security risk strategy is divided into three categories based on the methodology:

- **Maturity Model Methodology** – maturity models provide utilities with a method to assess the degree of an organization's alignment with the best practices in the structure and operation of the organization and its IT&OT systems.
- **Control-Based Methodology** – Controls based methodologies address the technical aspects related to the configuration of the IT&OT systems and protective hardware and software.
- **Compliance Methodology** – Compliance methodologies focus on specific mandatory requirements. Though the starting point is rules, the compliance methodology must necessarily be extended to control-level requirements. At this time, there are only regulations for the bulk electric systems.

These three methodologies pertain to some common and some different electric sector domains, e.g., nuclear, distribution, generation, and are associated with the guidance documents described

above and included in Figure 2-1 below. The bulk of this document provides comparative analyses between the documents relevant to the methodologies.

2.1 Pulling it all Together

The comparative analyses that follow provide a unified reference for each methodology. Each methodology, however, cannot stand alone. An organizational strategy, for example, is not useful unless the organization has an effective strategy for controls or if the strategy is developed without regard to regulations pertaining to the bulk electric system, if applicable.

These different aspects must be considered in a coordinated way and then combined into a unified cyber security risk strategy and, ultimately, into the Enterprise Risk Management Process and Strategy.

Development of a cyber security risk strategy is best accomplished by considering several guidance documents, specifically:

- DOE Risk Management Process
- Executive Order 13636
- NIST Cyber Security Framework

2.2 Where Do You Start?

The best way for a utility to get started is to quickly review the documents and not get into too much detail. A utility should then use the comparative analyses provided here and in the companion documents, with the documents at hand, as a guide to building the cyber security risk strategy step-by-step.

Figure 2-1 below provides an overview of an enterprise risk management process and strategy and the security methodologies that may be used to implement this process and strategy. Also included are documents that a utility may use in their enterprise to address the risk of operational systems. Following is a description of each of the elements of the diagram and the three paths in the diagram (maturity model, control-based, and compliance).

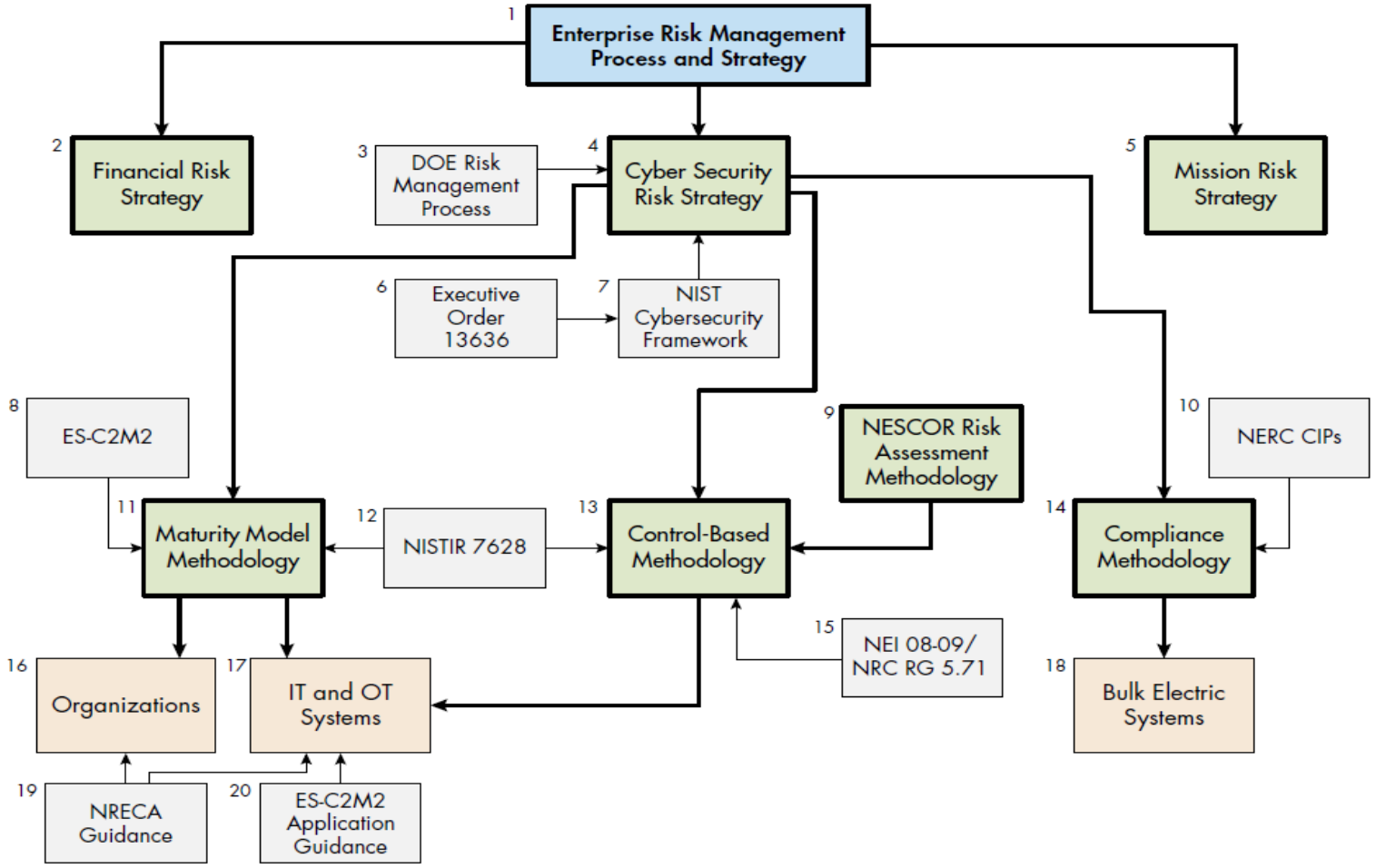

Figure 2-1
Enterprise Risk Management Process and Strategy

Each of the elements in the diagram is underlined below and includes the diagram reference number.

At the highest level is the enterprise risk management process and strategy (1). This process includes all the risk areas that a utility will address, for example, legal, mission, financial, and budgetary. A strategy should be developed to address risk in each of the areas. Each strategy should be based on the enterprise risk management strategy and process and further refine that overall strategy to the specific risk area. Included in the diagram are three risk strategy areas: financial risk strategy (2), mission risk strategy (5), and cyber security risk strategy (4). The balance of the diagram focuses on the cyber security risk strategy.

The DOE Risk Management Process (3) provides high level guidance on cyber security risk management. The document should be used by a utility in the development of the cyber security risk strategy that is specific to the utility's needs. Utilities vary in many dimensions such as size; the domains that are implemented, e.g., generation, transmission, distribution; and the overall system and network architecture. This cyber security risk strategy should be at a high level and apply to all systems within the utility.

A second document that may be used in the development of the cyber security risk strategy is the NIST Cybersecurity Framework (7). The NIST CSF focuses on using business drivers to guide cyber security activities and was developed in response to the EO 13636 (6). The EO includes other requirements:

- Cyber security information sharing
- Privacy and civil liberties protection
- Voluntary critical infrastructure cyber security program
- Identification of critical infrastructure at greatest risk.

