

Chapter 2

Cybersecurity Terminology and Frameworks

Richard D. Alexander and Srinivas Panguluri

Abstract The documents related to cybersecurity are often filled with information technology (IT) acronyms and with familiar business terms that need to be understood in the context of cybersecurity. In order to develop and implement an effective cybersecurity program, it is necessary to understand the terminology and its contextual use. Cybersecurity programs often evolve within an organization and, depending on the history of that evolution, the implemented measures may be somewhat unbalanced. For example, in some organizations the program may be headed by an IT professional who has exceptional IT skills, so she or he may place an emphasis on technical controls such as firewalls and authentication measures and the resulting program may not have enough administrative controls in place. Any organization can improve their cybersecurity posture by taking a balanced approach. A balance can be reached by utilizing a framework that allows a cybersecurity program to document its programmatic strengths and weaknesses thus hopefully achieving a better balance over time. This chapter defines key cybersecurity terminology and discusses three popular standards/frameworks that are very relevant to cybersecurity in the critical infrastructure sector. Specifically, the information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the ISO/IEC 27000 series is discussed, followed by a summary of the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Critical Infrastructure and the NIST Special Publication 800-82—A Guide to Industrial Control Systems (ICS) Security, both of which have direct relevance to many of the various critical infrastructure sectors in the U.S.

R.D. Alexander (✉)

Interlynx Group LLC, PO Box 36167, Cincinnati, OH 45236, USA

e-mail: Richard.Alexander@interlynx.org

S. Panguluri

CB&I Federal Services LLC, 5050 Section Avenue, Cincinnati, OH 45212, USA

e-mail: Srinivas.Panguluri@cbifederalservices.com

Acronyms

ABAC	Attribute based access control
AES	Advanced Encryption Standard
CIA	Confidentiality, integrity and availability
CRC	Cyclic redundancy checks
CSD	Computer security division
CSRC	Computer Security Resource Center
DCS	Distributed control systems
DNS	Domain name system
DMZ	De-militarized zone
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD-7	Homeland Security Presidential Directive 7
ICS	Industrial control systems
IDS	Intrusion detection system
IDPS	Intrusion detection and prevention systems
IEDs	Intelligent electronic devices
IEC	International Electrotechnical Commission
IP	Internet protocol
IPSec	Internet Protocol security
ISO	International Organization for Standardization
ISMS	Information Security management systems
IT	Information Technology
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NISTIRs	NIST Interagency or Internal Reports
PII	Personally identifiable information
PIV	Personal identity verification
PLC	Programmable logic controllers
RAID	Redundant array of independent disks
SCADA	Supervisory control and data acquisition
SP	Special publication
U.S.	United States
WLANs	Wireless Local Area Networks

2.1 Introduction

The challenges involved in improving an organization's security posture can at times seem overwhelming. Thankfully, there are resources available which ensure that it is not necessary to start with an entirely blank sheet of paper. By leveraging a

selection of existing resources, an organization can avoid “reinvention of the wheel” and accelerate progress towards an improved security posture.

In this chapter, we examine a number of published standards and framework resources which are available to organizations. We consider a number of sources from the widely applicable ISO 27001 (ISO/IEC 2013b) standard whose various versions have spanned over a decade through to the more recent NIST “Framework for Improving Critical Infrastructure Cybersecurity” published in February 2014, (NIST 2014) and Revision 2 of the NIST 800-82 standard “Guide to Industrial Control Systems Security” published in May 2015 (NIST 2015).

We provide an overview of what is covered by each resource, how they inter-relate and consider how an organization can use these resources to accelerate its own understanding of its current security posture. This understanding can be leveraged to chart a course to their desired security posture and by identifying and prioritizing the improvements necessary to achieve that transition. To aid an understanding of all these resources, we first define some of the typical terminology used in the field of cybersecurity.

2.2 Terminology

2.2.1 *Core Terminology*

Before considering the standards themselves, it is useful to review the terminology which (with occasional nuanced variations in emphasis) is common to the standards. Some of the terminologies will be familiar from everyday usage but may take on a more particular meaning in the context of cybersecurity.

2.2.2 *Scope*

The process of improving an organization’s cybersecurity can be considered as a continuous project and, like all projects, to be successful it is necessary to establish the project’s scope. It is not uncommon to find that an organization may not initially have the resources or experience to address a wide cybersecurity scope. In such cases, it may be considered prudent to concentrate initially on those areas where the risks are perceived to be greatest and subsequently widen the scope as resources and experience permit. Note however that it is important to ensure that limited resources do indeed target areas of highest risk, so the process of determining those areas will serve the organization best if it is carried out formally and in a manner which encourages the widespread input of viewpoints.

2.2.3 *Assets*

This term may be familiar from its use in financial contexts. In the context of cybersecurity, the term refers to any organizational information resource that may be subject to cyber-attack and which is therefore in need of protection. The term can cover a wide range of resources such as data resources, software, physical computer systems, networks, utilities, and even less tangible resources such as reputation or community standing.

Critical infrastructure organizations share many of the same information assets as other business types and may also have additional assets specific to their specialty such as process plant, process controls, and associated software.

A common approach to defining the scope of a particular cybersecurity system is to decide which information assets are included and which are excluded. Clearly, in the long run, it is desirable to protect as many assets as is practical and cost-effective. For an organization that is just starting to grapple with cybersecurity, it may be preferable to ensure that an initial project addressing the most risk-critical information assets is successful before widening the scope of the endeavor.

In the context of cyber security, the information assets may have one or more security requirements. The three most common requirements are those typically referred to as confidentiality, integrity, and availability.

