Chapter 14
Governance and Assessment Strategies for Industrial Control Systems

Daryl Haegley

14.1 Introduction

In spite of decision support technologies, such as experimentation and simulation discussed in the previous chapter, it remains challenging for ICS stakeholders (leaders, managers, operators, etc.) to make informed decisions regarding formulating guidance, assigning responsibilities, balancing security and efficiency, allocating funding, determining return on investment, and measuring performance. Formulating and establishing an overarching plan that supports and guides such decisions is often called governance. This is the subject of the present chapter.

While definitions of governance vary, some of such definitions are better suited to ICS. This chapter will discuss them in detail, but generally governance refers to processes of interaction and decision-making among the actors who are collectively solve the problem such as ensuring and maintaining security of an ICS. Governance includes actions and processes that engender and support stable practices and organizations. In the context of ICS, such processes ensure that benefits of ICS are delivered in a well controlled and are aligned with long-term goals and success of the enterprise.

Governance processes are reflected in, and guided by appropriate documents. The totality of such governance documents can be classified into four types: policies, standards, guidelines and procedures. Policies are the highest level of written governing documents that outline which standards, guidelines and procedures the organization is to follow. Standards offer a frame of reference for compliance and performance. Guidelines are typically not a mandatory governing document, but

D. Haegley (✉)
Department of Defense of the United States
e-mail: dhaegley@gmail.com

E.J.M. Colbert, A. Kott (eds.), *Cyber-security of SCADA and Other Industrial Control Systems*, Advances in Information Security 66,
DOI 10.1007/978-3-319-32125-7_14

rather are designed to be dynamic and flexible, updated to reflect relevant processes and adapt best practices and changes to the organizational situation. Finally, procedures represent a step-by-step process to achieve a specified result.

There are multiple benefits to establishing governance processes and the corresponding documents. They specify which organizational components are responsible for procurement, sustainment, and technical refresh of an ICS. They stipulate authorization roles, risk management process and performance accountability. They also standardize process and metrics for conducting security assessments.

This chapter begins with an illustrative story, inspired by real-life experiences of the author, that help the reader to appreciate some of the practical reasons for good governance of ICS. Then the chapter describes the definitions, purposes and sources of governance. Because governance is particularly important for the purposes of ICS security assessments, the chapter continues by focusing on frameworks and methodologies that govern ICS assessments.

14.2 Overview

14.2.1 A Motivating Story

On a not particularly noteworthy day, my boss approached and directed, "investigate why those information technology (IT) folks wont' approve thousands of smart meters recently purchased by the facility engineers to run on the network" (Smart meters are electronic devices that records energy consumption and enable two-way communication between the meter and a central system [Wikipedia]). At the time it did not seem there should be any issues—aren't all networked devices the same? Is the value of the investment to secure the smart meters greater than the risk not to secure them? What technical issues could the IT folks possibly have?

If there was an obvious concern regarding the smart meters, why didn't the facility engineers coordinate with the IT team in deciding which smart meters to purchase? There are a couple reasons why. First, the facility engineers have been managing their networks for decades. Typically they were not interconnected to an enterprise network or the Internet. There were several decentralized or independent facility–related networked systems that were managed by manually observing analog gauges. Some were electronically connected and centrally managed within the building containing the ICS.

Many of these ICSs did not connect to the Internet, although some did. There are instances where a vendor may have established a connection to verify ICS performance and warranty conditions or to install upgrades or patches. But even under these circumstances, the IT department was not informed or integrated into network purchasing decisions. Since it was not part of the email network, why would it be considered IT? The IT SMEs were not consulted for most all ICS network decisions, hardware, software, governance, security procedures, training, etc.

The facility or civil works budget for their network and any corresponding security controls would stand independently and compete among all other resource requests. If ICS networks were considered part of the IT department's purview, then the IT budget, which is often under budgeted according to the IT SMEs, would have even more competing hardware and software security requirements. Now, as the ICS networks are being exploited due to a lack of integrated security, there is an increased need for the IT and engineering communities and departments to collaborate and cooperate in performance, risk, security, resourcing and procurement discussions and decisions. Those conversations and partnering are critical to justify an ICS for authorization to operate or establish proof of net-worthiness on the corporate network or via the Internet.

If worrying about a smart meter being exploited was not on the organization's radar, then chances are that other exploitable devices connected to controls system are not either. For example, in December 2011, the Chamber of Commerce discovered that one of their digital thermostats was configured to communicate back to a location in China. [http://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642] While technically intriguing, it brings to bear a fundamental question: who in your organization would be responsible for monitoring and cybersecuring controls systems networks and devices? Subsequent questions follow: Would the IT folks know the thermostat is able to connect to the Internet? Would the facility engineers know? Would the IT folks be trained in control systems? How about the facility engineers, would they recognize a fault from a cyber source? What are the governing documents that outline how this should be handled? How have those governing documents demonstrated reasonable measures to ensure the organization's intellectual capital (and the shareholders) were adequately protected?

Although hope and luck can be integral for short-term success, long-term success requires a more structured approach. That begs the question: Where to start? In increasingly connected environments, it can be extremely challenging for executives, leaders, managers, operators to make informed decisions regarding formulating guidance, assigning responsibilities, balancing security and efficiency, allocating funding, determining return on investment, and measuring performance.

Overwhelmingly significant emphasis on interconnectedness and associated security concerns has been evident in the IT community over the past decade; the same concern has recently gathered momentum regarding ICS. Despite the prolific, continuous threats and concerns emanating from every direction, the interconnected benefits and efficiencies gained continue to inspire thoughts of opportunities and growth. A daunting task, specific exploitation risk to ICS was extremely difficult to calculate and seemed impossibly rare to occur on "my network," hopefully exploitation would occur on "someone else's network." Therefore many refrained from implementing security in ICS environments.

But exactly where to start? Westby (2003) offers that in increasingly connected environments, it can be extremely challenging for stakeholders (leaders, managers, operators etc.) to make informed decisions regarding formulating guidance, assigning responsibilities, balancing security and efficiency, allocating funding, determining return on investment, and measuring performance. What should be included in formulating an overarching plan for those interconnected or isolated environments? Many refer to establishing such a plan as "governance."