The cyber security risk strategy may be used as a reference in the implementation of the three methodologies: maturity model methodology (11), control-based methodology (13), and the compliance methodology (14).

A. The maturity model methodology uses the ES-C2M2 (8) document and the ES-C2M2 toolkit in the assessment. Currently, the ES-C2M2 is applied to organizations (16) rather than systems. To apply the ES-C2M2 to systems, ES-C2M2 application guidance (20) is used for IT and OT systems (17). The security controls are defined in the NISTIR 7628 (12) and the National Rural Electric Cooperative (NRECA) Guidance (19).

B. The control-based methodology uses the NESCOR risk assessment methodology (9) in the cyber security assessment of IT and OT systems (17) and the implemented security controls. The security controls are defined in NEI 08-09/NRC RG 5.71 (15) and in the NISTIR 7628 (12). For the NEI/NRC controls, the utility needs to determine if specific controls are necessary to counter a given risk and/or if alternate/compensating[4] controls may be used. The NISTIR 7628 requirements will need to be tailored and/or configured for each system(s) based on a preliminary risk assessment where the objective levels for confidentiality, integrity, and availability

[4] A compensating control is a cyber security control implemented as an alternative to a recommended control that provides equivalent or comparable control.

have been determined. For example, if the integrity level is set at high, the most appropriate technical control is cryptography. This is a significant technical control.

C. The compliance methodology uses the NERC CIP (10) standards and applies them to bulk electric systems (18). The NERC CIPs are mandatory standards. A utility cyber security risk strategy may be used to augment these mandatory standards. (Note: the compliance methodology is included for completeness. It is not discussed further in this technical update.)

3
COMPARATIVE ANALYSIS

As stated previously, all the referenced documents are at different levels of granularity and are intended for different purposes. The NIST CSF applies to all sixteen critical infrastructures and the ES-C2M2 applies only to the electric sector. Both documents may be used to manage risk from an organization perspective. One difference is that the ES-C2M2 is focused on the cyber security *maturity* of an organization and the NIST CSF provides general guidance on cyber security risk activities. Because both documents provide guidance on addressing cyber security risk, a comparative analysis was performed to provide utilities with information on the relationship between the *practices* in the ES-C2M2 and the *subcategories* in the NIST CSF. At least one ES-C2M2 practice is applicable to each NIST CSF subcategory. However, the relationship is not always one to one, for example, some ES-C2M2 practices are applicable to several NIST CSF subcategories.

Also included in the comparative analysis are the NISTIR 7628 security requirements. These are typically at a lower level of granularity than either the NIST CSF subcategories or the ES-C2M2 practices. The NISTIR 7628 security requirements fall into three categories: Governance, Risk and Compliance (GRC); Common Technical, and Unique Technical. Listed next to each NISTIR 7628 security requirement are the related ES-C2M2 practices.

The goal of the comparative analysis is to provide an overview of the relationship among the three documents. Because the documents are at different levels, the relationships are not exact. The comparative analysis is included in Table 3-3 below. The columns for the ES-C2M2 and the NIST CSF are extracted from the draft *Energy Sector Cybersecurity Framework Implementation Guidance.* Table 3-4, Table 3-5, Table 3-6, and Table 3-7 include a comparative analysis of the ES-C2M2 practices and the NIST CSF Tiers and are extracted from the draft *Energy Sector Cybersecurity Framework Implementation Guidance*. Included in Appendix A is a list of the ES-C2M2 practices that are not associated with any of the NIST CSF subcategories.

The ES-C2M2 practices are referenced by the domain abbreviation, a hyphen, the objective number, and the practice letter. For example, “ACM-1a” denotes practice “a” in Objective 1 of the Asset, Change, and Configuration Management domain. The domain abbreviations are listed in below.

Table 3-1
ES-C2M2 Domains and Abbreviations

[The following information is extracted from the ES-C2M2.]

Domain	Abbreviation
Asset, Change, and Configuration Management	ACM
Cybersecurity Program Management	CPM
Supply Chain and External Dependencies Management	EDM
Identity and Access Management	IAM
Event and Incident Response, Continuity of Operations	IR
Information Sharing and Communications	ISC
Risk Management	RM
Situational Awareness	SA
Threat and Vulnerability Management	TVM

The NISTIR 7628 requirements are referenced as SG (smart grid), family, and then the requirement number. For example, SG.AC-1 denotes the requirement for Smart Grid Access Control (family), Access Control Policies and Procedures (requirement). The table below lists the abbreviations for the families.

Table 3-2
Abbreviations for NISTIR 7628 Smart Grid Requirements Families

[The following information is extracted from the NISTIR 7628.]

Ref.	NIST Smart Grid Security Requirements Families
SG.AC	Access Control
SG.AT	Awareness and Training
SG.AU	Audit and Accountability
SG.CA	Security Assessment and Authorization
SG.CM	Configuration Management
SG.CP	Continuity of Operations
SG.IA	Identification and Authentication
SG.ID	Information and Document Management
SG.IR	Incident Response
SG.MA	Smart Grid system Development and Maintenance
SG.MP	Media Protection
SG.PE	Physical and Environmental Security
SG.PL	Strategic Planning
SG.PM	Security Program Management
SG.PS	Personnel Security
SG.RA	Risk Management and Assessment
SG.SA	Smart Grid system and Services Acquisition
SG.SC	Smart Grid System and Communication Protection
SG.SI	Smart Grid System and Information Integrity

3.1 Analysis Guidance

The ES-C2M2 practices that are associated with the NIST CSF subcategories vary in specificity. For example, in the first row in Table 3-3 below, the NIST CSF subcategory is ID-AM-1: Physical devices and systems within the organization are inventoried. The most directly related ES-C2M2 practice is ACM-1a: There is an inventory of OT and IT assets that are important to the delivery of the function. This practice is at maturity indicator level (MIL) 1. As described in the ES-C2M2, the MILs are hierarchical, with MIL 1 at the lowest level. The practices at MIL 2 and MIL 3 correspond to a higher maturity level and build upon the practices at the lower level. Also included in the table is ACM-1c that states: Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards). This practice includes additional detail that builds upon the NIST CSF subcategory content. The inclusion of all the related ES-C2M2 practices allows a utility to see progression from MIL 1 to MIL 3. The ES-C2M2 practices that are most closely related to the NIST CSF

subcategories are underlined in the table below. (Note: The current version of the NRECA Guidance Document aligns directly with the ES-C2M2 and therefore is not included.)

The NISTIR 7628 requirements are divided into three categories: Governance, Risk and Compliance; Common Technical Controls; and Unique Technical Controls. This categorization was not considered when associating the security requirements to the ES-C2M2 practices and the NIST CSF subcategories.

Included in a separate document, EPRI technical update 3002004712, *Risk Management in Practice - Comparative Analyses Tables* are several other tables that provide additional information. Below is a summary of these additional tables:

- A comparative analysis of the NISTIR 7628 security requirements and the NIST SP 800-53 security controls to the NIST CSF subcategories. This comparative analysis is provided because many organizations are using the NIST SP 800-53 as an overall security control document and the NISTIR 7628 is based on NIST SP 800-53.
- A comparative analysis of the NEI 08-09, NRC RG 5.71, and NISTIR 7628 requirements.
- A table relating the NESCOR failure scenarios, the common mitigations, and the vulnerability classes to the ES-C2M2 practices.