2.2.4 *Confidentiality*

Confidentiality of an information asset refers to the asset (or its contents) only being known to those authorized by the asset owner. Examples of information assets to be protected could be proprietary information, customer data, and employee data. For example, confidentiality of stored data might be achieved by implementing encryption of an individual file containing the data, the database, or the entire disk. For example, BitLocker is a full-disk encryption tool built into the Windows operating system.¹ It supports Advanced Encryption Standard (AES) 128-and 256-bit encryption, and it is primarily used for whole-disk encryption. The higher the bit level of encryption, the harder it is to break. Similarly, confidentiality of data can be protected during transmission by enforcing data encryption protocols such as the Internet Protocol Security (IPsec). IPsec is an Internet Protocol (IP) suite for securing communications by authenticating and encrypting each IP packet of a communication session.

¹Windows is a family of graphical operating systems developed, marketed, and sold by Microsoft. Bitlocker is built into Windows 7 (Ultimate and Enterprise Versions) and Windows 8 (Pro and Enterprise), as well as the Windows Server operating systems (2008 and later).

2.2.5 Integrity

The integrity of an asset is adversely affected if the asset is altered incorrectly. For example, the information contained in a database may be altered by accidental corruption (perhaps due to partial storage failure) or by the deliberate unauthorized actions of an individual or individuals. Whether the cause is accidental or deliberate, protecting the integrity of an information asset from unauthorized or unintended modification is an essential component of cyber security. For example, a customer can be overcharged if the integrity of billing information is not protected. A cyber-attacker might compromise system integrity leading to unintended operations of pumps and valves resulting in damage to both information and non-information assets. Integrity at the source can be protected by implementing access controls, process controls, and configuration management. Integrity during data transmission can be achieved by implementing hashing algorithms or cyclic redundancy checks (CRC) to detect corruption.

2.2.6 Availability

The availability of an information asset is the ability to provide reliable and timely access to information assets to authorized individuals. For example, redundant array of independent disks (RAID) technology is commonly used in data storage to combine multiple hard-drive components into a single logical unit. If one hard drive



Fig. 2.1 Cybersecurity goal

fails, the data is still available for use. Computer networks and system have a plethora of equipment and software that must all work in concert to ensure the data is available to authorized individuals.

At its core, the goal of a cyber security program is to provide the required confidentiality, integrity and availability (CIA) protection to the information assets of the organization. Figure 2.1 is a graphical representation of this cyber security goal.

2.3 Risk Assessment Terminology

2.3.1 *Threats*

Threats to the organization's cyber security-related assets can come from a variety of sources. At one level, we can split these threat sources under two primary headings, those arising from people and those arising elsewhere.

2.3.1.1 Threats from People

A variety of people may be considered as threat sources. They may be internal or external to the organization and they may be known or unknown to the organization itself. When considering threats it is often useful to group the threat sources. In the case of people-related threats a non-exhaustive list could be:

- Employees
- Customers
- Vendors
- Former Employees
- Black-hat hackers²

For people-based threat sources, groupings can be made according to criteria such as asset access, skills of the threat source, and motivation of the threat source. For example, an organization may determine that the threats it faces from general administrative staff are distinct from those faced from IT staff (due to different forms of access to assets and varying skill sets), in which case it may choose to further divide the "Employees" group into "General Employees" and "IT Employees". Grouping the threat sources in such a manner helps to simplify the subsequent processes of risk assessment and risk treatment.

²The use of the term hacker has varied over time. The term "black hat hacker" is used here to definitively identify those with both the required technical skills *and* malevolent intentions.

2.3.1.2 Threats from Other Sources

Non-people threat sources include many environmental factors such as fire, flood, temperature, adverse weather, or the availability of required utility services such as electricity and water.

2.3.2 Vulnerabilities

A vulnerability is a weakness in an asset's protections such that a threat source may be able to adversely affect the security requirements (confidentiality, integrity or availability) of an asset.

Consider a basic threat to an information asset such as a computer. A computer behind a locked door may be considered to be less likely to be stolen than one which is in an open area. In this case, the lack of a locked door is a vulnerability which may result in a breach of the asset's availability. Likewise, a locked but weak door may be considered to leave an asset more vulnerable than a locked sturdy door.

The foregoing simple example relates to physical security. In the field of cybersecurity, we often hear the term "vulnerability" used in the context of vulnerabilities found in software. While the detail is different, the premise is the same. A vulnerability is something that one or more threat sources can exploit to negatively impact the confidentiality, integrity or availability of an asset.

2.3.3 Probability

Determining the probability that an asset might be subject to a particular cybersecurity occurrence can be a difficult matter. In some cases, there may be relevant historical data which provides some quantitative input, e.g., the likelihood of earthquakes in a particular region. In other cases, it may be necessary to estimate probability in simple bands such as "low", "medium", and "high". While such banding might seem highly subjective, it nevertheless provides relevant information when it comes to the allocation of limited resources to gain the maximum improvement in cybersecurity posture.

2.3.4 Impact

When considering impact, the aim is to express the impact on the organization's business goals if a threat source successfully exploits an asset's vulnerabilities and negatively impacts its confidentiality, integrity or availability. Again, there may be

some cases where quantitative currency values can be assigned to impact whereas in other situations estimating the impact in bands such as “low”, “medium”, and “high” impact is more practical. For critical infrastructure organizations, the impact of certain events may extend well beyond its own borders and may be difficult to quantify in financial terms. In such cases, organizations may choose to mix quantitative and qualitative methods such as the creation of several bands each representing the number of customers which could be affected by a potential event and the degree to which they would be affected.

2.4 Risk Treatment Terminology

For each identified risk, an organization can consider a number of possible responses as discussed below.

2.4.1 Risk Acceptance

Risk acceptance typically occurs when the organization deems that there are no practical, cost-effective means of further reducing the probability or impact of an event occurrence and therefore decides to accept the residual risk.