14.2.2 Some Definitions

Enter "governance." In the Wikipedia entry of governance, subject matter expert Hufty (2011) provides specific definitions that can be aligned to ICS: "processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions," and "…governance is a theoretical concept referring to the actions and processes by which stable practices and organizations arise and persist. These actions and processes may operate in formal and informal organizations of any size; and they may function for any purpose."

In the context of IT and ICS, Howe (2009) describes governance referring to "the structure, oversight and management processes which ensure the delivery of the expected benefits of IT in a controlled way to help enhance the long term sustainable success of the enterprise." Those processes yield a simple governance construct that can be applied within organizations. The construct may be divided into the following four subcomponents: policies, standards, guidelines and procedures. This construct is especially useful for those in large or geographically separated organizations:.

Policies are regarded as the highest level of written governing document, outlining which standards, guidelines and procedures to follow. Effective polices must be realistic, identify achievable goals, and focus on elements. Alternately, they may comprise a number of related standards, guidelines and procedures. Policies should receive input from all aspects of the organization with the key stakeholders having the most influence. They can broadly or specifically reflect leadership direction, goals, objectives or mission, leaving execution details to the referenced documents. With few exceptions, these overarching documents routinely apply to all employees and supporting contractors; non-adherence consequences should be clearly articulated to include specified disciplinary action.

Standards offer a frame of reference for compliance and performance. They can span an entire range of options, from minimal to maximum, as well as local, national and international. Often aligned to a statutory law or consequence, the organization determines the most appropriate that apply. Additionally, within an organization there may be different requirements or tolerances and different standards or exceptions that should be detailed, approval and documented. For example, the same NIST ICS security control standard could be applied for two systems but there would be fewer security controls necessary for a building escalator compared to the critical infrastructure supporting a data center. Standards are adapted or internally developed to satisfy compliance or respond to industry competition/rivalry, then organizational leadership would select which to "mandate."

Guidelines are routinely developed by those while trying to meet the requirements outlined by the standards within a specific environment or context. Typically not a mandatory governing document, guidelines are designed to be dynamic and flexible, updated to reflect relevant processes and adapt best practices and changes to the organizational situation. As an example relating to baselining the configuration of an ICS, one may generate an organizational specific guide or adapt what's outlined in the NIST Special Publications. The two NIST

special publications offer guidance for controls that can apply to ICS: NIST SP 800–53 "Recommended Security Controls for Federal Information Systems and Organizations," and even more specifically, NIST SP 800–82 "Guide to Industrial Control Systems (ICS) Security."

Examining excerpts from each publication in Tables 14.1 and 14.2, the Configuration Management (CM) family provides the following guidance that IT or ICS managers can employ:

As shown, there are multiple options for the ICS owner/operator/manager to choose. Tailoring the guidance to a specific ICS environment is encouraged. The most important aspect is to document the guidance and obtain leadership approval.

Table 14.1 Excerpt from NIST SP 800–53 CM-2 baseline configuration

	NIST SP 800–53 CM-2 baseline configuration (p. F-64)
Control	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system
Supplemental guidance	This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture
Related controls	CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7
Control enhancements	(2) *Baseline configuration|automation support for accuracy/currency*
	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system
Supplemental guidance	Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities
Related controls	CM-7, RA-5

Table 14.2 Excerpt from NIST SP 800–53 CM-2 Baseline Configuration

	NIST SP 800–82 CM-2 Baseline Configuration (p. G-27)
Control enhancements	(1) *Baseline configuration|reviews and updates*
	The organization reviews and updates the baseline configuration of the information system:
	(a) [Assignment: organization-defined frequency];
	(b) When required due to [Assignment organization-defined circumstances]; and
	(c) As an integral part of information system component installations and upgrades
Related control	CM-5
Control enhancements	(2) *Baseline configuration|automation support for accuracy/currency*
	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system
Supplemental guidance	Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities
Related control	CM-7, RA-5

Procedures represent a step-by-step process to complete a specified result. Each step should be clearly articulated, simple to follow even when the subject matter expert is not available. A simple example procedure is “press red button when centrifuge is exceeding operating tolerance of 5000 to 7500 RPM.” In the configuration example above, procedures would be the “how” outlined for each tool, control and device in the proper order of sequence and or precedence.

In an example guidance, a policy may require all networks to be secured. The referenced standards would list which security controls could apply to the different types of networks (e-mail, cell phone, control systems, wired and wireless, etc.). Guidance documents could identify applicable processes, best practices and lessons learned when applying the security controls to each network type. Procedures could outline the individual steps required in each particular process to implement individual security controls.

- Policy: Secure control system network
- Standard: Routinely change administrator level passwords
- Guidance: Change passwords every 90 days consisting of a minimum of 16 characters, upper/lower case, including special characters

- Procedure: Send email reminder on 15th of each month to change passwords; verify status of changes by logging in to terminal named "Skyrunner," folder located x://ICS polices/monthly reminders; document compliance; lockout/disconnect those non-compliant

If there is no procedure for verifying changing passwords, or if that procedure is not followed properly, then the best practice guidance is not implemented, standards are not followed, and the network may not be secure.

14.2.3 Purpose of Governance

Setting the tone from the top is a critical enabler for the success of ICS security. One must publish policies that promote compliance and performance, incorporate relevant standards, and generate guidelines to facilitate consistent application of procedures. It is critically important to outline the specific expectation as well as the consequences of not adhering to policy. If it cannot be clearly demonstrated that the appropriate standards are in compliance, the ICS may be deemed exploitable and lose its accreditation or permission to operate on the corporate network.

A common concern with ICS stakeholders is the resourcing decisions to secure IT-related or automated assets in another part of the organization. As reflected by Allen (2005), "Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. To achieve a sustainable capability, organizations must make the protection and security of digital assets the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance."

Tangible benefits to establishing governing documents include:

- Specify organizational resource responsibility for procurement, sustainment, and technical refresh
- Stipulate authorization roles, risk management process and performance accountability
- Provide compliance evidence to regulators, shareholders, insurers, etc.
- Enable continuity of operations despite unpredictable environments and skilled personnel turnover
- Justify certificate of net-worthiness/authority to operate
- Standardize process and metrics for conducting security assessments

14.2.4 Groups Issuing ICS Governance

Various global entities have written many relevant standard documents for assisting with risk management and cybersecurity within ICS environments. Fabro (2012, p. 125) relays a simple, overarching purpose, "Understanding these standards will allow asset

owners to create and manage a program to mitigate cyber security risks in their control systems environments. When an asset owner is without formal direction to adhere to a certain security standard or practice, these standards allow for great flexibility to accommodate for the unique challenges presented by control system environments."