A comparative analysis of the ES-C2M2 practices, the NISTIR 7628 security requirements, and the NIST SP 800-53 security controls.

Table 3-3
Comparative Analysis of the NIST CSF, the ES-C2M2, and the NISTIR 7628

[The following information is extracted from the NIST CSF, the draft *Energy Sector Cybersecurity Framework Implementation Guidance*, and the NISTIR 7628.]

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
ACM-1a	ACM-1c	ACM-1e ACM-1f	SG.CM-2 (ACM-1a) SG.CM-8 (ACM-1a, 1c, 1e, 1f)	IDENTIFY (ID	**Asset Management (AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried
ACM-1a	ACM-1c	ACM-1e ACM-1f	SG.CM-2 (ACM-1a) SG.CM-8 (ACM-1a, 1c, 1e, 1f)			**ID.AM-2:** Software platforms and applications within the organization are inventoried
	RM-2g	ACM-1e	SG.AC-5 (RM-2g) SG.CA-4 (RM-2g, ACM-1e) SG.PM-4 (RM-2g, ACM-1e)			**ID.AM-3:** Organizational communication and data flows are mapped
EDM-1a	EDM-1c EDM-1e	EDM-1g RM-1c	SG.AC-18 (EDM-1a)			**ID.AM-4:** External information systems are catalogued
ACM-1a ACM-1b	ACM-1c ACM-1d		SG.CP-2 (ACM-1d) SG.RA-3 (ACM-1b, 1c, 1d) SG.SC-6 (ACM-1b, 1c, 1d)			**ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
WM-1a WM-1b	WM-1c		SG.CP-3 (WM-1a, 1b, 1c) SG.PL-3 (WM-1a, 1b, 1c) SG.PS-9 (WM-1a, 1b, 1c) SG.SC-19 (1c)			**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
EDM-1b	EDM-1d EDM-1f	EDM-1g RM-1c			**Business Environment (BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated
EDM-1b	EDM-1d CPM-1c EDM-1f	EDM-1g RM-1c				**ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated
	RM-3b	RM-1c	SG.PM-7 (RM-3b, 1c)			**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated
ACM-1a ACM-1b EDM-1a	ACM-1c ACM-1d EDM-1c EDM-1e	ACM-1e ACM-1f RM-1c EDM-1g	SG.CP-9 (ACM-1b, 1d) SG.SA-11 (EDM-1a, 1c, 1e)			**ID.BE-4**: Dependencies and critical functions for delivery of critical services are established

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
IR-4a IR-4b IR-4c	IR-4e		SG.CP-2 (IR-4a, 4b, 4c) SG.CP-10 (IR-4a, 4b, 4c)			**ID.BE-5**: Resilience requirements to support delivery of critical services are established
	CPM-2g	RM-3e CPM-5d	All -1 requirements, except for SG.RA-1 (CPM-2g, 5d) SG.RA-1 (RM-3e)		**Governance (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 information security policy is established
WM-1a WM-1b	ISC-2b WM-1c WM-1d WM-5b	WM-1e WM-1f WM-1g	SP.PS-9 (WM-1a, 1b, 1c, 1d, 5b) SG.SC-19 (WM-1a, 1b, 1c, 1d)			**ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
		RM-3f ACM-4f IAM-3f TVM-3f SA-4f ISC-2f IR-3n IR-5f EDM-3f WM-5f CPM-2k	All -1 requirements (RM-3f ACM-4f IAM-3f TVM-3f SA-4f ISC-2f IR-3n IR-5f EDM-3f WM-3f CPM-2k)			**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
RM-2a RM-2b		RM-2h RM-1c RM-1e RM-3e	SG.PM-5 (RM-1c, 2a, 2b, 2h)			**ID.GV-4**: Governance and risk management processes address cybersecurity risks
TVM-2a TVM-2b	TVM-2d TVM-2e TVM-2f	RM-1c RM-2j TVM-2i TVM-2j TVM-2k TVM-2l TVM-2m	SG.CA-2 (TVM-2b, 2e, 2i, 2j, 2k, RM-1c) SG.CA-6 (TVM-2b, 2e, 2i, 2j, 2k, RM-1c) SG.RA-6 (TVM-2b, 2e, 2i, 2j, 2k, RM-1c) SG.SA-10 (TVM-2b, 2e, 2i, 2j, 2k, RM-1c) SG.SI-2, (TVM-2b, 2i, 2j, 2k, RM-1c) SG.SI-5 (TVM-2a)		**Risk Assessment (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
TVM-1a TVM-1b TVM-2a TVM-2b	TVM-2d		SG.AT-5 (TVM-1a, 1b, 2a, 2b, 2d) SG.SI-5 (TVM-1a, 1b, 2a, 2b, 2d)			**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources
TVM-1a TVM-1b	TVM-1d TVM-1e	RM-2j TVM-1j	SG.RA-4, (TVM-1b, 1d, 1e, RM-2j) SG.SI-5 (TVM-1a, 1b, 1e)			**ID.RA-3:** Threats, both internal and external, are identified and documented

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
	TVM-1d TVM-1f	TVM-1i RM-1c	SG.PM-5 (TVM-1f, 1i, RM-1c) SG.PM-7 (RM-1c) SG.RA-3 (TVM-1d, 1f, 1i, RM-1c) SG.RA-4 (RM-1c)			**ID.RA-4:** Potential business impacts and likelihoods are identified
		RM-1c RM-2j TVM-2m	SG.RA-3 (TVM-2m) SG.RA-4 (TVM-2m)			**ID.RA-5**: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
	RM-2e TVM-1d	RM-1c RM-2j IR-3m	SG.PM-5 (RM-2e, 1c, 2j)			**ID.RA-6:** Risk responses are identified and prioritized
RM-2a RM-2b	RM-1a RM-1b RM-2c RM-2d RM-2e RM-2g RM-3a RM-3b RM-3c RM-3d	RM-1c RM-1d RM-1e RM-2h RM-2j RM-3g RM-3h RM-3i	SG.PM-5 (all practices listed)		**Risk Management Strategy (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

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
		RM-1c RM-1e	SG.PM-5 (RM-1c, 1e) SG.RA-2 (RM-1c, 1e)			ID.RM-2: Organizational risk tolerance is determined and clearly expressed
	RM-1b	RM-1c	SG.PM-5 (RM-1b, 1c) SG.PM-7 (RM-1b, 1c)			**ID.RM-3**: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis
IAM-1a IAM-1b IAM-1c	IAM-1d IAM-1e IAM-1f	RM-1c IAM-1g	SG.AC-3 (IAM-1a, 1b, 1c, 1d, 1e, 1f) SG.AC-19 (IAM-1b) SG.AC-21 (IAM-1b) SG.IA-2 (IAM-1a, 1g) SG.IA-3 (IAM-1b, 1e) SG.IA-4 (IAM-1a, 1b) SG.IA-5 (IAM-1a, 1b) SG.IA-6 (IAM-3e)	**PROTECT (PR)**	**Access Control (AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users
IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g	SG.PE-2 (IAM-2a-2g) SG.PE-3 (IAM-2b)			**PR.AC-2:** Physical access to assets is managed and protected