2.4.2 Risk Avoidance

In order to truly avoid a risk, it is generally necessary to change the organization’s behavior in some manner such that the risk simply does not arise. An example would be ceasing a particular process because the associated risk was considered to be too high.

2.4.3 Risk Treatment/Risk Mitigation

Treating or mitigating risks is a cornerstone of cybersecurity. It involves applying one or more controls such that the overall risk to an asset (in terms of probability and impact) is within the organization’s tolerance levels. Some controls are specifically aimed at reducing probability whereas others may target impact. By using a combination of controls, both factors can often be reduced.

2.4.4 Risk Transfer

Anybody who has insurance is familiar with one example of risk transfer. In return for payments, a third-party organization agrees to pay out to cover a financial loss in the event of a particular occurrence. Risk transfer can indeed be a useful way of dealing with certain cyber security risks; however, it should be remembered that not all risks are financial in nature. For critical infrastructure organizations, it may for instance, be appropriate to reduce the impact of a theft-related event through risk transfer (i.e., insurance), but intangible assets such as the organization's goodwill and standing in the community may be more difficult or impossible to protect in a similar way.

2.5 Controls Terminology

2.5.1 Controls Overview

Controls are the means by which risk can be mitigated. Individual controls may reduce the probability of a particular cybersecurity occurrence or the impact of such an occurrence. Typically, to reduce both probability and impact of the occurrence multiple controls will be applied.

2.5.1.1 Types of Controls

The word “controls” tends to conjure up images of electromechanical devices, but in the cyber security context controls can take on many forms. Some examples of control types are shown in Table 2.1.

2.5.2 ISO 27001/ISO 27002

The ISO 27001 and ISO 27002 standards were first published in their 2002 versions. These standards are also collectively referred to (with others) as the ISO2700 standards, or ISO27k for short. The current versions at the time of writing are the 2013 versions (ISO/IEC 2013a, b). Prior to 2005, ISO 27001/27002 can trace its roots to earlier British standards under the BS7799 heading, so these standards have matured over many years.

Unless stated otherwise, references to ISO 27001 (ISO/IEC 2013b) or ISO 27002 (ISO/IEC 2013a) in this chapter refer to the 2013 versions of the standard.

A selection of the ISO 27000 family of standards is shown in Table 2.2.

Table 2.1 Example control types

Control type	Description
Directive controls	Directive controls may be administrative instruments such as policies, standards and procedures. An example of a directive control would be the creation of an Acceptable Use Policy for employee use of information resources
Preventive controls	A preventative control attempts to make the occurrence of a breach less likely by making it more difficult for the threat source to cause one. Examples are security guards, security fences, security training, firewalls and intrusion prevention systems
Detective controls	A detective control detects a security breach once it has occurred. Examples are intruder alarms, intrusion detection systems, system monitoring and log monitoring
Corrective controls	A corrective control reduces the effect of a security breach. An example is an anti-virus system isolating an infected file
Recovery controls	A recovery control aims to restore business operations after a security breach. An example of such a control is the creation of a Disaster Recovery Plan

Table 2.2 A selection of ISO/IEC cybersecurity standards

ISO standard number	Main focus of the standard
ISO/IEC 27000:2014	Information security management systems—overview and vocabulary
ISO/IEC 27001:2013	Information security management systems—requirements
ISO/IEC 27002:2013	Code of practice for information security controls
ISO/IEC 27003:2010	Information security management system implementation guidance
ISO/IEC 27004:2009	Information security management—measurement
ISO/IEC 27005:2011	Information security risk management
ISO/IEC 27006:2011	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007:2011	Guidelines for information security management systems auditing
ISO/IEC 27008:2011	Guidelines for auditors on information security controls
ISO/IEC 27031:2011	Guidelines for information and communication technology readiness for business continuity

ISO 27001 and ISO 27002 are designed to be used in tandem. ISO 27001 lays out the requirements for the implementation of an “Information Security Management Systems” (ISMS) compliant with the standard. Annex A of ISO

27001, lists 114 information security controls grouped under 14 control categories. These categories cover functional headings such as supplier relationships, compliance, system acquisition, etc. ISO 27002 provides a code of practice for information security controls and includes further implementation guidance for each of the controls found in ISO 27001 Annex A.

2.6 Requirements of the ISO 27001 Information Security Management System

ISO/IEC 27001 describes an Information Security Management System (ISMS) and details the steps involved in the establishment of such a system in sections 4 through 10 of the standard. Those steps are summarized below.

2.6.1 Context

Under the heading of “context” the organization is required to:

- Determine the external and internal issues which affect the organization as it carries out its business objectives.
- Determine the information security requirements of relevant interested parties.
- Determine the scope of the information security management system. The scope should consider the points above along with the organization’s interfaces with and dependencies on other organizations with regards to the information processes.
- Establish, implement, and maintain an information security management system consistent with the above.

2.6.2 Interested Parties

The concept of “interested parties” was introduced in the 2013 version of ISO 27001. The standard requires that the organization identify “interested parties that are relevant to the information management security system and the requirements of these interested parties relevant to information security”. This approach ensures that an organization is considering the expectations of a wide range of parties which may extend beyond the organization itself into other areas such as customers, vendors, government regulators, and other third parties with an interest in the organization’s information security practices.

2.6.3 Leadership and Commitment

The requirements under this heading are designed to ensure:

- That the information security policies and objectives are consistent with and support the organization's strategic objectives.
- That information security processes are integral to the organization's processes.
- That the resources required for the information management system are available.
- That the importance of information security management is communicated and understood.
- That the objectives of the information security management system are met.
- That relevant organizational people are supported and capable of supporting the information security management system.
- That the information security management system is continually improved.
- That management charged with responsibilities for the ISMS are supported as they provide leadership in the operation of the ISMS.