Below is a list of the organizations routinely developing authoritative and internationally recognized standards and specific ICS guidance (not all inclusive, see Table 14.3 for more details):

- IEC—International Electrotechnical Commission
- IET—Institution of Engineering and Technology
- ISA—International Standards of Automation
- ISO—International Organization for Standardization
- NIST—National Institute of Standards and Technology
- NRC—Nuclear Regulatory Commission
- U.S. DoD—Department of Defense

14.2.5 ICS Assessments

Unless specifically dictated, the standards listed above can be used as prescribed or modified to apply to unique ICS environments. While no ICS configuration may be exactly the same, the standards can be applied consistently across an enterprise of multiple assets, systems and or networks. Even if the ICS configuration fully complies with all the regulations, standards, guidelines, etc., disruption, exploitation and manipulation may occur. Targeted by undeniably persistent and complex vectors of cyber threats, ICS owners and operators must endeavor to remain proactively vigilant in their security perspective. Therefore, it is critically important to conduct routine evaluations to ascertain operational and security performance.

The assessment process is essential. Among all the governing documents within an organization, assessments are the most powerful for enabling resource decisions, revealing vulnerabilities, and making security modifications. Assessments are applied at the design, construction and completion phases. They establish the baseline and consider modifications when they occur. When regular assessments are completed the organization understands the precise ICS hardware and software configuration. When all is operating well, assessments verify system communications are all according to expectations and plans. On the other hand, assessments can reveal existence of unexpected communications illuminating the extent of malware or exploitation, and/or the lack of updates, patches, and adherence to best security practices.

Despite assessment benefits, due to a general lack of oversight from an IT security context, many ICS assessments were never conducted and, consequently, security was not integrated into the design. When assessments do occur, the following are common negative findings:

- Existence of undocumented network connections (wired and wireless)
- Presence of known or unknown connection to Internet or vendor (for maintenance/warranty)

Table 14.3 List of many standards and guidance documents applicable to ICS (not all inclusive)

IET *Institution of Engineering and Technology*	Code of practice for cyber security in the built environment	Describes cyber security options to consider throughout a building's lifecycle and offers community best practices when integrating building related systems with enterprise cyber environment
ISA 99/IEC 62443 *International Society of Automation/International Electrotechnical Commission*	Industrial automation and control systems (IACS) security	Procedures for implementing electronically secure IACS and security practices and assessing electronic security performance
ISO/IEC 15408 *International Organization for Standardization/International Electrotechnical Commission*	Common criteria for information technology security evaluation; usually referred as simply "Common Criteria"	Established to facilitate a unified set of pre-existing standards enabling mutually agreed evaluation reference for vendors, testing laboratories and government customers combined by Canada, France, Germany, the Netherlands, the UK, and the U.S. governmental organizations
ISO/IEC 27001:2015	Information technology—Information security management systems—Requirements	Specifies requirements for establishing, implementing, maintaining and continually improving an organization's information security management system; requirements for assessment and treatment of information security risks tailored to the needs of the organization
ISO/IEC 27002:2013	Information technology—Security Techniques—Code of practice for information security controls	Designed for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as guidance for implementing commonly accepted information security controls; facilitates consideration of specific information security risk environment(s)
ISO/IEC 27003:2010	Information technology—Security techniques—Information security management system implementation guidance	Describes the process of ISMS specification and design from inception to the production of implementation plans
ISO/IEC 27004:2009	Information technology—Security techniques—Information security management—Measurement	Provides guidance on development and use of measures and measurement in order to assess effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001
ISO/IEC 27005:2011	Information technology—Security techniques—Information security risk management	Relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities

(continued)

Table 14.3 (continued)

ISO 31000:2009 *International Organization for Standardization*	Risk management—Principles and guidelines	Establishes a number of principles to enable effective risk management; can be applied to an entire organization, its sub-components, at any time, as well as to specific functions, projects and activities
ISO 50001:2011	Energy management	Outlines how organizations can apply energy management techniques resulting in improved quality and environmental management
NIST SP 39 *National Institute of Science and Technology (NIST)*	Managing information security risk	Organization, Mission, and Information System View; provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems
NIST SP 800–53 revision 4	Recommended security controls for federal information systems and organizations	Provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations
NIST SP 800–82 revision 2	Guide to industrial control systems (ICS) security	Provides an overview of the differences between ICS and transitional IT, typical ICS topologies, threats, vulnerabilities, and mitigation controls
NIST SP 160 DRAFT	Systems security engineering: An integrated approach to building trustworthy resilient systems	Provides recommend steps to help develop a more defensible and survivable IT infrastructure—including the component products, systems, and services that compose the infrastructure
NRC 5.71 *Nuclear Regulatory Commission*	Cyber security programs for nuclear facilities	Regulatory guide that identifies cyber-security program implementation procedures for U.S. nuclear facilities
U.S DoDI 8500.01 *United Stated Department of Defense Instruction*	Cybersecurity	Implements a multi-tiered cybersecurity risk management process
U.S. DoDI 8510.01	Risk management framework (RMF) for DoD information technology (IT)	Establishes using an integrated enterprise-wide decision structure for cybersecurity risk management

- Incorrect configurations (modified from initial installation or adapted to customer environment)
- Incomplete patches and upgrades (HW/SW)
- Non-secure configuration
- Owners/operators not familiar with configuration, appropriate cyber/security practices

14.3 Examples of ICS Assessment Processes

One significant concern is that with many ICSs, taking the system off-line for software upgrades or patches may have operational impacts. For example, if the HVAC system were to come offline, the server room temperature may increase to the point where computers overheat and shut down. In another example, applying a patch to a critical life-support medical device during an operation may cause it to fail. If clear governance exists, all system operators and network administrators would cooperate on specific procedures, would routinely review the systems and devices using network communications, and would work together on implementing upgrades and patches. This would reduce the risk of avoiding lapse in normal operations or initiating catastrophic results.

