Software Engineering Institute
Carnegie Mellon University

Structuring the Chief Information Security Officer Organization

Julia H. Allen
Gregory Crabb (United States Postal Service)
Pamela D. Curtis
Brendan Fitzpatrick
Nader Mehravari
David Tobar

September 2015

TECHNICAL NOTE
CMU/SEI-2015-TN-007

CERT® Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by USPS under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of USPS or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg. 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0002696

Table of Contents

List of Figures

List of Tables

Acknowledgments

The authors acknowledge the contributions to this report of the SEI Library staff who provided extensive sources on CISO organizational functions and structures.

Abstract

Chief Information Security Officers (CISOs) are increasingly finding that the tried-and-true, traditional information security strategies and functions are no longer adequate when dealing with today's increasingly expanding and dynamic cyber risk environment. Many opinions and publications express a wide range of functions that a CISO organization should be responsible for governing, managing, and performing. How does a CISO make sense of these functions and select the ones that are most applicable for their business mission, vision, and objectives?

This report describes how the authors defined a CISO team structure and functions for a large, diverse U.S. national organization using input from CISOs, policies, frameworks, maturity models, standards, codes of practice, and lessons learned from major cybersecurity incidents.

1 Introduction

Chief Information Security Officers (CISOs), responsible for ensuring various aspects of their organizations' cyber and information security, are increasingly finding that the tried-and-true, traditional information security strategies and functions are no longer adequate when dealing with today's increasingly expanding and dynamic cyber risk environment. The continuous occurrence of highly publicized, global cyber intrusions illustrate the inadequacy of reactive controls- and practices-based approaches, which may be necessary but are not sufficient for protecting and sustaining their organizations' critical cyber assets.

The literature is filled with numerous descriptions of the wide range of functions that a CISO organization should be responsible for governing, managing, and performing. How does a CISO make sense of these and select those functions that are most applicable for his or her organization's mission, vision, and business objectives? In assisting a large, diverse, U.S. national organization in answering this question, we considered the following inputs:

- sources describing the expanding operational risk environment with respect to IT operations, cybersecurity, business continuity, and disaster recovery
- numerous discussions over several years with CISOs and security professionals
- in-depth analysis of recent, large-scale, high-impact cybersecurity incidents including the identification of what worked well and what did not

From these inputs and our experience developing and applying the CERT Resilience Management Model [Caralli 2011], we identified four key functions that capture the majority of a CISO's responsibilities, as shown in Figure 1:

- **Protect, Shield, Defend, and Prevent**
  Ensure that the organization's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the enterprise from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.
- **Monitor, Detect, and Hunt**
  Ensure that the organization's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible.
- **Respond, Recover, and Sustain**
  When a cybersecurity incident occurs, minimize its impact and ensure that the organization's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible. Assets include technologies, information, people, facilities, and supply chains.
- **Govern, Manage, Comply, Educate, and Manage Risk**
  Ensure that the organization's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities. This function includes ensuring compliance with all external and internal requirements and mitigating risk commensurate with the organization's risk tolerance.