2.6.4 Policy

Under policy, the senior management of the organization is required to establish an information security policy which:

- Is appropriate to the organization's business objectives.
- Defines information security objectives or a framework for setting the same.
- Commits to meeting relevant information security requirements.
- Commits to the continual improvement of the information security management system.
- Is available in document form.
- Is communicated within the organization.
- Is available to interested parties where appropriate.

In ISO 27001 as with other information security frameworks the definition, adoption, authorization, and resourcing of an information security policy by senior management (at the organizational governance level) is considered to be essential to the success of the cyber security endeavor.

The definition of policy may start with a high-level overview statement from the board regarding the organization's approach to cyber security, its alignment with business objectives, its role in meeting compliance requirements and the resources, roles and responsibilities allocated towards these objectives by the board. Authorities and responsibilities for further fleshing out the details in terms of standards, procedures, guidelines and further subpolicies will flow from the initial high-level policy statement. Taken together, all of these policies, standards,

procedures, and guidelines become the manual which guides stakeholders both in terms of what a particular policy says and what resources are available for carrying out related security measures.

2.6.5 Organizational Roles, Responsibilities, and Authorities

This section requires senior management to assign the responsibilities and authority for information security roles and to ensure that these assignments are widely communicated.

The standard also calls out two specific responsibilities to be assigned, namely:

- The responsibility for ensuring that the information security management system conforms to ISO 27001.
- The responsibility for reporting to senior management on the performance of the information security management system.

2.6.6 Planning

2.6.6.1 Actions to Address Risks and Opportunities

Under the planning heading, ISO 27001 requires the organization to consider the organizational context and the information security requirements of interested parties (as identified under the Context heading above) and to identify and address the risks and opportunities which could impact the ability of the ISMS to achieve its objectives, achieve continual improvement or prevent or reduce undesired effects.

The use of the term “opportunity” may seem out of place, however, this term is being used by ISO 27001 in the context typically found in project management. In that context, a risk is a possibility that future events may not go exactly as planned or expected. Such deviations from the planned or expected path may have negative or positive implications for a project’s success and the term “opportunity” is often used to describe deviations which would have a positive effect on the project outcome.

2.6.6.2 Information Security Risk Assessment

A previous version of the standard published in 2005 detailed a specific mandatory risk assessment process which involved identification of assets, threats, vulnerabilities, and the impact of any resultant breaches to the security requirements of assets. In the 2013 version of the standard this specific asset-based approach is no

longer mandatory, but a formal risk assessment is still required. The current version of ISO 27001 makes reference to the risk assessment methodologies of ISO 31000, however, the organization is free to determine which risk assessment methodology it deems appropriate to its own particular situation. The standard does require that risk owners are identified regardless of the method used to identify risks.

2.6.6.3 Information Security Risk Treatment

For those risks that are higher than the organization is willing to accept, the organization must identify ways to mitigate the risk either by reducing the probability of occurrence or reducing the impact of the occurrence or both. As described in the terminology section above, ISO 27001 refers to the methods of reducing probability or impact (or both) as controls. In the 2005 version of ISO 27001, the controls identified in Annex A of the standard were to be applied first and any remaining unaddressed risks could then be addressed using additional supplementary controls. In the 2013 version of ISO 27001 that sequence has been reversed so that the organization should first apply the controls which it may be obligated to use for contractual, regulatory, or other reasons. The controls listed in ISO 27001 Annex A are then used to supplement those controls which the organization has already deployed. This change reflects the fact that organizations may increasingly find themselves obligated to apply certain controls by a contract, trade group standards, or government regulation, or for other reasons.

ISO 27001 requires the explicit creation of a “statement of applicability” which details which controls have been implemented, why they have been implemented (in the case of controls which are not from Annex A.) or why controls from Annex A. have been omitted. The requirement to create this statement ensures that all of the controls in Annex A. must be considered by the organization and a justification for any implementation omissions of Annex A. controls must be recorded.

2.6.6.4 Information Security Objectives and Planning to Achieve Them

This section of the standard requires that an organization establish measurable and appropriate information security objectives at various levels in the organization. Such objectives must be communicated and updated as required and should include answers to the following:

- How the objective will be achieved?
- What resources are required?
- Who will be responsible?
- What is the timeline to completion?
- Which method will be used to evaluate the results?

2.6.7 Support

The support section of ISO 27001 calls on the organization to provide the necessary resources, skills, awareness, communications, and documentation to support the success of the ISMS.

2.6.7.1 Competence

The standard requires organizations to identify the necessary competences required to successfully operate the ISMS and to support the achievement of those competencies by the relevant roles through education, training, and experience.

The organization is required to measure its success in achieving this goal and is also required to document the necessary competencies and how they have been met by the organization.

2.6.7.2 Awareness

The standard requires the organization to make those working in the organization aware of the organization's information security policies, how their actions can contribute to the objectives of those policies and the implications (for the organization and the individual) of not conforming to the requirements of those policies.

2.6.7.3 Communication

Under this heading, the standard requires the organization to document the critical internal and external communication paths which can support the ISMS. This section should detail:

- The subject of the communications.
- The timing of the communications.
- The other party involved in the communications.
- Who will represent the organization in such communications.
- The process involved in such communications.

2.6.7.4 Documented Information

The standard requires the organization to create, update, and control such documentation as is required by the standard itself and such additional documentation as is necessary to ensure the effectiveness of the ISMS.

Under control of documentation, the standard makes specific reference to access, distribution, use, storage, preservation, change control, retention, and disposition as the areas to be addressed.

2.6.8 Operation

2.6.8.1 Operational Planning and Control

The organization is required to plan the processes necessary for the ISMS and to monitor their effectiveness.

2.6.8.2 Information Security Risk Assessment

The standard requires the organization to perform a risk assessment at planned intervals and when significant changes occur or are proposed. The organization is required to document and retain the results of such assessments.