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
IAM-2a IAM-2b IAM-2c	*IAM-2d* IAM-2e IAM-2f	IAM-2g	SG.AC-2 (IAM-2a, 2b) SG.AC-13 (IAM-2a) SG.AC-14 (IAM-2a) SG.AC-15 (IAM-2a, 2b, 2c, 2e)			**PR.AC-3:** Remote access is managed
	IAM-2d		SG.AC-6 (IAM-2d) SG.AC-7 (IAM-2d)			**PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties
CPM-3a	CPM-3b CPM-3c	CPM-3d	SG.AC-5 (CPM-3a, 3b, 3c) SG.SC-7 (CPM-3a, 3b, 3c) SG.AC-19 (CPM-3a, 3b)			**PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate
WM-3a WM-4a	WM-3b WM-3c WM-3d	WM-3g WM-3h WM-3i	SG.AT-2 (WM-3a, 3b, 3c, 3d, 3g, 3h, 4a) SG.AT-3 (WM-3a, 3b, 3c, 3d) SG.AT-7 (WM-3a, 3g)		**Awareness and Training (AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained
WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g	SG.AT-3 (WM-1a, 1c, 1d) SG.CP-4 (WM-1a, 1c) SG.IR-3 (WM-1a, 1c)			**PR.AT-2:** Privileged users understand roles & responsibilities

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
			SG.PS-9 (WM-1a, 1c, 1d) SG.SC-19 (WM-1a, 1c, 1d)			
WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g	SG.PS-9 (WM-1a, 1c, 1d)			**PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g	SG.AT-3 (WM-1a, 1c) SG.PM-8 (WM-1a, 1c), SG.PS-9 (WM-1a, 1c, 1d)			**PR.AT-4:** Senior executives understand roles & responsibilities
WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g	SG.AT-3 (WM-1a, 1c) SG.PS-9 (WM-1a, 1c, 1d)			**PR.AT-5:** Physical and information security personnel understand roles & responsibilities
TVM-1c TVM-2c			SG.SC-26 (TVM-1c, 2c)		**Data Security (DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
TVM-1c TVM-2c			SG.SC-8 (TVM-1c, 2c) SG.SC-9 (TVM-1c, 2c)			**PR.DS-2:** Data-in-transit is protected
ACM-3a ACM-3b	ACM-3c ACM-3d ACM-4a ACM-4b ACM-4c ACM-4d	ACM-3f ACM-4e ACM-4f ACM-4g	SG.CM-8 (ACM-3b, 4a, 4b, 4d, 4e) SG.CM-9 (ACM-3b, 3d, 4a, 4e) SG.MP-6 (ACM-3d, 4a) SG.PE-10 (ACM-3b, 3d, 4a)			**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition
TVM-1c TVM-2c	CPM-3b		SG.SC-5 (TVM-1c, 2c, CPM-3b)			**PR.DS-4:** Adequate capacity to ensure availability is maintained
TVM-1c TVM-2c	CPM-3b	TVM-2n	SG.AC-6 (TVM-1c, 2c) SG.AC-7 (TVM-1c, 2c) SG.SC-7 (TVM-1c, 2c, CPM-3b) SG.SC-9 (TVM-1c, 2c) SG.SC-12 (TVM-1c, 2c)			**PR.DS-5:** Protections against data leaks are implemented

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
	SA-2e	SA-2i	SG.SI-7 (SA-2e, 2i)			**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity
	ACM-3c	ACM-3e	SG.CM-2 (ACM-3c, 3e)			**PR.DS-7:** The development and testing environment(s) are separate from the production environment
ACM-2a ACM-2b	ACM-2c	ACM-2d ACM-2e	SG.CM-2 (ACM-2a, 2b, 2c, 2d, 2e) SG.CM-6 (ACM-2a, 2b) SG.SA-9 (ACM-2a, 2b)		**Information Protection Processes and Procedures (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-1:** A baseline configuration of information technology/industrial control systems is created and maintained
	ACM-3d		SG.SA-3 (ACM-3d) SG.SA-8 (ACM-3d) SG.SA-9 (ACM-3d) SG.SA-10 (ACM-3d)			**PR.IP-2:** A System Development Life Cycle to manage systems is implemented
ACM-3a ACM-3b	ACM-3c ACM-3d ACM-4a	ACM-3e ACM-3f ACM-4e	SG.CM-3 (ACM-3a, 3b, 3c, 3d, 4a, 4e) SG.CM-4 (ACM-3a, 3e, 4a, 4e) SG.CM-5 (ACM-4a)			**PR.IP-3:** Configuration change control processes are in place

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
			SG.CM-6 (ACM-3b, 4a, 4e) SG.CM-10 (ACM-3d, 4a) SG.SA-9 (ACM-3b, 3d, 4a)			
IR-4a IR-4b			SG.CP-5 (IR-4a, 4b) SG.IR-10 (IR-4a, 4b)			**PR.IP-4:** Backups of information are conducted, maintained, and tested periodically
		ACM-4f RM-3f	SG.PE-1 (ACM-4f, RM-3f) SG.PE-8 SG.PE-9 SG.PE-12 (ACM-4f)			**PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met
	ACM-3d		SG.MP-6 (ACM-3d)			**PR.IP-6:** Data is destroyed according to policy
		CPM-1g	SG.CA-2 (CPM-1g) SG.CA-3 (CPM-1g) SG.CA-6 (CPM-1g) SG.PL-2 (CPM-1g)			**PR.IP-7:** Protection processes are continuously improved
ISC-1a ISC-1b	ISC-1c ISC-1d ISC-1e ISC-1f ISC-1g ISC-2b	ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l	SG.AT-5 (ISC-1a-j, 1l)			**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
IR-4c	TVM-1d IR-3f IR-4d IR-4f IR-5a IR-5b IR-5d	RM-1c IR-3k IR-3m IR-4i IR-4j IR-5e IR-5f IR-5g IR-5h IR-5i	SG.CP-2 (IR-3f, 4d, 5a, 5b, 5d) SG.CP-3 (IR-5h, 5i) SG.CP-6 (IR-3k, 4j, 5g) SG.IR-1 (IR-3f, 5a, 5d, 5e, 5f, 5g) SG.IR-2 (IR-3f, 5a, 5d, 5e, 5f, 5g, 5h, 5i) SG.IR-11 (IR-5e)			**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
	IR-3e IR-4f	IR-3k IR-4i	SG.CP-5 (IR-4f) SG.IR-4 (IR-3e)			**PR.IP-10:** Response and recovery plans are tested
WM-2a WM-2b	*WM-2c* WM-2d	WM-2e WM-2f WM-2g WM-2h	SG.PS-1 (WM-2g) SG.PS-2 (WM-2e, 2f, 2g) SG.PS-3 (WM-2c) SG.PS-4 (WM-2b) SG.PS-5 (WM-2d) SG.PS-7 (WM-2h) SG.PS-8 (WM-2h) SG.PS-9 (WM-2h)			**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
	TVM-3a	TVM-3e	SG.RA-4 (TVM-3a) SG.RA-5 (TVM-3a) SG.RA-6 (TVM-3a) SG.SI-2 (TVM-3a)			**PR.IP-12:** A vulnerability management plan is developed and implemented