There exist several documented processes to complete ICS security assessments. They can be performed independently or in concert with the IT assessments. The following list is not comprehensive but reveals varying approaches with underlying common themes. Inclusion does not represent or imply endorsement of any commercial product or government process. A brief overview is provided with the recommendation to further investigate these and others to determine the most relevant, repeatable assessment process for your organization.

1. NIST Cyber security framework
2. Department of Energy (DoE) & DHS Cyber Capability Maturity Model (C2M2)
3. Robust ICS Planning & Evaluation (RIPE) Framework
4. DHS ICS Cyber Emergency Response Team (CERT) Cyber Security Evaluation Tool (CSET)

In the next four subsections, we describe aspects of these assessment processes in more detail.

14.3.1 NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NCF) is a “risk-based” methodology for managing cybersecurity risk, consisting of: Framework Core, Framework Implementation Tiers, and Framework Profiles (http://www.nist.gov/cyberframework/). Each Framework component emphasizes interactions among business drivers and cybersecurity activities.

The NCF systematic process can be used to establish a new cybersecurity program or advance an existing one. Working through each step, the organization can evaluate current capabilities and gaps to attain desired performance. Essentially the NCF (2014, p. 15) can provide "a roadmap to improvement" and ability to "prioritize expenditures to maximize the impact of the investment."

The Framework Core in the NCF (2014, p. 6) is designed to enable "communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level." In Fig. 14.1, there are five functions on the left side: Identify, Protect, Detect, Respond, and Recover; and four elements across the top: Functions, Categories, Subcategories, and Informative References. The Core (p. 6) is not a simple task-list, it "provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk."

The NCF (2014, p. 7) describes Framework Implementation Tiers ("Tiers") to facilitate self-evaluation of cybersecurity risk and associated processes. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4)." When selecting the appropriate Tier, "an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints."

Further, the NCF (2014, p. 7) specifies the next level, Framework Profile. "*Framework Profile ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations*."

Figure 14.2 provides the next stage in establishing a relevant framenwork template, an organization may include additional "Category" and "Category Unique Identier" to optimally align with the functions.

As the example depicts, it may appear the "intended outcomes" listed in the Functions, Categories, and Subcategories are similar for IT and ICS. However, the operational environments and considerations for IT and ICS differ. The NCF (2014,

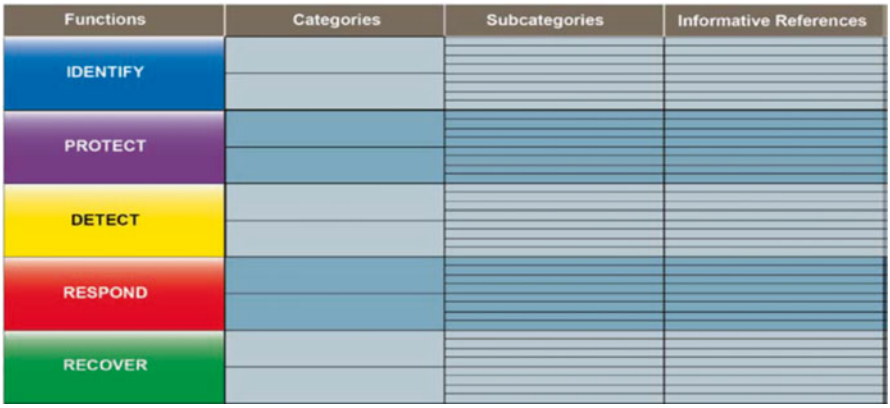

Fig. 14.1 NCF core elements

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

Fig. 14.2 Example of NCF functions, category unique identifier and category

p. 20) surmises "ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures."

The NCF prescribes separate representative "Profiles" and a separate characterize of an organization's practices or "Tiers." Below is an adoption of all the concepts into one table. It includes only one example for each Function, Category and Subcategory, and integrates the Tier evaluation under a "current" Profile measured against attaining the task outlined in the subcategory column. This is not precisely prescribed by the Framework but offers a means to view all the concepts integrated together. As noted in the NCF, the Tiers are not "maturity levels" and an organization may decide not to invest in resources to progress from a lower Tier to a higher one. Leadership may decide to assume a level of risk commensurate with one or more Tiers.

The NCF provides a template along five functional areas common to IT and ICS: Identify, Protect, Detect, Respond, Recover (see Fig. 14.3). It aligns informative references overarching view of current cybersecurity practice, but it does not identify which specific security controls should be in place to protect ICS networks. It certainly emphasizes collaboration and cooperation among and across all lines of business/operations within an organization to determine the appropriate categories for evaluation. On its own, however, generating a "current state profile" and "to-be state profile" it will not serve as a justification for authorization to operate on the corporate network or proof of net-worthiness. It will undoubtedly serve as another management resource investment decision aid and/or capability oversight tool.

Profile:		Attain by June 20XX	Current	
Function	**Category**	**Subcategory**	**Implementation Tiers**	**Informative References**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**Tier 1: Partial**	· **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
PROTECT (PR)	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**Tier 4: Adaptive**	· **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
DETECT (DE)	**Anomalies and Events (DE.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	**Tier 3: Repeatable**	· **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
RESPOND (RS)	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.RP-1:** Response plan is executed during or after an event	**Tier 2: Risk Informed**	· **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
RECOVER (RC)	**Recovery Planning (RC.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	**Tier 2: Risk Informed**	· **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

Fig. 14.3 Integration of all NCF concepts into single table

14.3.2 Department of Energy (DoE) and DHS Cyber Capability Maturity Model (C2M2)

The C2M2 evaluation can enable organizations to assess and bolster their cybersecurity program, prioritize cybersecurity actions and investments, and maintain the desired level of security throughout the IT systems life cycle (http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity). Stemming from a diverse set of cybersecurity standards, frameworks, programs, and initiatives, it outlines implementable steps applicable to almost any organization (see Fig. 14.4).