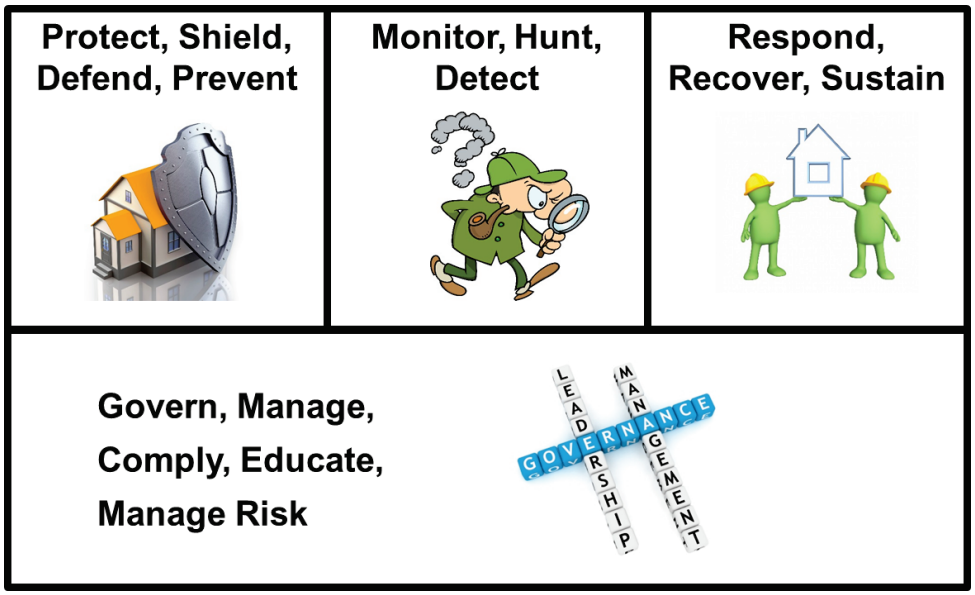

Figure 1: Four CISO Functions

Using these four functions as the foundation, we proceeded to review selected policies, standards, and codes of practice to further decompose the functions into subfunctions and activities, which we then grouped into candidate organizational departments (Section 2) and a proposed organization structure (Section 3). We describe some guidelines and rules of thumb on sizing the CISO organization (Section 4) and recommend several next steps (Section 5).

We recommend that readers consider using this approach as a "strawman" or template for structuring a CISO organization and for allocating roles and responsibilities to its various organizational units. Clearly, CISOs will want to adapt and tailor what is suggested here to meet their specific requirements and priorities.

2 Define Subfunctions, Activities, and Departments

2.1 Process

We selected the following policies, frameworks, maturity models, standards, and codes of practice (referred to as "sources") to expand the definitions and scope of each of the four functions described in Section 1. These sources are broadly accepted as providing credible, reputable guidance that covers the scope of cybersecurity, information security, and continuity of operations as it relates to cybersecurity:

- topics typically addressed in a large organization's information security policy
- *CERT Resilience Management Model, version 1.1* [Caralli 2011]
- U. S. National Institute of Standards and Technology Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2015]
- U.S. Department of Energy *Cybersecurity Capability Maturity Model* (C2M2) [DOE 2014]
- U. S. National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* [NIST 2014]
- National Initiative for Cybersecurity Education (NICE) The National Cybersecurity Workforce Framework Version 1.0 [NICE 2013][1] and the Office of Personnel Management extensions to it [OPM 2014]
- SANS Critical Security Controls [SANS 2015]

For each source, we mapped its specific topics to one of the four functions, Protect, Monitor, Respond, and Govern. Each source topic was expressed as a subfunction (i.e., the next level of detail in support of a function) with one or more supporting activities. As we constructed this mapping, we also recommended several subfunctions that might be "subcontracted" or "outsourced" to an internal or external party where the CISO organization retains an oversight responsibility but does not directly perform the subfunction. Once the mappings were complete, we analyzed the collection of subfunctions and activities and grouped them into meaningful departments, informed by several of the resources listed in the bibliography [EYGM 2014, Kark 2010, Rehman 2013, Scholtz 2011, UW 2015]. Related departments were then collected and represented as a hierarchical organizational chart. This process is depicted in Figure 2. Additional steps of the process are described in Sections 2.2 and 3.

[1] "The National Cybersecurity Workforce Framework establishes the common taxonomy and lexicon that is to be used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed. The Framework is intended to be applied in the public, private, and academic sectors" [NICE 2013, pg. 3].