2.6.8.3 Information Security Risk Treatment

The organization is required to implement the risk treatment plan and document the results thereof.

2.6.9 Performance Evaluation

2.6.9.1 Monitoring, Measurement, Analysis, and Evaluation

The organization is required to establish a system to monitor the effectiveness and performance of the ISMS.

2.6.9.2 Internal Audit

The standard requires the organization to “plan, establish and maintain” audit programs with the purpose of ensuring that the ISMS meets the organization’s requirements and the requirements of the standard and that the ISMS is effectively implemented and maintained. The standard also requires that the results of such audits are reported to management.

2.6.9.3 Management Review

The management review required by the standard should consider internal and external changes which are relevant to the ISMS. The review should also monitor trends in areas such as nonconformance and should also consider audit results. The management review should consider feedback from interested parties, review the status and effectiveness of the risk assessment and risk treatment plan, and should review opportunities for continual improvement of the ISMS.

2.6.10 Improvement

2.6.10.1 Nonconformity and Corrective Action

The standard requires the organization to:

- React to nonconformities and their consequences.
- Document such nonconformities, the subsequent actions taken and the results of those actions.

2.6.10.2 Continual Improvement

The organization is required to continually improve the appropriateness and effectiveness of the ISMS as it relates to the organization's business objectives.

2.7 NIST Computer Security Resource Center

NIST's Information Technology Laboratory (ITL), has a broad mission to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. The Computer Security Division (CSD) is a component of NIST's ITL that develops standards, guidelines, tests, and metrics that are designed to protect the cyber-infrastructure. The CSD's Computer Security Resource Center (CSRC) website³ facilitates broad sharing of information security tools and practices. The CSRC also serves as a resource for information security standards and guidelines, and identifies key security web resources to support users. Between April 1991 and May 2015, the CSD has released 323 publications.

³<http://csrc.nist.gov/>.

Table 2.3 A selection of NIST cybersecurity-related publications

Publication number	Publication title	Publication date
800-12	An Introduction to Computer Security: the NIST Handbook	October 1, 1995
800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems	September 1, 1996
800-27 Rev. A	Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	June 4, 2015
800-30 Rev. 1	Guide for Conducting Risk Assessments	September 12, 2015
800-34 Rev. 1	Contingency Planning Guide for Federal Information Systems	May 10, 2015
800-35	Guide to Information Technology Security Services	October 3, 2015
800-36	Guide to Selecting Information Technology Security Products	October 3, 2015
800-37 Rev. 1	Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach	February 10, 2015
800-39	Managing Information Security Risk: Organization, Mission, and Information System View	March 11, 2015
800-41 Rev. 1	Guidelines on Firewalls and Firewall Policy	September 9, 2015
800-44 Version 2	Guidelines on Securing Public Web Servers	September 7, 2015
800-45 Version 2	Guidelines on Electronic Mail Security	February 7, 2015
800-46 Rev. 1	Guide to Enterprise Telework and Remote Access Security	June 9, 2015
800-47	Security Guide for Interconnecting Information Technology Systems	August 2, 2015
800-50	Building an Information Technology Security Awareness and Training Program	October 3, 2015
800-60 Rev. 1	Guide for Mapping Types of Information and Information Systems to Security Categories	August 8, 2015
800-61 Rev. 2	Computer Security Incident Handling Guide	August 12, 2015
800-65 Rev. 1	Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process	July 9, 2015
800-82 Rev. 2	Guide to Industrial Control Systems Security	May 15, 2015
800-83 Rev. 1	Guide to Malware Incident Prevention and Handling for Desktops and Laptops	July 13, 2015
800-92	Guide to Computer Security Log Management	September 6, 2015
800-94 Rev. 1	Guide to Intrusion Detection and Prevention Systems (IDPS)	July 12, 2015

(continued)

Table 2.3 (continued)

Publication number	Publication title	Publication date
800-100	Information Security Handbook: A Guide for Managers	October 6, 2015
800-114	User's Guide to Securing External Devices for Telework and Remote Access	November 7, 2015
800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	April 10, 2015
800-128	Guide for Security-Focused Configuration Management of Information Systems	August 11, 2015
800-153	Guidelines for Securing Wireless Local Area Networks (WLANs)	February 12, 2015
800-160	Systems Security Engineering Guideline	May 12, 2014
800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	April 15, 2015
800-171	Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	June 15, 2015

Many of these publications are first released in draft forms and then finalized based on comments. Some of the critical documents are also revised on an as-needed basis. The CSD's publications are broadly categorized in one of the following three categories:

1. Federal Information Processing Standards (FIPS) publications are issued by NIST after approval by the Secretary of Commerce pursuant to the Federal Information Security Management Act (FISMA) of 2002.
2. NIST Interagency or Internal Reports (NISTIRs) describe the research of a technical nature of interest to a specialized audience. The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in a more comprehensive form.
3. Special Publications in the 800 series (established in 1990) are of general interest to the cybersecurity community.

This chapter discusses two key cybersecurity-related publications from NIST. Specifically, the Framework for Improving Critical Infrastructure Cybersecurity (NIST 2014) and the Special Publication 800-82—Guide to Industrial Control Systems Security (NIST 2015). In Table 2.3 we have listed a small selection of NIST publications which have particular relevance to the two aforementioned NIST publications. A comprehensive list of NIST CSRC publications including specialist

security information for specific technologies can be downloaded from <http://csrc.nist.gov/publications/>.

2.8 NIST Framework for Improving Critical Infrastructure Cybersecurity

The NIST Framework for Critical Infrastructure Cybersecurity (NIST 2014) was developed in response to Executive Order 13636 which called for the development of a voluntary risk-based cybersecurity framework. The authors of this framework have sought not to “reinvent the wheel,” rather they provide an alternative process approach that is closely aligned to the typical requirements of critical infrastructure providers. The NIST framework makes many references to external resources such as the ISO/IEC 27000 family.