The DoE (2014, p. 1) claims the resulting scores from the C2MC model can reflect the "implementation and management of cybersecurity practices" integrating traditional information technology systems and ICSs, as well as the overall security culture of the organization:

- Strengthen organizations' cybersecurity capabilities
- Enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities

	Inputs	Activities	Outputs
Perform Evaluation	1. ES-C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct ES-C2M2 Self-Evaluation Workshop with appropriate attendees	ES-C2M2 Self-Evaluation Report
Analyze Identified Gaps	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

Fig. 14.4 Table illustrating how the C2M2 can contribute to an overall prioritized implementation plan (2014, p. 19)

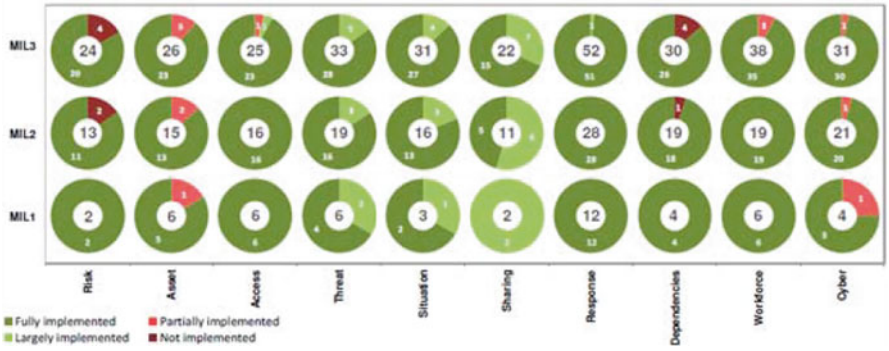

Fig. 14.5 Sample summary scores after completing the C2M2 questions (2014, p. 15)

- Share knowledge, best practices, and relevant references across organizations as a means to improve cybersecurity capabilities
- Enable organizations to prioritize actions and investments to improve cybersecurity

Within the C2M2, there exist ten domains comprised of cybersecurity practices, corresponding objectives, and practices identified by Maturity Indicator Levels (MIL). See Fig. 14.5 for a sample score result. The C2M2 Self Evaluation Toolkit (excel spreadsheet) contains over 600 questions which are graded at a four-point scale using: Fully Implemented (FI), Largely Implemented (LI), Partially Implemented (PI), and Not Implemented (NI).

The process is fairly simple to repeat as "plans are implemented, business objectives change, and the risk environment evolves" (DOE (2014, p.15). The DoE defines two energy sector specific models: Electricity Subsector C2M2 (ES-C2M2) and Oil and Natural Gas Subsector C2M2 (ONG-C2M2).

While the C2MC provides an overarching view of current cybersecurity practice, it does not identify which specific security controls should be in place to protect ICS networks. It does reiterate the need for collaboration and cooperation among and across all aspects of business/operations within an organization to determine the appropriate practices, objectives and corresponding MILs. As a stand-alone product however, it will not serve as a justification for authorization to operate on the corporate network or proof of net-worthiness. It does serve as a resource investment and capability oversight tool.

14.3.3 Robust ICS Planning & Evaluation (RIPE) Framework

Mr. Ralph Langner, founder and director of Langner Communications GmbH, the cyber-security consulting firm focused on ICS security, has developed the Robust ICS Planning & Evaluation (RIPE) Framework (http://www.langner.com/en/solutions/).

The specific details are proprietary information, but some insightful information is publically available from a whitepaper accessible on the company's website (see Tables 14.4 and 14.5). Langer (2013, p. 1) explains that RIPE consists of evaluating "eight different domains, establishing benchmarks and scorecards enabling measurable cyber security capability and identifying weak spots. Such a framework-based approach to ICS security provides economies of scale that can result in significantly improved efficiency compared to risk management exercises that approach every single plant as a completely unique universe."

Unlike the other assessment processes described in this chapter, RIPE requires that an organization purchase RIPE materials to ascertain its cyber security effectiveness

Table 14.4 Captures the whitepaper attributes used to measure cybersecurity capability and indicates these can be routinely "blurred" (2013, p. 4)

Attribute	System properties (Think: Sensors)	Procedural guidance (Think: Actuators)
Verifiability	Documentation on system properties is verifiable by walk-down inspection or experiment	Conformity to procedural guidance documents is verifiable by audit
	Blur example: System documentation claims that a component (such as a PLC, or software application) is "secure" without detailing why and how	Loss example: Security policies that contain language such as "as soon as possible" or "as appropriate", resulting in unpredictable execution that cannot be audited
Completeness	System architecture models are complete, verified by walk-down inspection or experiment	Written procedural execution items (policies, SOPs, guidelines) are provided for all procedures that otherwise leave room for variation that could affect the cyber security posture
	Blur example: Systems used on the plant floor (including mobile devices), or software applications running on computers, are not listed in the system inventory	Loss example: Security policies are produced and enforced for employees, but not for contractors
Accuracy/compliance	Walk-down inspection or experiment verify that documentation of system properties is accurate	Audits verify that procedure execution is compliant with written policy
	Blur example: A system is configured differently than documented, for example in respect to network connectivity, software version, security patch level etc.	Loss example: Mobile devices are configured or used in a manner that violates policy; backups are not performed according to policy; network segregation (firewall rules) is not configured according to policy

Table 14.5 Reveals an example of how the performance characteristics would be measured (2013, p. 7)

RIPE system	*Inventory quality*
SI quality	Completeness and accuracy of the system inventory
	Computation: SI Accuracy * SI Completeness/100
SI completeness	Percentage of components listed in the system inventory based on total number of components as identified by walk-down inspection
SI accuracy	Percentage of components listed accurately in the system inventory as identified by walk-down inspection
RIPE system	*Procurement quality*
SP quality	Completeness of system procurement guideline application and compliance of acquired systems
	Computation: SP Completeness * SP Compliance/100
SP completeness	Percentage of system acquisitions during last audit interval for which system procurement guidelines have been applied
SP compliance	Percentage of system acquisitions during last audit interval for which systems proved to be compliant with system procurement guidelines
RIPE training	*Program quality*
TP quality	Completeness of training program and compliance with training obligations and offerings Computation: TP Completeness * TP Compliance/100
TP completeness	Percentage of user roles relevant for industrial control systems and process IT, including contractors, for which a formal training program beyond awareness is established
TP compliance	Percentage of users, including contractors, eligible or obligated for training actually finishing respective training sessions during the last audit interval

(see http://www.langner.com). One option is to purchase licensed guidelines and templates for an organization and to simply self-populate those guidelines and documents. A much more robust on-site process is also offered, consisting of an audit lasting 30 days, resulting in a RIPE Framework implementation certification.