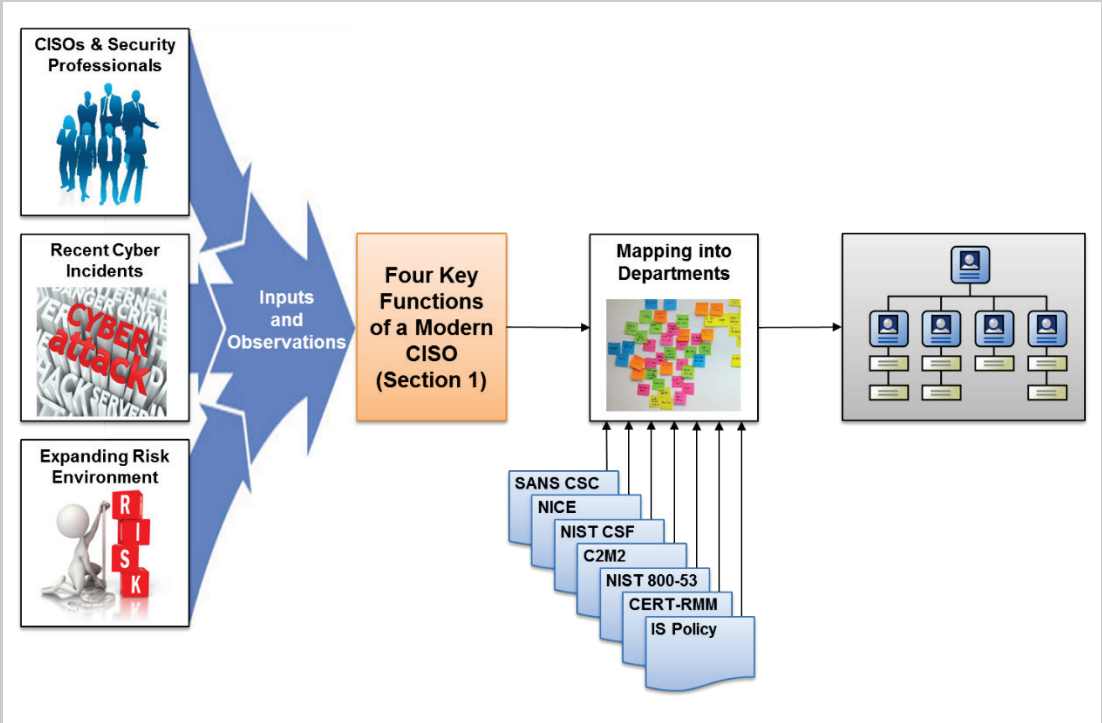

Figure 2: Process for Deriving a CISO Organizational Structure

Table 1 presents several examples from the mapping described above (functions to departments to subfunctions to activities, with supporting sources). Expansion of the source acronyms used in Table 1 appears in Table 2. The full mapping can be found in Appendix A; the full list of acronyms from all sources is available in Appendix B.

Table 1: Sample CISO Function to Source Mapping

Function	Department	Subfunction	Activities	Subcontracted To	IS Policy	CERT-RMM	NIST 800-53	C2M2	NIST CSF	SANS CSC	NICE CWF
Protect, Shield, Defend, Prevent	Application Security	Configuration management	Manage configurations for software and applications	IT[2]	Configuration and change management	KIM, TM	CM	ACM-2	PR.IP, DE.CM	#3	OM:SA
Monitor, Hunt, Detect	Security Operations Center	Virus and malicious code management	Detect, analyze, and eliminate viruses and malicious code		Protection against viruses and malicious code	KIM, TM	SC, SI	TVM-1	DE.CM	#5	OM:SA, PD:VA
Respond, Recover, Sustain	Emergency Operations and Incident Command Center	Incident management and response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents		Security incident management	IMC	IR	IR-1, IR-2, IR-3	DE.AE, DE.DP, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.CO, RC.RP	#18	PD:IR
Govern, Manage, Comply, Educate, Manage Risk	Program Management Office	Information security program/plan	Develop, implement, and maintain an information security program and plan		Information security plan	GP2	PL, PM	CPM	none	none	OD:SO

[2] The most frequently occurring "subcontract to" function is IT or the organization's IT service provider. It is important to note that if a security-related activity is performed by IT, the CISO organization retains oversight responsibility.

Table 2: Source Acronyms[3]

CERT-RMM		**NIST 800-53**		**C2M2**	
IMC	Incident Management and Control	CM	Configuration Management	ACM	Asset, Change and Configuration Management
KIM	Knowledge and Information Management	IR	Incident Response	TVM	Threat and Vulnerability Management
TM	Technology Management	PL	Planning	IR	Event and Incident Response, Continuity of Operations
GP2	Plan the Process	PM	Program Management	CPM	Cybersecurity Program Management
		SC	System and Communications Protection		
		SI	System and Information Integrity		
NIST CSF		**SANS CSC**		**NICE CWF**	
PR.IP	Protect: Information Protection Processes and Procedures	3	Secure Configurations for Hardware and Software	OD:SO	Information Systems Security Operations
DE.AE	Detect: Anomalies and Events	5	Malware Defenses	OM:SA	System Administration
DE.CM	Detect: Security Continuous Monitoring	18	Incident Response and Management	PD:IR	Incident Response
DE.DP	Detect: Detection Processes			PD:VA	Vulnerability Assessment and Management
RS.RP	Respond: Response Planning				
RS.CO	Respond: Communications				
RS.AN	Respond: Analysis				
RS.MI	Respond: Mitigation				
RS.IM	Respond: Improvements				
RC.CO	Recover: Communications				
RC.RP	Recover: Recovery Planning				

[3] There is no relationship between the source entries in each row of Table 2.