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
ACM-3a ACM-3b	ACM-4c	ACM-3f	SG.MA-3 (ACM-3a, 3b, 3f) SG.MA-4 (ACM-4c) SG.MA-5 (ACM-4c) SG.MA-7 (ACM-4c)		**Maintenance (MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
IAM-2a IAM-2b IAM-2c SA-1a IR-1c	IAM-2d IAM-2e IAM-2f	IAM-2g IAM-2h	SG.MA-6 (IAM-2a, 2b, 2c, 2e, 2g, 2h)			**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
SA-1a SA-2a	SA-1b SA-1c SA-2c SA-4a	SA-1d SA-1e SA-3d SA-4e SA-4f SA-4g	SG.AU-1 (4a, 4e, 4f, 4g) SG.AU-2 (SA-1a, 1b) SG.AU-3 (SA-4a) SG.AU-6 (SA-1c, 1d, 1e, 2a, 2c, 3d) SG.AU-7 (SA-3d) SG.AU-15 (SA-1b, 1c, 1d)		**Protective Technology (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
IAM-2a IAM-2b IAM-2c		IAM-3e IAM-3f	SG.AC-17 (IAM-2a, 2b, 3e) SG.MP-4 (IAM-2a, 2b) SG.MP-5 (IAM-2a, 2b)			**PR.PT-2:** Removable media is protected and its use restricted according to policy

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g IAM-2h IAM-2i	SG.AC-3 (IAM-2f) SG.AC-4 (IAM-2a, 2b) SG.CM-7 (ACM-2c)			**PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality
CPM-3a	CPM-3b CPM-3c	CPM-3d	SG.SC-7 (CPM-3b, 3c) SG.SC-18 (CPM-3b, 3c)			**PR.PT-4:** Communications and control networks are protected
SA-2a			SG.AU-6 (SA-2a) SG.CA-6 (SA-2a)	**DETECT (DE)**	**Anomalies and Events (AE):** Anomalous activity is detected in a timely manner 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
		IR-1f IR-2i IR-3h	SG.AU-6 (IR-1f, 2i) SG.IR-5 (IR-1f, 2i, 3h)			**DE.AE-2:** Detected events are analyzed to understand attack targets and methods
	IR-1e	IR-1f IR-2i	SG.AU-6 (IR-1f, 2i) SG.IR-5 (IR-1e, 1f) SG.IR-6 (IR-1e, 1f)			**DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors
IR-2b	TVM-1d IR-2d	RM-2j IR-2g	SG.IR-5 (IR-2b, 2d)			**DE.AE-4:** Impact of events is determined

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
IR-2a	TVM-1d IR-2d SA-2d	RM-2j IR-2g	SG.SI-4 (IR-2a, 2d, 2g)			**DE.AE-5:** Incident alert thresholds are established
SA-2a SA-2b	SA-2e SA-2f TVM-1d	SA-2g SA-2i	SG.CA-6 (SA-2a, 2b, 2g) SG.SC-7 (SA-2a, 2b, 2e, 2f, 2g, 2i) SG.SI-4 (SA-2a, 2b, 2e, 2f, 2g, 2i)		**Security Continuous Monitoring (CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
SA-2a SA-2b	SA-2e	SA-2i	SG.PE-4 (SA-2a, 2b, 2e, 2i)			**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events
SA-2a SA-2b	SA-2e	SA-2i	SG.PS-1 (SA-2a, 2b, 2e)			**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events
SA-2a SA-2b	SA-2e CPM-4a	SA-2i	SG.SI-3 (SA-2a, 2b, 2e, 2i)			**DE.CM-4:** Malicious code is detected
SA-2a SA-2b	SA-2e	SA-2h SA-2i	SG.SC-16 (SA-2a, 2b, 2e, 2h, 2i)			**DE.CM-5:** Unauthorized mobile code is detected
EDM-2a SA-2a SA-2b	SA-2e	EDM-2j EDM-2n	SG.PS-7 (SA-2a, 2b, 2e, EDM-2a, 2n) SG.SI-4 (SA-2b, 2e, EDM-2j)			**DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
SA-2a SA-2b	SA-2e SA-2f TVM-1d	SA-2g SA-2i	SG.AC-15 (SA-2a, 2b, 2e, 2f, 2g, 2i) SG.AC-16 (SA-2a, 2b, 2e, 2g, 2i) SG.AC-17 (SA-2a, 2b, 2e, 2f, 2g, 2i) SG.CM-4 (SA-2a, 2b, 2i) SG.PE-4 (SA-2a, 2b, 2e, 2i) SG.SI-4 (SA-2a, 2b, 2e, 2f, 2g, 2i)			**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed
	TVM-2e	TVM-2i TVM-2j TVM-2k RM-1c	SG.RA-6 (TMV-2e, 2i, 2j)			**DE.CM-8:** Vulnerability scans are performed
WM-1a	WM-1d	WM-1f	SG.SC-19 (WM-1a, 1d)		**Detection Processes (DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability
	IR-1d IR-5a TVM-1d	RM-1c RM-2j IR-1g IR-5f	SG.IR-1 (IR-5a, 5f)			**DE.DP-2:** Detection activities comply with all applicable requirements

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
	IR-3e	IR-3j	SG.SI-4 (IR-3e)			**DE.DP-3:** Detection processes are tested
IR-1b IR-3c ISC-1a	ISC-1c ISC-1d	IR-3n ISC-1h ISC-1j	SG.AU-6 (IR-1b, 3c, ISC-1a, 1h) SG.IR-7 (IR-1b, 3c, 3n, ISC-1a)			**DE.DP-4:** Event detection information is communicated to appropriate parties
		IR-3h IR-3k	SG.RA-6 (IR-3h) SG.CA-3 (IR-3h)			**DE.DP-5:** Detection processes are continuously improved
	IR-3d		SG.CP-2 (IR-3d) SG.CP-10 (IR-3d)	**RESPOND (RS)**	**Response Planning (RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event
IR-3a	IR-5b		SG.CP-3 (IR-3a, 5b) SG.IR-2 IR-3a, 5b) SG.IR-11 (IR-3a, 5b)		**Communications (CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
IR-1a IR-1b			SG.IR-7 (IR-1a, 1b)			**RS.CO-2:** Events are reported consistent with established criteria
ISC-1a ISC-1b	ISC-1c ISC-1d IR-3d	IR-3i IR-3l	SG.CP-2 (ISC-1a, 1b, 1c, 3i, 3l) SG.IR-11 (ISC-1a, 1b, 1c, 3i, 3l)			**RS.CO-3:** Information is shared consistent with response plans
	IR-3d IR-5b		SG. CP-2 (IR-5b) SG.IR-11 (IR-5b)			**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans
ISC-1a	ISC-1c ISC-1d ISC-1e ISC-1f	ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l	SG.AT-5 (ISC-1a, 1c, 1d, 1e, 1f, 1h, 1i, 1l) SG.SI-5 (ISC-1a, 1c, 1d, 1e, 1f, 1h, 1i, 1l)			**RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
	IR-1e	IR-1f	SG.AU-6 IR-1f) SG.IR-8 (IR-1f)		**Analysis (AN):** Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated
	TVM-1d IR-2d	RM-2j IR-2g	SG.IR-5 (IR-2d)			**RS.AN-2:** The impact of the incident is understood