The RIPE (2013, p. 5–6) focuses on "eight domains of the plant ecosystem" and measures the effectiveness of each as a percentage of the optimal performance:

- System Population Characteristics
- Network Architecture
- Component Interaction
- Workforce Roles and Responsibilities
- Workforce Skills and Competence Development
- Procedural Guidance
- Deliberate Design and configuration Change
- System Acquisition

Once each of the eight domains is scored, the results can be plotted in a spider web diagram as in Fig. 14.6, which is a fictitious comparison of the Atlanta and Birmingham plants, clearly revealing differences in performance.

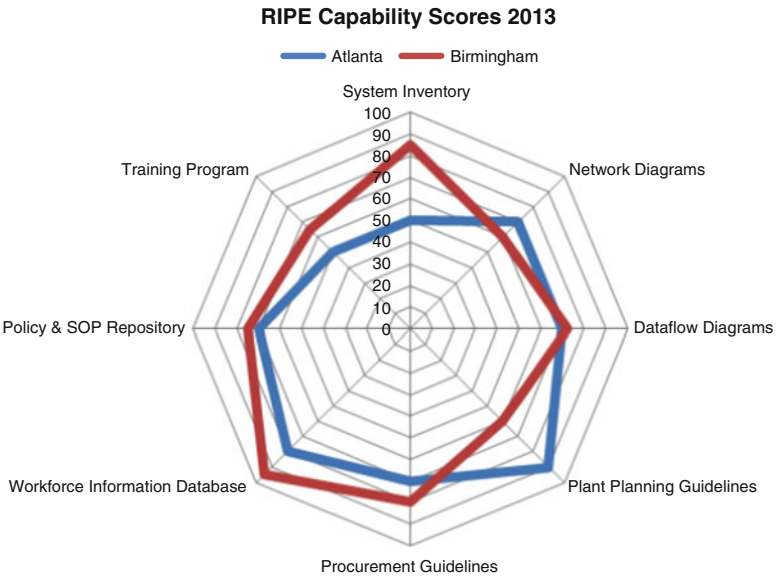

Fig. 14.6 RIPE comparison of the Atlanta and Birmingham plants (2013, p. 7)

As with most assessment processes based on metrics or measures of effectiveness, the results can be used by leadership to make logical, non-subjective risked-based investment decisions. Per the whitepaper (2013, p. 10), "Based on the RIPE Framework documentation, it is also feasible to determine which security controls yield the best mitigation for the cost—if implemented properly (as specified in mitigation advice). Mitigation advice will usually involve multiple security domains."

However, a common problem seen in many organizations is a lack of insight to the actual problems and relevant mitigating solutions. Moreover, even after a solution is purchased, it is critical to ensure the controls are implemented properly. For example, everyone has a lock on their front door to keep out intruders but sometimes the lock is not engaged. Within the context of cybersecurity, Mr. Langer (2013, p. 9) notes "It is discouraging to see how many asset owners (from management down to control system engineers) are satisfied with the idea to "have addressed the problem" of ICS insecurity by having invested in firewalls, anti-virus solutions, security patching regimes etc. without ever bothering to check their effectiveness."

The RIPE Framework can provide an overarching view of current cybersecurity practices, risk management tolerance and measures of effectiveness of eight domains common to plant operations. Once a product license is procured, independently or with the RIPE team, a holistic view based on performance metrics can be implemented to protect ICS networks. It reinforces the need for an understanding across all aspects of business/operations within an organization. It may

provide relevant artifacts to help justify authorization to operate on the corporate network or proof of net-worthiness. However, the specifics are not detailed in the whitepaper. Similarly to the other methodologies, it can serve as a resource investment and capability oversight tool.

14.3.4 DHS ICS Cyber Emergency Response Team (CERT) Cyber Security Evaluation Tool (CSET)

The Department of Homeland Security (DHS) National Cyber Security Division (NCSD) developed CSET for control systems asset owners (https://ics-cert.us-cert.gov/Assessments). Their primary objective was to assist organizations identified as parts of nation's critical infrastructure and reduce their cyber risk. However, since its initial release in August of 2009, it has become a useful tool suitable for almost all systems that control a physical process, from expansive power utilities, sewage treatment plants, to manufacturing plants, logistical or medical facilities as well as individual buildings. The most recent CSET version as of this chapter's printing is 7.0, released in August, 2015.

CSET (2015, p. 15) can be basically described as "CSET implements a simple, transparent process that can be used effectively by all sectors to perform an evaluation of any network." One can order a free CD or download the file directly from the DHS ICS CERT website. The software tool includes a step-by-step guide to assist user's enter their organizational-specific control system information (hardware, software, administrative policies, etc.) into predefined parameters based on relevant security standards and regulations (see Figs. 14.7 and 14.8):

Fig. 14.7 CSET Step 1—select relevant assessment mode (2015, p. 44)

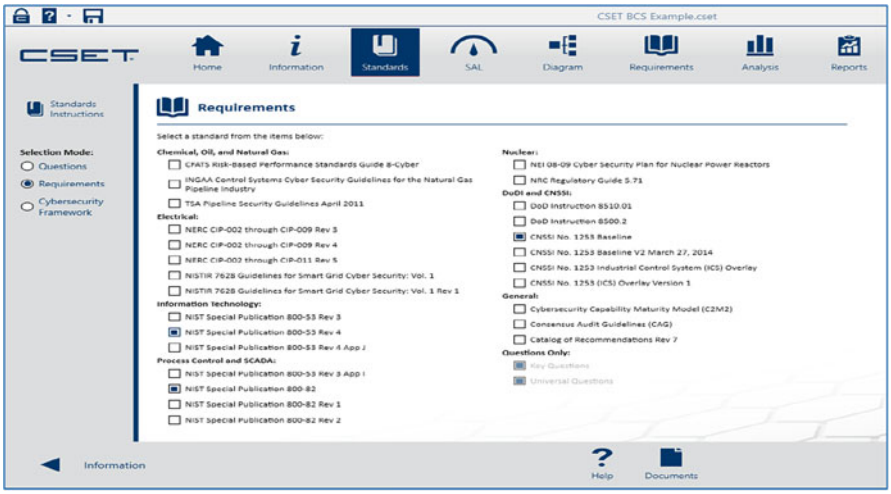

Fig. 14.8 From selected standards stem appropriate questions in CSET (2015, p.47)