2.2 Departments, Subfunctions, and Activities

We used the outcome of the mapping process to identify and allocate each subfunction to one or more of the four functions. The aggregation of related subfunctions resulted from an affinity grouping process. Each group of subfunctions was given a descriptive name that was then used to identify and label candidate organizational departments.

Table 3 lists the departments, subfunctions, and activities for the Protect/Shield function. Table 4, Table 5, and Table 6 contain similar information for the remaining three functions.

Table 3: Protect, Shield, Defend, and Prevent Departments, Subfunctions, and Activities

Department	Subfunction	Activity
Security Engineering (all asset lifecycle-related activities)	Security requirements	Specify and allocate/assign confidentiality, integrity, and availability requirements.
	Security architecture	Develop and maintain a security architecture.
	Secure lifecycle	Address security throughout the development lifecycle.
	Secure lifecycle	Address security throughout the acquisition lifecycle.
	Certification and accreditation	Perform certification and accreditation prior to releasing new systems to production.
Identity Management	Identity and access management	Define and manage identities and access controls based on identities (password management, single sign on, two-factor authentication, PIN management, digital signatures, smart cards, biometrics, Active Directory, etc.)
Application Security (operations, not development lifecycle)	Software and application inventories	Develop and maintain software and application inventories
	Software and application controls	Define, implement, assess, and maintain controls necessary to protect software and applications in accordance with security requirements (operating systems, applications, database management systems, web-based PCI applications, COTS; maintenance)[4]
	Configuration management	Manage configurations for software and applications
	Change management	Manage changes for software and applications
	Host and network inventories	Develop and maintain network, hardware, device, and system inventories (including wireless)
	Host and network controls	Define, implement, assess, and maintain controls necessary to protect networks, hardware, and systems in accordance with security requirements (intrusion prevention/detection)
	Network perimeter controls	Define, implement, assess, and maintain controls necessary to protect the network/Internet perimeter in accordance with security requirements (firewalls, DMZ, network connections, third-party connectivity, remote access, VPNs)[5]
	Configuration management	Manage configurations for networks (including wireless), hardware, and systems
	Change management	Manage changes for networks, hardware, and systems

[4] PCI: payment card industry; COTS: commercial off-the-shelf

[5] DMZ: demilitarized zone; VPN: virtual private network

Department	Subfunction	Activity
Information asset security	Information asset categorization	Designate and categorize information and vital assets (including PII[6]) (includes privacy requirements)
	Information asset inventories	Develop and maintain information asset inventories
	Information asset controls	Define, implement, assess, and maintain controls necessary to protect information and vital assets (including media) in accordance with security requirements (includes privacy requirements, PII, encryption, PKI, backups, DLP, data retention/destruction)[7]
Physical access control	Physical access controls	Define and enforce access controls for facilities and other physical assets (such as networks and hosts)

Table 4 describes the departments, subfunctions, and activities for the Monitor function.

Table 4: Monitor, Hunt, and Detect Departments, Subfunctions, and Activities

Department	Subfunction	Activity
Security operations center	Intelligence collection and threat management	Collect, analyze, triage, and disposition information from all threat sources
	Situational awareness and common operating picture	Collect, analyze, and report information in (near) real time that provides situational awareness and a common operating picture
	Logging	Perform audit logging (includes review and retention) of users, applications, networks, systems, and access to physical assets
	Monitoring	Monitor users, applications, networks, systems, and access to physical assets (includes intrusion prevention/detection, email/spam filtering, web filtering)
	Vulnerability management	Scan for, analyze, and disposition vulnerabilities
	Virus and malicious code management	Detect, analyze, and eliminate viruses and malicious code
	Information security help desk (a.k.a. CIRT[8])	Accept, triage, assign, and disposition all reported suspicious events and security incidents
	Incident management and response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents

6 PII: personally identifiable information

7 PKI: public key infrastructure; DLP: data loss prevention

8 CIRT: Computer Incident Response Team

Table 5 presents the departments, subfunctions, and activities for the Recover/Sustain function.