Perhaps the simplest way to contrast the NIST framework approach with that envisaged in ISO27001 is that ISO/IEC 27001 envisages a process cycle leading towards ISO/IEC 27001 certification followed by subsequent cycles during re-certification. The NIST framework by comparison encourages an organization to more rapidly complete a cycle and document their current status across multiple headings, even if the current cybersecurity posture is not where the organization ultimately wants to be. Once improvements have been made the new status can be compared with the old to document progress towards the desired security posture.

This is not to say that ISO/IEC 27001 could not be used in a similar way. By starting with a small scope and progressively increasing the scope through each iterative cycle, the ISO/IEC 27001 approach could result in similar progressive improvements in security posture. However, the NIST framework encourages organizations to consider the wider-scope initially, even if it will be some time before all of the identified issues can be addressed.

Ultimately, an organization which has iterated through the NIST framework and arrived at its desired security posture could then consider the ISO/IEC 27001 certification path. If the organization has been careful to align its NIST framework activities with ISO/IEC 27001 in areas such as risk analysis and application of controls then much of the NIST framework effort should be applicable to the ISO/IEC 27001 certification path.

2.8.1 *Framework Core*

The Framework Core is essentially a set of cybersecurity activities that are common across the critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

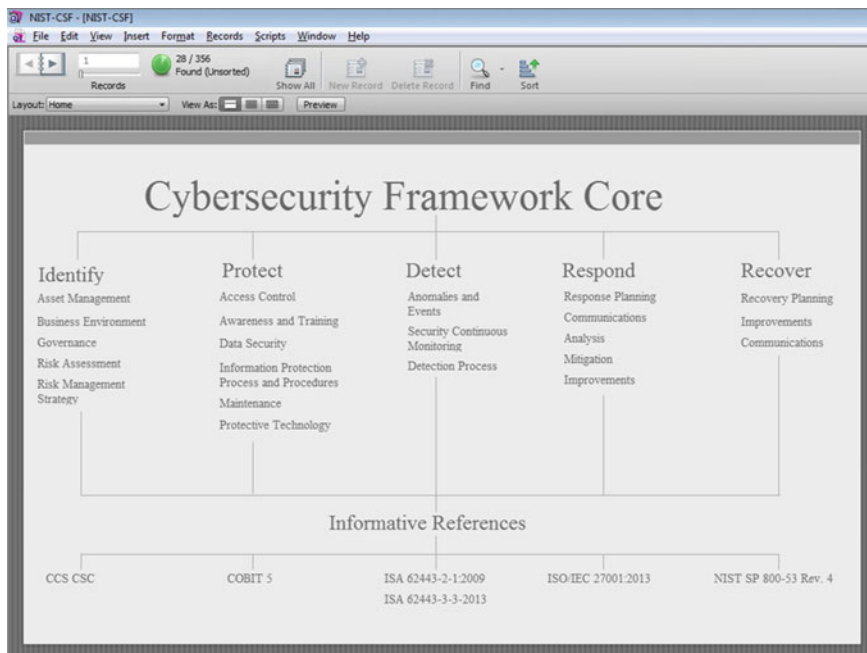


Fig. 2.2 NIST cybersecurity framework reference tool

2.8.1.1 Core Functions

The Framework consists of five core concurrent and continuous functions—Identify, Protect, Detect, Respond, Recover. When these functions are carried out, they provide a high-level strategic view of the lifecycle of an organization's management of cyber security risk. NIST has also developed a Cybersecurity Framework Reference Tool⁴ which allows a user to browse the Framework Core by functions, categories, subcategories, informative references, search for specific words, and export the information. Figure 2.2 shows a screenshot of the reference tool.

The following sections contain an overview of the five core functions.

2.8.1.2 Identify

In order for an organization to improve its security posture, the organization must understand what it is attempting to protect. The identify function includes:

- Identification of assets and their security requirements.
- Identification of security threat sources.

⁴http://www.nist.gov/cyberframework/csf_reference_tool.cfm.

- Estimation of the probability that a threat source may breach an asset's security requirements.
- Estimation of the business impact or consequences of such breaches.
- Prioritization of the risks based on the estimated probabilities and impacts/consequences.
- Development of a risk management approach for the prioritized risks.

2.8.1.3 Protect

Having identified and prioritized the risks that the organization faces the organization will typically wish to apply additional protections as part of its risk management approach. The protect function reduces risks through application of controls such as:

- Policies
- Auditing of policy implementation
- User awareness training
- Access Controls
- Firewalls
- Encryption
- System patching and hardening

ISO27002 (ISO/IEC 2013a) and NIST 800-53 (NIST 2013) include comprehensive lists of such controls and in many critical infrastructure cases organizations will wish to use additional controls due to the nature of specific assets or the nature of the threats to which such assets are exposed.

2.8.1.4 Detect

While the controls that may be deployed under the Protect function above may be thought of as preventative controls, the controls which feature in the Detect function will typically be detective controls, which are concerned with the detection of a cybersecurity event.

The Detect function will typically include:

- Auditing activities.
- Logging and log analysis.
- Use of detective controls such as an Intrusion Detection System.

2.8.1.5 Respond

The Respond function covers how the organization responds to a cybersecurity event. The key purpose of this function is to encourage the organization to be

prepared for response by creating an incident response plan which will include a definition of key responsibilities and determine where they fall.

The Respond function will typically include:

- Creation and updating of an incident response plan.
- Identification of roles and responsibilities prior to, during, and following incident response.
- Post-incident review, analysis, and improvement processes.

2.8.1.6 Recover

The Recover function is concerned with the restoration of business operations.