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
	IR-3d	IR-3h IR-3i	SG.IR-5 (IR-3d, 3h) SG.IR-8 (IR-3h)			**RS.AN-3:** Forensics are performed
IR-2a	IR-1d IR-1e		SG.CP-2 (IR-1d)			**RS.AN-4:** Incidents are categorized consistent with response plans
IR-3b			SG.IR-5 (IR-3b)		**Mitigation (MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained
IR-3b			SG.IR-5 (IR-3b)			**RS.MI-2:** Incidents are mitigated
TVM-2c	TVM-2f TVM-2g	RM-2j TVM-2m TVM-2n	SG.RA-6 (TVM-2c, 2g, 2m, 2n)			**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks
		IR-3h	SG.CP-2 (IR-3h) SG.IR-5 (IR-3h) SG.IR-9 (IR-3h)		**Improvements (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
		IR-3h IR-3k	SG.CP-6 (IR-3h, 3k) SG.IR-1 (IR-3h, 3k) SG.IR-2 (IR-3k) SG.IR-5 (IR-3k)			**RS.IM-2:** Response strategies are updated

ES-C2M2 Practices			NISTIR 7628	NIST Cybersecurity Framework		
MIL 1	MIL 2	MIL3		Function	Category	Subcategory
IR-3b	IR-3d	IR-3o IR-4k	SG.CP-2 (IR-3b, 3d)	RECOVER (RC)	**Recovery Planning (RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event
		IR-4i	SG.CP-6 (IR-4i)		**Improvements (IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned
		IR-3h IR-3k	SG.CP-6 (IR-3k) SG.IR-1 (IR-3k)			**RC.IM-2:** Recovery strategies are updated
		RM-1c			**Communications (CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed
	IR-3d					**RC.CO-2:** Reputation after an event is repaired
	IR-3d		SG.CP-2 (IR-3d)			**RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams

Table 3-4
NIST CSF Tier 1 and the ES-C2M2

[The following information is extracted from the draft *Energy Sector Cybersecurity Framework Implementation Guidance*.]

NIST Cybersecurity Framework			ES-C2M2 Reference		
Implementation Tier	**Tier Category**	**Characteristics**	**MIL 1**	**MIL 2**	**MIL3**
Tier 1: Partial	Risk Management Process	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.	RM-2a* RM-2b*		
		Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	RM-2a* RM-2b*		
	Integrated Risk Management Program	There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established.	RM-2a* RM-2b*		
		The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.	RM-2a* RM-2b*		
		The organization may not have processes that enable cybersecurity information to be shared within the organization.	RM-2a* RM-2b*		
	External Participation	An organization may not have the processes in place to participate in coordination or collaboration with other entities.	RM-2a* RM-2b*		

*As described in the Framework, these Tier characteristics correspond to the specified C2M2 practices performed in an ad hoc manner.

Table 3-5
NIST CSF Tier 2 and the ES-C2M2

[The following information is extracted from the draft *Energy Sector Cybersecurity Framework Implementation Guidance*.]

NIST Cybersecurity Framework			ES-C2M2 Reference		
Implementation Tier	**Tier Category**	**Characteristics**	**MIL 1**	**MIL 2**	**MIL3**
Tier 2: Risk Informed	Risk Management Process	Risk management practices are approved by management but may not be established as organizational-wide policy.		RM-3a* RM-3b*	
		Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.			RM-1c
	Integrated Risk Management Program	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established.	RM-2a RM-2b		
		Risk informed, management -approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties.	CPM-2a CPM-2b	RM-3a RM-3b RM-3c	RM-1c
		Cybersecurity information is shared within the organization on an informational basis.	ISC-1a		
	External Participation	The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.	EDM-1a EDM-1b	ISC-1c	RM-3e

*As described in the Framework, these Tier characteristics correspond to the specified C2M2 practices performed in an ad hoc manner.

Table 3-6
NIST CSF Tier 3 and the ES-C2M2

[The following information is extracted from the draft *Energy Sector Cybersecurity Framework Implementation Guidance*.]

NIST Cybersecurity Framework			ES-C2M2 Reference		
Implementation Tier	**Tier Category**	**Characteristics**	**MIL 1**	**MIL 2**	**MIL3**
Tier 3: Repeatable	Risk Management Process	The organization's risk management practices are formally approved and expressed as policy.			RM-3e
		Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.		TVM-1d	RM-1d CPM-1g
		There is an organization-wide approach to manage cybersecurity risk.	CPM-1a	RM-1a RM-1b	
	Integrated Risk Management Program	Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.			RM-3e RM-3g CPM-2i CPM-5d
		Personnel possess the knowledge and skills to perform their appointed roles and responsibilities		WM-3b WM-3c WM-3d	RM-3i ACM-4i IAM-3i TVM-3i SA-4i ISC-2i IR-5i EDM-3i WM-5i CPM-5f

NIST Cybersecurity Framework			ES-C2M2 Reference		
Implementation Tier	**Tier Category**	**Characteristics**	**MIL 1**	**MIL 2**	**MIL3**
		The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.	EDM-2a	ISC-1d	
	External Participation	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.			RM-1d RM-2j TVM-1j TVM-2m

Table 3-7
NIST CSF Tier 4 and the ES-C2M2

[The following information is extracted from the draft *Energy Sector Cybersecurity Framework Implementation Guidance*.]

NIST Cybersecurity Framework			**ES-C2M2 Reference**		
Implementation Tier	Tier Category	Characteristics	MIL 1	MIL 2	MIL3
Tier 4: Adaptive	Risk Management Process	The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.			RM-1d RM-2j TVM-1j TVM-2m
		Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.			RM-1d RM-3g CPM-1g
		There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.		TVM-1d	RM-2h RM-3e TVM-1i TVM-2j TVM-2l IR-3m IR-4h EDM-1g EDM-2k
	Integrated Risk Management Program	Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.			SA-3d SA-3e

NIST Cybersecurity Framework			ES-C2M2 Reference		
Implementation Tier	Tier Category	Characteristics	MIL 1	MIL 2	MIL3
		The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.			ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l
	External Participation	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.			ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l

4
GAP ANALYSIS

This section includes a summary of the gaps in the comparative analyses among the NISTIR 7628, the ES-C2M2, and the NIST CSF. Because the three documents have different scopes and levels of specificity, these differences may be acceptable.