- NIST Cybersecurity Framework
- NIST SPs: 800–39; 800–53 Rev 4; 800–82 Rev 2
- NISTR 7628
- NERC CIP
- ISA 99/IEC 62443
- ISO/IEC 15408; 27001—27005
- ISO 31000 and ISO 50001
- NRC 5.71
- U.S. DoDI 8500.01 and 8510.01
- Others

As with the other assessment methodologies listed in this chapter, CSET should be completed by a cross-functional team consisting of subject matter experts spanning administrative, business, information technology, maintenance, operational and security functional areas. There are hundreds of questions to be answered and while the software is simple to install and use, the breadth and depth of answers required to effectively respond to the questions necessitates knowledgeable and proficient personnel. Those personnel will be routinely located in various parts of the organization. Answering the series of diverse and technical questions is a forcing function to bring them together, potentially enabling unprecedented collaboration among entities that seldom otherwise communicate, if at all.

CSET assessments (see Fig. 14.9) cannot be successfully completed by any one individual as no single person maintains sufficient enterprise knowledge to provide effectual responses to all of the questions. To be truly effective and efficient, completing a CSET (2015, p. 20) assessment requires a cross-functional team consisting of representatives from the following areas:

Fig. 14.9 CSET depiction of general security assessment level (SAL) (2015, p. 70)

- ICSs (knowledge of ICS architecture and operations),
- System Configuration (knowledge of systems management),
- System Operations (knowledge of system operation),
- Information Technology (IT) Network/Topology (knowledge of IT infrastructure),
- IT Security/Control System Security (knowledge of policies, procedures, and technical implementation),
- Risk Management (knowledge of the organization's risk management processes and procedures),
- Business (knowledge of budgetary issues and insurance postures), and
- Management (a senior executive sponsor/decision maker).

Conveniently, CSET can generate the System Security Plan and the Artifacts; adding the Security Assessment Report (SAR), CONOPS, and Incident Response Plan provides an organization with the basic analysis to understand the risks, impacts, and recovery/mitigation options. CSET includes an extensive complement of templates (see Fig. 14.10) to facilitate network, systems and device inventories and diagrams. Since proprietary design and potential vulnerability information will be revealed after completing the assessment, the corresponding reports must be handled appropriately.

CSET is a compliance verification tool rather than a risk or vulnerability assessment tool. Once the assessment is completed, CSET (2015, p. 14) "pulls its recommendations from a database of the best available cybersecurity standards, guidelines, and practices." The resulting reports (see Fig. 14.11) outline specific mitigation actions to obtain full compliance with the selected policies, standards and corresponding security controls and thereby improving the ICS's cybersecurity capability.

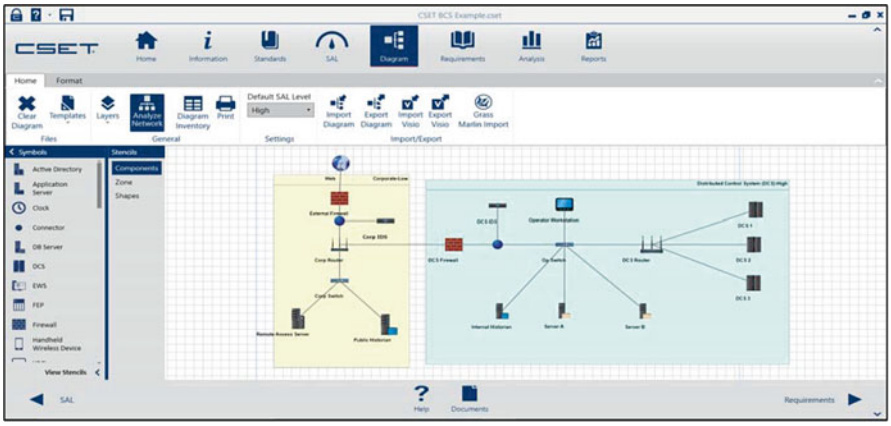

Fig. 14.10 CSET offers many templates to create inventory and network diagrams (2015, p. 111)

Fig. 14.11 Sample final CSET report summary (2015, p. 153)

CSET should be combined with other tools to fully evaluate the security posture. For example, one may use network scanning, penetration testing, and other tests on nonproduction systems that will not adversely impact mission, operations, health or safety.

CSET is a stand-alone software application that enables organizational self-assessment using national and internationally recognized standards. It can integrate ICS community cybersecurity best practices into the organizational corporate risk management strategy. Since its inception, many have posted video tutorials on-line, demonstrating its wide user community. Within CSET is a comprehensive and expansive reference library. If preferred, DHS ICS CERT has an on-site service that can assist with the assessment process. A benefit of CSET is that a system security plan can be exported as an artifact toward justification for authorization to operate

on the corporate network, or proof of net-worthiness. While a CSET "all green" cybersecurity standards compliance evaluation is impressive, as for other assessments, it does not equate to an impenetrable or un-exploitable network.

14.3.5 Overview of Assessment Methodologies

Each assessment approach described is based upon extensive subject matter experience and community best practices. None offer shortcuts or exclusions from their process; the process must be followed in order to obtain an accurate, accountable inventory of all ICS systems, networks and devices. They all recommend that all stakeholders within an organization—especially IT and ICS—work together and systematically conduct self-assessments on the networked assets in order to capture dependencies and interdependencies. The results can inform leadership to help with resource decisions and management task prioritization. It's important to understand not every asset will require robust security controls. Despite many executives stating "securing all these is an impossible task," there are many methodologies available to achieve the security level relevant for a given organization.. When the appropriate people come together and are required to discuss issues related to protecting their assets, they are often able to recognize areas of weakness and the required improvements for their organization.