The Recover function will typically include:

- Creation and updating of a business continuity plan.
- Creation and updating of a disaster recovery plan.
- Post-incident review, analysis, and improvement processes.

2.8.2 *Framework Profile*

An organization determines its target profile by selecting categories and subcategories from those provided in the framework based on its own business objectives and priorities. The target profile can then be compared with the organization's current profile to determine opportunities for improvement. As improvements in cyber security posture are implemented, the current profile will change and provide an indication of progress towards the chosen target profile.

2.8.3 *Implementation Tiers*

Implementation tiers reflect varying degrees of sophistication in cyber security management practices. The framework does not advocate that all organizations seek the most sophisticated tier; rather the framework indicates that an organization should select the tier that meets the organizations' objectives by reducing the risk associated with certain assets to a level acceptable to the organization. Thus, the implementation tiers should not be seen as representing maturity since the most sophisticated tier may not be appropriate to every organization.

The tiers are listed below along with a short description to indicate the level of sophistication of each tier. A full description of the tiers is available in the framework document (NIST [2014](#)).

- Tier 1: Partial
This is the least sophisticated of the tiers and describes low awareness and a somewhat ad hoc and reactive approach to cyber security.
- Tier 2: Risk informed
In this tier, there is awareness of cyber security risk at the organizational level but the necessary structures to successfully manage cyber security across the organization are not in place.
- Tier 3: Repeatable
In this tier, the organization has in place the structures to manage cyber security risk across the organization and the organization is able to respond to changes in risk.
- Tier 4: Adaptive
This is the most sophisticated tier in which cyber security risk management is part of the organizational culture. Suitable cyber security risk management and improvement structures are in place and the organization fully communicates with external partners to achieve cyber security goals.

2.9 NIST Special Publication 800-82—Guide to Industrial Control Systems (ICS) Security

NIST 800-82 (NIST 2015) differs from both the ISO27001 and the cyber security described above in that it focuses directly on cyber security as it relates to ICS which is one of the most critical information asset of a critical infrastructure. NIST defines ICS to include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The ICSs are vital to the operation of the US critical infrastructures that are often highly interconnected and mutually dependent systems. It is estimated that approximately 90 % of the nation's critical infrastructures are privately owned and operated (NIST 2015).

To make this distinction clearer, consider a small gas, electricity, or water utility. Such a utility faces many cyber threats, but only a subset of these threats will be relevant to the ICS. Some threats, for instance, may relate to general customer data such as customer credit/debit card information. Such threats are broadly similar to the threats facing many retailers in terms of the nature of the threats and the impacts that they may cause. However, these utilities also face cyber threats which are quite different from those faced by general retail businesses, in that they target the control systems which are critical to the normal operation of the critical infrastructure. The potential impacts of such threats, when realized, can be vastly different from those faced by the non-critical business sector.

Historically, business and ICS networks were separate because the network topologies were vastly different. Even if a utility owner recognized the value of integrating ICS/SCADA data into their strategic decision support systems, they could not because of limitations in the network topologies. The SCADA systems relied heavily on serial connectivity and very low-frequency radio communications that could provide enhanced range and partial line-of-sight connectivity, none of which supported standard IP connectivity desired by business networks (Panguluri et al. 2011). Furthermore, many ICS components were in physically secured areas and the components were not connected to the traditional IT business networks or systems. However, the recent evolution in low-cost IP devices is promoting the replacement of the older proprietary solutions. This evolution also promotes the connectivity of corporate business systems and the ICSs provide remote access capabilities using industry standard computers, operating systems, and network protocols. While the new connectivity and integration supports new IT capabilities, it also increases the possibility of cyber security vulnerabilities and incidents.

By focusing on the ICS, NIST 800-82 is able to be significantly more specific in its recommendations than the other two standards discussed so far in this chapter. NIST 800-82's focus is broad enough to be relevant to all critical infrastructure entities which operate some type of ICS, yet narrow enough to be able to make specific recommendations relevant to the cyber security of typical ICS components and systems. NIST originally developed the SP 800-82 guidance to meet its statutory responsibilities under the FISMA and the Homeland Security Presidential Directive 7 (HSPD-7) of 2003. NIST SP 800-82 complements NIST SP 800-53's (NIST 2013) recommendations for security controls for Federal IT systems and organizations. NIST 800-82 is designed to specifically assist in developing and deploying an overall security program for ICS architecture including SCADA, DCS and supporting devices, such as PLCs, Remote Terminal Units RTUs, and intelligent electronic devices (IEDs). The standard document that is freely available includes the following five key sections:

- Overview of ICS
- ICS risk management and assessment
- ICS security program development and deployment
- ICS security architecture
- Applying security controls to ICS

Whereas confidentiality is often a particularly high priority requirement in many cyber security scenarios, the ICS security objectives typically follow the priority of availability and integrity, followed by confidentiality. Possible threat incidents that an ICS faces include the following: (NIST 2014)

- Blocked or delayed flow of information through ICS networks disrupting ICS operation
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life

- Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment
- Interference with the operation of safety systems, which could endanger human life

At a minimum, the cybersecurity program implementation and measures at a critical infrastructure should address the following elements:

- Restrict physical and logical access to the ICS network, devices, and network activity.
- Implement measures to protect individual ICS components from exploitation.
- Restrict unauthorized modification of data.
- Implement measures to detect security events and incidents.
- Devise the ability to maintain infrastructure functionality during adverse conditions.
- Have a plan to restore the system after an adverse incident.

NIST SP 800-82 recommends that an effective cyber security program for an ICS should apply the “defense-in-depth,” strategy by layering security mechanisms. The layering approach minimizes the impact of a failure in any one defense mechanism. A defense-in-depth strategy should include a variety of controls as described in the following sections.