4.1 NISTIR 7628 Gaps

Included in the companion document, *Risk Management in Practice Comparative Analyses Tables,* EPRI Technical Update 3002004712 is Table 1-4 that lists the NISTIR 7628 security requirements that are not associated with either the NIST CSF or the ES-C2M2 or both. Following is a summary of these gaps:

- Security requirements that are typically developed as internal policies or procedures such as SG.ID-2: Information and Document Retention, SG.PE-7: Physical Access Log Retention, and SG.SA-6: Software License Usage Restrictions.
- Security requirements that are more applicable to classified system, such as SG.SC-29: Application Partitioning and SG.SC-30: Information System Partitioning.
- Security requirements that are more applicable to the corporate environment, such as SG.SC-17: Voice-Over-Internet-Protocol and SG.PM-6: Security Authorization to Operate Process.
- Security requirements that are commonly used in federal government systems, such as SG.CA-5: Security Authorization to Operate and SG.PM-6: Security Authorization to Operate Process.

4.2 NIST CSF and ES-C2M2 Gap Analysis

Included in Appendix A is Table 7-1 that lists the ES-C2M2 practices that are not associated with any of the NIST CSF subcategories. Below is a summary of these differences.

In general, the majority of the practices that are not associated with the NIST CSF are in the management activities objective of each ES-C2M2 domain. This difference can be explained because the ES-C2M2 focuses on organization *maturity* and the NIST CSF provides more general guidance on the creation and management of a cyber security program.

Several practices were not associated in the following domains and objectives:

- 7.5 Situational Awareness: 3. Establish and Maintain a Common Operating Picture (COP)
- 7.7 Event and Incident Response, Continuity of Operations: 2. Escalate Cybersecurity Events and Declare Incidents
- 7.8 Supply Chain and External Dependencies Management: 2. Manage Dependency Risk
- 7.9 Workforce Management: 4. Increase Cybersecurity Awareness
- 7.10 Cybersecurity Program Management: 1. Establish Cybersecurity Program Strategy, 2. Sponsor Cybersecurity Program

5
SUMMARY AND NEXT STEPS

The focus of this technical update is to provide guidance on the various cyber security regulations, guidelines, and security specifications that may be applicable to the electric sector. This document is not intended to provide new guidance but rather to provide information on how to navigate and relate the diverse existing guidance that is applicable to the electric sector. Utility management and external organizations, such as DOE and state PUCs are requesting utilities to provide information on how they are meeting the various cyber security documents. The process flow and comparative analyses included in this technical update, and in the companion EPRI technical update 3002004712, *Risk Management in Practice Comparative Analyses Tables* are intended to provide this guidance. In addition, EPRI technical update 3002003332, *Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)* provides guidance on applying the ES-C2M2 to systems.

This is version 1.0 of this document, and version 1.0 of the companion documents. One of the objectives is to have a *baseline* set of tables that all utilities, research organizations, vendors, and others may use. Currently, utilities are developing their own tables or are requesting external companies to develop the tables. To move forward, it is important to have a baseline set that is agreed to by everyone. The intent is to make this information publicly available and have utilities use the information and provide comments on the documents.

The next steps are to receive comments and recommendations and then revise the tables. This review and revision process will take several months to ensure that all interested organizations have sufficient time to read and comment. Because it is not feasible to keep all the various tables synchronized when they are changed, the next phase will consider developing a database that contains all the information and making this publicly available. Also under consideration is adding additional international standards and guidelines to the tables, for example, ISO standards.

6
REFERENCES

1. The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, Revision 1, September 2014 [report].
2. U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),* Version 1.1, February 2014 [government publication].
3. National Electric Sector Cybersecurity Organization Resource (NESCOR), *Electric Sector Failure Scenarios and Impact Analyses,* Version 2.0, June 2014 [report].
4. U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Risk Management Process*, May 2012 [government publication].
5. U.S. Department of Energy (DOE), *Energy Sector Cybersecurity Framework Implementation Guidance*, draft for public comment, September 2014 [government publication].
6. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014 [government publication].
7. Office of the President, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, February 12, 2013 [government publication].
8. EPRI and DOE, *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology*, EPRI technical update 3002001181, 2013 [report] (The document is posted as a joint DOE/EPRI publication at: http://energy.gov/sites/prod/files/2014/05/f15/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology_1.pdf)
9. National Institute of Standards and Technology, NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, revision 4, April 2013 [government publication].
10. Nuclear Regulatory Commission, Regulatory Guidance 5.71, *Cyber Security Programs for Nuclear Facilities*, January 2010 [government publication].
11. Nuclear Energy Institute, **NEI 08-09** Revision 6, *Cyber Security Plan for Nuclear Power Reactors*, April 2010 [government publication].

A
ES-C2M2 GAP ANALYSIS

Table A-1
ES-C2M2 Gap Analysis

[The following information is extracted from the ES-C2M2.]

ES-C2M2	
Risk Management	
1. Establish Cyber Security Risk Management Strategy	
2. Manage Cyber Security Risk	
MIL2	f. Identified risks are monitored in accordance with the risk management strategy
MIL3	i. A current cybersecurity architecture is used to inform risk analysis
3. Management Activities	
Asset, Change and Configuration Management	
1. Manage Asset Inventory	
2. Manage Asset Configuration	
3. Manage Changes to Assets	
4. Management Activities	
MIL3	h. Responsibility and authority for the performance of asset inventory, configuration, and change management activities are assigned to personnel
	i. Personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities (Note: allocated at the tier level)
Identity and Access Management	
1. Establish and Maintain Identities	
2. Control Access	
3. Management Activities	
MIL2	a. Documented practices are followed to establish and maintain identities and control access
	b. Stakeholders for access and identity management activities are identified and involved
	c. Adequate resources (people, funding, and tools) are provided to support access and identity management activities
	d. Standards and/or guidelines have been identified to inform access and identity management activities
MIL3	g. Access and identity management activities are periodically reviewed to ensure conformance with policy
	h. Responsibility and authority for the performance of access and identity management activities are assigned to personnel
	i. Personnel performing access and identity management activities have the skills and knowledge needed to perform their assigned responsibilities (Note: allocated at the tier level)
Threat and Vulnerability Management	
1. Identify and Respond to Threats	
MIL3	h. The threat profile for the function is validated at an organization-defined frequency
2. Reduce Cybersecurity Vulnerabilities	
MIL2	h. Operational impact to the function is evaluated prior to deploying cybersecurity patches
3. Management Activities	
MIL3	g. Threat and vulnerability management activities are periodically reviewed to ensure conformance with policy