Table 5: Respond, Recover, and Sustain Departments, Subfunctions, and Activities

Department	Subfunction	Activity
Emergency operations and incident command centers	Incident management and response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents
	Business continuity	Plan for business continuity
	IT disaster recovery	Plan for disaster recovery
	Test/exercise/drill response plans	Test and exercise BC, DR, and incident management plans (penetration testing, etc.)[9]
	Problem management, root cause analysis, and post mortem reports	Perform problem management, analyze root causes, and develop after action reports for high-profile, high-impact incidents
	Investigations	Perform forensic analysis and support investigations (includes interfaces with law enforcement)

Table 6 lists the departments, subfunctions, and several example activities for the Govern/Manage function.

Table 6: Govern, Manage, Comply, Educate, and Manage Risk Departments, Subfunctions, and Example Activities

Department	Subfunction	Example Activity
Program management office	Information security program/plan	• Develop, implement, and maintain an information security program and plan • Allocate adequate trained/skilled resources to implement the information security program and plan • Measure and monitor cost, schedule, and performance
Governance, risk, and compliance	Information security program/plan	Define, implement, and enforce information security policies
	Risk management	Establish an information security risk management strategy, process, and program
	Governance and compliance	• Govern/oversee the information security program and plan (includes CCB and other oversight boards/groups) • Ensure that controls are adequate to meet legal, regulatory, policy, standards, and security requirements (PCI, SOX,[10] etc.) • Conduct audits
Personnel and external relationships	External relationship management	• Manage relationships with third parties (vendors, suppliers, contractors, partners, and critical infrastructure owners/operators) • Manage relationships with external stakeholders (for example, NCCIC, NSA, DHS, US-CERT, FBI, and the press)[11]
	Personnel management	• Manage the employment lifecycle and performance of personnel in accordance with security requirements (background checks, vetting, transfers, risk designations, succession planning, disciplinary action, and termination) • Manage knowledge, skills, capabilities, and availability of the information security team • Implement an enterprise-wide role-based information security awareness and training program

[9] BC: business continuity; DR: disaster recovery

[10] SOX: Sarbanes-Oxley Act

[11] NCCIC: National Cybersecurity and Communications Integration Center; NSA: National Security Agency; DHS: Department of Homeland Security; US-CERT: United States Computer Emergency Readiness Team; FBI: Federal Bureau of Investigation

In the next section, we present the process we performed to derive and define a CISO organizational structure based on these candidate departments, subfunctions, and activities.

3 Derive and Describe the CISO Organizational Structure

3.1 Derive

Using the mapping and analysis outcomes described in Section 2, we developed a CISO organizational structure that includes all of the identified functions, departments, subfunctions, and activities. This structure is depicted in Figure 3 and further defined in the subsequent sections.