2.9.1 Administrative or Directive Controls

- Performing a comprehensive risk assessment and developing a risk management plan.
- Developing security policies, procedures, training, and educational materials that apply specifically to the ICS. In addition, consider enhancing ICS policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases.
- Addressing security throughout the lifecycle of the ICS from architecture design, to procurement, to installation, to maintenance, and to decommissioning.
- Restricting ICS user privileges to only those that are required to perform each person’s job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).

2.9.2 Preventive Controls

- Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer. Providing a logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks, or unidirectional gateways). Employing a de-militarized zone (DMZ) network architecture (i.e., prevent direct traffic between the corporate and ICS networks). Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Restricting physical access to the ICS network and devices.
- Employing reliable and secure network protocols and services were feasible.
- Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications were determined appropriate.
- Expediently deploying security patches after testing all patches under field conditions on a test-system if possible, before installation on the ICS.
- Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).
- Using modern technology, such as smart cards for Personal Identity Verification (PIV).

2.9.3 Detective Controls

- Implementing security controls such as intrusion detection software, anti-virus software, and file integrity checking software, were technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.
- Tracking and monitoring audit trails on critical areas of the ICS.

2.9.4 Corrective Controls

- Ensuring that critical components are redundant and are on redundant networks. Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.

NIST has also developed specific guidance on the application of the security controls in NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations to ICS. While many controls in Appendix F of NIST SP 800-53 are applicable to ICS as written, they may require ICS-specific interpretation and/or augmentation.

Table 2.4 Comparable control groups in NIST and ISO frameworks

NIST 800-53 control families		Examples of related ISO27002-2013 controls	
Name	Section	Title	
Access control	11	Access control	
Awareness and training	8.2.2	Information security awareness, education and training	
Audit and accountability	15.3	Information systems audit considerations	
Security assessment and authorization	15	Compliance	
Configuration management	12.4	Security of systems files	
Contingency planning	14	Business continuity management	
Identification and authentication	11	Access control	
Incident response	13	Information security incident management	
Maintenance	12	Information systems acquisition, development and maintenance	
Media protection	10.7	Media handling	
Physical and environmental protection	9	Physical and environmental security	
Planning	5	Security policy	

2.10 Comparison of Controls

NIST 800-82 (NIST 2015) refers to the 18 control families defined in NIST 800-53 (NIST 2013). There is not a one-to-one mapping of the NIST 800-53 control families with the major control headings in ISO 27002; however, the two standards do cover much of the same ground.

By defining a range of common controls, these standards provide organizations with a template on which to build their own control framework. Note however that the standards also recognize that the changing nature of threats, vulnerabilities, and even assets means that organizations may have to supplement these common controls with new additional controls to address new forms of risk.

Larger organizations may wish to implement ISO 27001/27002 as their general information security framework but may also wish to use NIST 800-82 to address cyber security of their ICS. Despite the lack a one-to-one mapping between the controls in these different standards, it is possible to see distinct similarities in some areas. In Table 2.4, some examples are given of where ISO 27001 control headings cover similar ground to the corresponding NIST 800-53 control family. This list is not meant to be exhaustive, but gives some indication that by being aware of the two standards early in the process it would be possible for an organization to use NIST 800-82 for its ICS security within a larger ISO 27001/ISO 27002 framework without fully duplicating the efforts involved. NIST 800-53 revision 4 (NIST 2013) provides a table which gives an extensive mapping of ISO/IEC 27001 (ISO/IEC 2013b) controls with NIST 800-53 controls (NIST 2013).

2.11 Summary and Conclusions

For those charged with roles and responsibilities regarding an organization's cyber security posture, there are many resources available to assist. Many of these resources use a shared and increasingly standardized terminology and some familiarity with that terminology is beneficial.

Cyber security frameworks provide organizations with useful templates to guide their cyber security efforts. By leveraging the work which has already been done to develop these frameworks, an organization can achieve a better improvement in cyber security more rapidly than would otherwise be possible for a given resource expenditure. Frameworks are available in varying degrees of focus. They range from the broad applicability of ISO 27001/27002 through the critical infrastructure industry focus of the NIST Cybersecurity Framework for Critical Infrastructure to the ICS specificity of NIST 800-82. Each of these frameworks in turn references a wide range of additional documents and standards which can be drawn on by organizations. Where appropriate, organizations may wish to use elements from multiple frameworks to mold a structure that meets the specific requirements of their organization. Likewise, the controls advocated within the framework standards may be augmented as required by additional controls to meet new risks arising from changing threats, changing vulnerabilities, changing assets, changing business objectives, or other varying factors that may arise.

References

- ISO, IEC. (2013a). *ISO/IEC27002:2013 Information technology—Code of practice for information security controls*. Geneva, Switzerland: ISO/IEC.
- ISO, IEC. (2013b). *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements*. Geneva, Switzerland: ISO/IEC.
- NIST. (2013). SP 800-53: Security and privacy controls for Federal Information Systems and Organizations. Washington, DC.
- NIST. (2014). *Framework for improving critical infrastructure security*. Washington: DC, NIST.
- NIST. (2015). *SP 800-82: Guide to Industrial Control Systems (ICS) Security*. Washington: DC, NIST.
- Panguluri, S., Phillips, J. W. R., & Ellis, P. (2011). Cybersecurity: Protecting water and wastewater infrastructure. In S. Hakim, R. M. Clark, & A. Ostfeld (Eds.), *Handbook of water and wastewater systems protection* (pp. 285–318). Springer-Science: New York.

Cyber-Physical Security

Protecting Critical Infrastructure at the State and Local
Level

Clark, R.M.; Hakim, S. (Eds.)

2017, XVIII, 281 p. 32 illus. in color., Hardcover

ISBN: 978-3-319-32822-5