ES-C2M2	
	h. Responsibility and authority for the performance of threat and vulnerability management activities are assigned to personnel
	i. Personnel performing threat and vulnerability management activities have the skills and knowledge needed to perform their assigned responsibilities (Note: allocated at the tier level)
Situational Awareness	
1. Perform Logging	
2. Perform Monitoring	
MIL3	j. Risk register (RM-2j) content is used to identify indicators of anomalous activity
	k. Alarms and alerts are configured according to indicators of anomalous activity
3. Establish and Maintain a Common Operating Picture (COP)	
MIL2	a. Methods of communicating the current state of cybersecurity for the function are established and maintained
	b. Monitoring data are aggregated to provide an understanding of the operational state of the function (i.e., a common operating picture; a COP may or may not include visualization or be presented graphically)
	c. Information from across the organization is available to enhance the common operating picture
MIL3	e. Information from outside the organization is collected to enhance the common operating picture (Note: allocated at the tier level)
	f. Predefined states of operation are defined and invoked (manual or automated process) based on the common operating picture
4. Management Activities	
MIL2	b. Stakeholders for logging, monitoring, and COP activities are identified and involved
	c. Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities
	d. Standards and/or guidelines have been identified to inform logging, monitoring, and COP activities
MIL3	h. Responsibility and authority for the performance of logging, monitoring, and COP activities are assigned to personnel
	i. Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities (Note: allocated at the tier level)
Information Sharing and Communications	
1. Share Cybersecurity Information	
2. Management Activities	
MIL2	a. Documented practices are followed for information-sharing activities
	c. Adequate resources (people, funding, and tools) are provided to support information-sharing activities
	d. Standards and/or guidelines have been identified to inform information-sharing activities
MIL3	e. Information-sharing activities are guided by documented policies or other organizational directives
	g. Information-sharing activities are periodically reviewed to ensure conformance with policy
	h. Responsibility and authority for the performance of information-sharing activities are assigned to personnel
	i. Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities (Note: allocated at the tier level)
	j. Information-sharing policies address protected information and ethical use and sharing of information, including sensitive and classified information as appropriate
Event and Incident Response, Continuity of Operations	
1. Detect Cybersecurity Events	

ES-C2M2	
MIL3	h. The common operating picture for the function is monitored to support the identification of cybersecurity events (SA-3a)
2. Escalate Cybersecurity Events and Declare Incidents	
MIL1	c. Escalated cybersecurity events and incidents are logged and tracked
MIL2	e. Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are updated at an organization-defined frequency
	f. There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure
MIL3	h. Escalated cybersecurity events and declared cybersecurity incidents inform the common operating picture (SA-3a) for the function
3. Respond to Incidents and Escalated Cybersecurity Events	
MIL2	g. Training is conducted for cybersecurity event and incident response teams
4. Plan for Continuity	
MIL3	g. Business impact analyses are periodically reviewed and updated
	h. RTO and RPO are aligned with the function's risk criteria (RM-1c) (Note: allocated at the tier level)
5. Management Activities	
MIL2	c. Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response as well as continuity of operations activities
Supply Chain and External Dependencies Management	
1. Identify Dependencies	
2. Manage Dependency Risk	
MIL1	b. Cybersecurity requirements are considered when establishing relationships with suppliers and other third parties
MIL2	c. Identified cybersecurity dependency risks are entered into the risk register (RM-2j)
	d. Contracts and agreements with third parties incorporate sharing of cybersecurity threat information
	e. Cybersecurity requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate
	f. Agreements with suppliers and other external entities include cybersecurity requirements
	g. Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet cybersecurity requirements
	h. Agreements with suppliers require notification of cybersecurity incidents related to the delivery of the product or service
	i. Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements
MIL3	k. Cybersecurity requirements are established for supplier dependencies based on the organization's risk criteria (RM-1c) (Note: allocated at the tier level)
	l. Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products
	m. Acceptance testing of procured assets includes testing for cybersecurity requirements
3. Management Activities	
MIL2	a. Documented practices are followed for managing dependency risk
	b. Stakeholders for managing dependency risk are identified and involved
	c. Adequate resources (people, funding, and tools) are provided to support dependency risk management
MIL3	e. Dependency risk management activities are guided by documented policies or other organizational directives
	g. Dependency risk management activities are periodically reviewed to ensure conformance with policy
	h. Responsibility and authority for the performance of dependency risk management are assigned to personnel

ES-C2M2	
	i. Personnel performing dependency risk management have the skills and knowledge needed to perform their assigned responsibilities (Note: allocated at the tier level)
Workforce Management	
1. Assign Cybersecurity Responsibilities	
2. Control the Workforce Life Cycle	
3. Develop Cybersecurity Workforce	
MIL3	e. Cybersecurity workforce management objectives that support current and future operational needs are established and maintained
4. Increase Cybersecurity Awareness	
MIL2	b. Objectives for cybersecurity awareness activities are established and maintained
	c. Cybersecurity awareness content is based on the organization's threat profile (TVM-1d)
MIL3	d. Cybersecurity awareness activities are aligned with the predefined states of operation (SA-3f)
	e. The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency and improvements are made as appropriate
5. Management Activities	
MIL2	a. Documented practices are followed for cybersecurity workforce management activities
	c. Adequate resources (people, funding, and tools) are provided to support cybersecurity workforce management activities
	d. Standards and/or guidelines have been identified to inform cybersecurity workforce management activities
MIL3	e. Cybersecurity workforce management activities are guided by documented policies or other organizational directives
	f. Cybersecurity workforce management policies include compliance requirements for specified standards and/or guidelines
	g. Cybersecurity workforce management activities are periodically reviewed to ensure conformance with policy
	h. Responsibility and authority for the performance of cybersecurity workforce management activities are assigned to personnel
	i. Personnel performing cybersecurity workforce management activities have the skills and knowledge needed to perform their assigned responsibilities i. Personnel performing dependency risk management have the skills and knowledge needed to perform their assigned responsibilities (Note: allocated at the tier level)
Cybersecurity Program Management	
1. Establish Cybersecurity Program Strategy	
MIL1	a. The organization has a cybersecurity program strategy (Note: allocated at the tier level)
MIL2	b. The cybersecurity program strategy defines objectives for the organization's cybersecurity activities
	d. The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities
	e. The cybersecurity program strategy defines the structure and organization of the cybersecurity program
	f. The cybersecurity program strategy is approved by senior management
2. Sponsor Cybersecurity Program	
MIL1	a. Resources (people, tools, and funding) are provided to support the cybersecurity program (Note: allocated at the tier level)
	b. Senior management provides sponsorship for the cybersecurity program (Note: allocated at the tier level)
MIL2	c. The cybersecurity program is established according to the cybersecurity program strategy
	d. Adequate funding and other resources (i.e., people and tools) are provided to establish and operate a cybersecurity program aligned with the program strategy

ES-C2M2	
	e. Senior management sponsorship for the cybersecurity program is visible and active (e.g., the importance and value of cybersecurity activities is regularly communicated by senior management)
	f. If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program
	h. Responsibility for the cybersecurity program is assigned to a role with requisite authority
MIL3	i. The performance of the cybersecurity program is monitored to ensure it aligns with the cybersecurity program strategy (Note: allocated at the tier level)
	j. The cybersecurity program is independently reviewed (i.e., by reviewers who are not in the program) for achievement of cybersecurity program objectives
	l. The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives
3. Establish and Maintain Cybersecurity Architecture	
4. Perform Secure Software Development	
MIL3	b. Policies require that software that is to be deployed on assets that are important to the delivery of the function be developed using secure software development practices
5. Management Activities	
MIL2	a. Documented practices are followed for cybersecurity program management activities
	b. Stakeholders for cybersecurity program management activities are identified and involved
	c. Standards and/or guidelines have been identified to inform cybersecurity program management activities
MIL3	e. Cybersecurity program management activities are periodically reviewed to ensure conformance with policy
	f. Personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities (Note: allocated at the tier level)

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002003333

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com