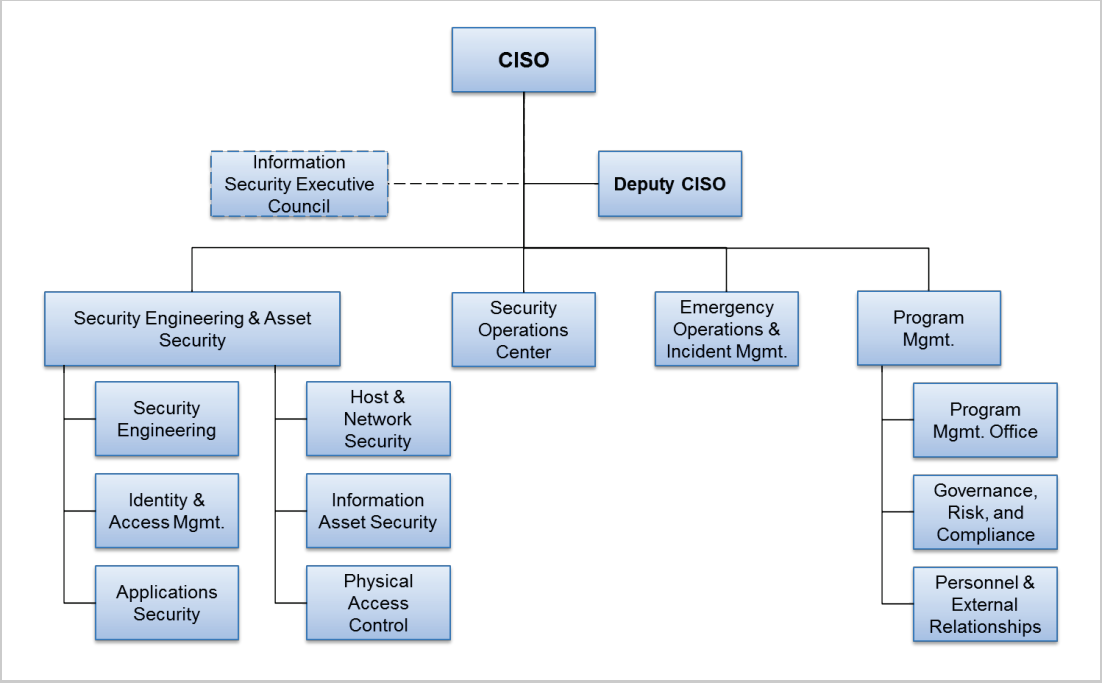

Figure 3: CISO Organizational Structure

3.2 Describe

3.2.1 Program Management

The Program Management unit of the CISO organization includes the three departments shown in Figure 3. The Program Management Office (PMO) performs all activities necessary to develop and successfully implement an information security plan and the program based on that plan. The set of activities performed by the PMO includes the following:

- Develop, implement, and maintain an information security program, plan, and processes
- Define information security roles and responsibilities
- Allocate adequately trained, skilled resources to implement the information security program and plan
- Identify, manage, and maintain the work products required to implement the information security program and plan
- Communicate with and report to (as required) all internal and external stakeholders
- Allocate and manage funding for all information security activities

- Measure and monitor cost, schedule, and performance against the information security plan
- Identify and involve relevant stakeholders (internal and external)
- Review the status of the information security program with higher level managers
- Identify, review, assess, and enable business functions that impact information security (SAAS,[12] cloud, mobile, etc.)

The Governance, Risk, and Compliance (GRC) unit performs all activities required to ensure proper oversight, risk management, and compliance with legal, regulatory, policy, and other information-security related requirements with which the organization is required to comply. The set of activities performed by the GRC unit includes the following:

- Information security program and plan: define, implement, and enforce information security policies
- Risk management: establish an information security risk management strategy, process, and program
- Governance: govern and oversee the information security program and plan (includes the Change Control Board (CCB) and other oversight boards and groups)
- Compliance: ensure that controls are adequate to meet security requirements; conduct audits

The Personnel and External Relationships unit is concerned with managing relationships—those with staff and those with all external parties that are involved in the information security program.

External Relationship Management includes the following:

- managing relationships with third parties (vendors, suppliers, contractors, partners, etc.)
- managing relationships with external stakeholders (for example, NCCIC, NSA, DHS, US-CERT, FBI, the press)

Personnel Management includes the following:

- managing the employment lifecycle and performance of personnel in accordance with security policies and requirements (background checks, succession planning, disciplinary action, termination, etc.)
- managing the knowledge, skills, capabilities, and availability of the information security team
- implementing an enterprise-wide, role-based information security awareness and training program
- defining, implementing, and enforcing the acceptable use policy

3.2.2 Security Operations Center

The Security Operations Center (SOC) is responsible for all day-to-day security operations activities, many of which may be performed by members of the IT organization with regular

[12] SAAS: software as a service

oversight by and reporting to members of the CISO's organization. Typical SOC activities include the following:

- collecting sources of intelligence (adversary behaviors, active incidents, national and international events, etc.)
- analyzing and managing threats to the organization's information security
- conducting situational awareness based on intelligence and threat information, and formulating and reporting an operational view of the external environment
- conducting logging (users, applications, networks, systems, access to physical assets, etc.)
- monitoring logs and other sources of information (users, applications, networks, systems, access to physical assets, etc.)
- managing vulnerabilities, viruses, and malicious code
- providing a responsive information security Help Desk. This activity may also be known as a Computer Incident Response Team (CIRT) or a Computer Security Incident Response Team (CSIRT)
- managing security incidents (detection, analysis, response, and recovery)
- communicating with internal stakeholders and external entities, as required