Improvements are needed in automated identification of assets on an ICS network, its topology, connectedness, adherence to rules/polices/patches, visualization, evaluation of instantaneous performance (and trend analysis) and exploitability based on continuous alerts, intelligence community inputs, 100 % verification of vendor patch authenticity, identification of potential consequences of applying new patch in real-time operational environment versus first applying to test bed. A cyber range or test laboratory can be used for replicating all vendors, all protocols, all levels of updates and patches, as well as automating responses to alerts such as updating and patching. Predictive maintenance and mitigation options incorporating associated expenses would also be very useful. There are tremendous business opportunities in this space. Beyond hardware or software advancements, additional labor and training may need to be considered to complete the job well.

Each methodology can be a catalyst change. Many hesitate to take the first step because security, especially ICS cybersecurity, is unfamiliar territory. It is overwhelming to be faced with reading through the totality of hundreds of security questions to answer in the standards documents. However, if one takes on the challenge one step at a time and embraces the opportunity to safeguard the organization, catastrophes can be avoided. There are a vast number of free resources. One will need to dedicate resources, time and effort, internally and perhaps engage external expertise. It is imperative that the technical specialists representing IT and ICS collaborate instead of compete. Assessments offer a measurable, repeatable, non-subjective process to make informed security related decisions.

It is prudent to invest in community best practices and conduct regular assessments. Security evaluations and investments are reported directly to the CEO. If a breach

occurs and the media questions company officers or shareholders, one may confirm that an assessment was performed. Quarterly reports include those investment decisions in cybersecurity solutions as a differentiator. As it is commonly said but rarely implemented: Security should be "baked in" from the beginning and not "bolted on" after all the equipment is installed. If you are in the planning and or design phase, then security capability requirements can be applied now.

If the smart meters mentioned in the very beginning of this chapter are already installed but it is not known if they were securely installed, the organization could use the methods from this chapter to create a relevant governance structure and assess current security procedures via structured and repeatable processes. In the process you one may discover that the ICS networks are unknowingly connected to other networks within the organization, presenting significant risks to critical ICS processes. In the Code of Practice for the Cyber Security in the Built Environment, Boyes (2014, p.57) explains "This cascade from the strategy through policy to process and individual procedures is most important as it provides an audible trail that links specific actions and activities to the overall vision of how the cyber-security risks will be managed and mitigated."

14.4 Summary and Conclusions

ICS networks are being exploited due to a lack of integrated security. This motivates a much stronger need for interdepartmental collaboration and cooperation in an organization. Cooperative discussions can optimize system performance and security while minimizing cost and risk. Contributors must manage procurement practices and weigh consequences of other relevant corporate decisions. Although cooperative motivation can be integral for short-term success, long-term success requires a more structured approach.

Security governance is critically important for outlining both the specific expectation of ICS operations, as well as the consequences for not adhering to specified policies. Once asset owners understand the security standards for their organization, they are able to create and manage a program to mitigate cyber security risks. In addition, it is critically important to conduct routine evaluations (assessments) to ascertain operational and security performance. Assessments are applied at the design, construction and completion phases. Among all the governing documents within an organization, assessments are the most powerful for enabling resource decisions, revealing vulnerabilities, and making security modifications.

Four sample methods of ICS security assessments are discussed in detail in this chapter: The NIST Cyber Security Framework (CSF), DoE/DHS Cyber Capability Maturity Model (C2M2), the proprietary Robust ICS Planning and Evaluation (RIPE) framework, and the DHS ICS CERT Cyber Security Evaluation Tool (CSET). Each of these approaches is based upon extensive subject matter experience and community best practices, and each can be used as a starting point for establishing security practices in an organization. A large amount of informational and tutorial documents are available for using these methods.

Although engaging governance and security assessments requires significant investment by the organization, the benefits can far outweigh the costs. Security evaluations and investments are shared directly with organization executives, who are consequently become integrated in the process. Due diligence or corporate responsibility is usually evident if a breach occurs. Documentation of security processes and well-kept security logs can be instrumental for forensics, and for overall process improvement in an organization.

References

Allen, J. (2005). *Governing for enterprise security (CMU/SEI-2005-TN-023)*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Boyes, H. (2014). *Code of practice for cyber security in built environment* (p. 57). London: The Institution of Engineering and Technology.

Department of Energy. (2014). *Cybersecurity Capability Maturity Model (C2M2) Facilitator Guide* (pp. 1, 15, 19). Retrieved from http://energy.gov/sites/prod/files/2014/02/f7/C2M2-FacilitatorGuide-v1-1-Feb2014.pdf.

Department of Homeland Security Industrial Control System Cyber Emergency Response Team. (2015), *Cyber Security Evaluation Tool (CSET), Users Guide* (pp. 14, 15, 20, 44, 47, 70, 111, 173). Retrieved from https://ics-cert.us-cert.gov/Assessments.

Fabro, M. (2012). *Study on cyber security and threat evaluation in SCADA systems* (p. 125). Ontario: Defense Research and Development Canada Centre for Security Science.

Howe, D. (2009), *Information technology governance*. The Free On-line Dictionary of Computing from Dictionary.com website. Retrieved from http://dictionary.reference.com/browse/information_technology_governance.

Hufty, M. (2011). Investigating policy processes: The governance analytical framework (GAF). In U. Wiesmann, H. Hurni, et al. (Eds.), *Research for sustainable development: Foundations, experiences, and perspectives* (pp. 403–424). Bern: Geographica Bernensia. Retrieved from https://en.wikipedia.org/wiki/Governance.

Joint Task Force Transformation Initiative Interagency Working Group. (2013*). Security and privacy controls for federal information systems and organizations*. Gaithersburg, MD: National Institute of Science and Technology, Special Publication 800–53 revision 4, p. F-64. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

Langer, R. (2013), *Robust ICS Planning & Evaluation (RIPE) Framework* (pp. 1, 9). Retrieved from http://www.langner.com/en/solutions/.

National Institute of Science and Technology. (2014), *Cybersecurity framework* (pp. 6, 7, 15, 20). Retrieved from http://www.nist.gov/cyberframework/.

Stouffer, K., Pillitteri, V., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, MD: National Institute of Science and Technology, Special Publication 800–82 revision 2, pp. 2–117, G-27. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

Westby, J.R. (2003). *Information security governance: Toward a framework for action business software alliance*. Retrieved from http://www.bsa.org/country/Research%20and%20Statistics/~/media/BD05BC8FF0F04CBD9D76460B4BED0E67.ashx.