3.2.3 Emergency Operations and Incident Command

The Emergency Operations and Incident Command unit works closely with the SOC. The primary responsibility of this unit is to mobilize staff, activate response plans, and manage time-critical incident management and response activities when a high-impact incident is declared. During normal operations, this unit conducts the following activities in concert with members of the SOC:

- planning for incident management and response
- planning for business continuity
- planning for IT disaster recovery
- performing tests, exercises, and drills of all response plans
- performing problem management, root cause analysis, and post mortem reviews following the occurrence of an incident
- conducting forensic investigations and working with law enforcement and other regulatory bodies during and following an incident

3.2.4 Security Engineering and Asset Security

The Security Engineering and Asset Security unit includes the six departments shown in Figure 3. One of the primary reasons for including these two subfunctions (Security Engineering and Asset Security) in the same organizational unit is to ensure greater collaboration and cooperation between the development and acquisition activities that occur during security engineering and the operational security activities that occur to ensure that assets (hosts, networks, systems, applications, and information) are secure during operations. Much has been learned over the past several years about the benefits of such collaboration as part of the DevOps approach.[13] That said,

[13] http://www.cert.org/digital-intelligence/research/devops.cfm; https://en.wikipedia.org/wiki/DevOps

some CISOs may choose to separate these subfunctions into distinct organizational units based on technical leadership and staff skills and capabilities.

The Security Engineering department performs the following activities:

- Security requirements: specify, allocate, and assign confidentiality, integrity, and availability requirements to development and acquisition organizations and assets
- Security architecture: Develop and maintain an enterprise security architecture
- Secure lifecycle: ensure that security requirements are adequately addressed throughout the development and acquisition lifecycles for all assets
- Certification and accreditation: perform certification and accreditation prior to releasing new systems and software to production

The Identity and Access Management department is responsible for defining and managing identities that represent persons, objects, and other assets (such as information, technology, and facilities) requiring access. This department is also responsible for defining and implementing access controls based on these identities and their rights. Methods used for identity and access management include Active Directory, passwords, PINs (personal identification numbers), digital signatures, smart cards, biometrics, etc.

The Application Security department conducts the following activities:

- Develop and maintain inventories of software and application assets
- Define, implement, assess, and maintain controls necessary to protect software and applications in accordance with security requirements
- Manage configurations for software and applications
- Manage changes for software and applications

The Host and Network Security department is responsible for performing the following:

- Develop and maintain inventories of network (including wireless), hardware, system, and mobile device assets
- Define, implement, assess, and maintain controls necessary to protect networks, hardware, systems, and mobile devices in accordance with security requirements (This includes, for example, intrusion prevention and detection controls.)
- Define, implement, assess, and maintain controls necessary to protect the network and Internet perimeters in accordance with security requirements (This includes, for example, firewalls, and VPNs.)
- Manage configurations for networks, hardware, systems, and mobile devices
- Manage changes for networks, hardware, systems, and mobile devices

The Information Asset Security department conducts the following activities:

- Designate, prioritize, and categorize information and vital assets (Categorization is typically informed by the criticality and sensitivity of the information asset.)
- Develop and maintain inventories of information assets
- Define, implement, assess, and maintain controls necessary to protect information and vital assets (including media) in accordance with security requirements

Physical security is typically assigned to another organizational executive such as the Chief Security Officer (CSO), so it is not included as a responsibility of the CISO. That said, the CSO and CISO must work closely to ensure that physical assets such as facilities are properly secured, particularly those containing information technology and other operational assets. We do include a Physical Access Control department within the CISO organization that is responsible for defining and enforcing digital and electronic access controls for physical access to facilities and other physical assets such as networks and hosts. Given the limited scope of this department, it could be combined with another one, such as Identity and Access Management.

3.2.5 Information Security Executive Council

The Information Security Executive Council (ISEC) is responsible for advising the CISO and helping to ensure that all (1) information security objectives and requirements are met; (2) policies, programs, and plans are implemented; and (3) externally imposed compliance obligations are met. The ISEC is one aspect of the CISO's governance and oversight responsibility.

The ISEC includes members from all key stakeholder organizational units including, for example, the Chief Operations Officer, Chief Information Officer, Chief Financial Officer, Chief Security Officer (or the role responsible for physical security), General Counsel, Chief Privacy Officer, Human Resources, Communications, Marketing, business unit directors/officers, Director of Engineering, and Director of Information Technology.

The next section provides some guidelines and rules of thumb for determining the number of staff that are required to execute the roles, responsibilities, and activities described in this section.

4 Sizing the CISO Organization

We surveyed several reputable sources for information describing how best to determine the appropriate size for a CISO organization. The sources included

- "Tips and Guidelines for Sizing Your Information Security Organization" [Scholtz 2014]
- "IT Key Metrics Data 2014: Key IT Security Measures: Current Year" [Guevara 2013]
- "Information Security and Data Privacy Staffing Survey 2011" [Wood 2012]
- "How Many Information Security Staff Do We Need?" [Aubuchon 2010]
- "Calculating Security Staffing Requirements" [Rolfe 2003]

"Tips and Guidelines for Sizing Your Information Security Organization" [Scholtz 2014] described results from a survey of 555 organizations in four countries with at least $50M in total annual revenue. The survey timeframe was 24 April to 10 May 2013. Results include the following:

- Number of end users per security full time equivalent (FTE)
  - 75% of organizations reported 500–3,000 end users per security FTE
    - 25% 500–1,000; 25% 1,000–2,000; 25% 2,000–3,000 (33% for federal government)
  - Enterprises that are information centric, with a considerable Internet exposure and a low risk appetite, should typically expect to have a staffing ratio closer to the 500 users to 1 security FTE
  - Enterprises with less data dependence, less Internet exposure, and a higher risk appetite might expect a ratio closer to 3,000 users to 1 security FTE
- Security FTEs as a percentage of IT FTEs: 5.2% (This percentage excludes staff responsible for business continuity and disaster recovery.)
- Security budget as a percentage of IT budget: 5.1%

"IT Key Metrics Data 2014: Key IT Security Measures: Current Year" [Guevara 2013] was drawn from Gartner's IT Key Metrics Data (ITKMD) research, which has been ongoing since 1995. This research collects and analyzes 2,000 metrics from 96 documents covering 21 industries and is supported through Gartner's Benchmark Analytics consulting engagements. Banking and financial services and organizations with revenue from $1B to $10B provided the majority of the data. Per this research, annual IT security and risk management investments are roughly 5.1% of total IT spending, broken out as follows:

- 2.7% for IT infrastructure security
- 0.8% for application security
- 1.6% for IT risk management

Charles Cresson Wood has been conducting the Information Security and Data Privacy Staffing Survey for several years. These surveys draw from reputable sources and use a rigorous survey

methodology. Each survey discusses how percentages rise and fall based on the maturity of an organization's security program. According to his 2011 survey [Wood 2012]

- Information security (IS) staff is typically 0.5% of total organizational staff (includes contractors, consultants, temporaries, and outsourced workers). This means that there is 1 security FTE for every 200 staff.
- IS budgets were expected to increase by 15% in 2012 (average), with the U.S. federal government anticipating a 35% increase.
- 37% of all IS expenditures (average) are devoted to personnel (versus tools, etc.). This statistic may be misleadingly low given the number of unaccounted for IS activities performed by IT and user departments. For the U.S. federal government, 64% of the IS budget is allocated to in-house staff.
- The U.S. federal government outsources 26% of IS work, and 18% of IS work is performed by temporary employees.

The survey provides a prioritized list of seven budgetary influences, with legal and regulatory compliance being the highest. It presents an example of staffing levels and budget calculations for a 10,000-person health care organization using the percentages in various tables in the survey. This survey could be easily translated for a private or public sector organization.

The InfoSec Island article "How Many Information Security Staff Do We Need?" [Aubuchon 2010] examines nine other reports and surveys on the subject of information security staffing. It reports the following summary findings from these sources:

- 3–6 information security staff per 100 IT staff
- 1.75 information security staff per 1 internal IT auditor
- 1 information security staff per 5000 networked devices (workstations, switches, firewalls, servers, etc. This list does not appear to include mobile devices.)
- 3%–11% of the total IT budget is allocated to information security (The authors have often seen 3–5% from CISOs and other literature sources.)

These findings provide general, rule-of-thumb guidance that CISOs can use to help determine the appropriate staff size and budgets for their organizations. That said, these results are highly dependent upon the functions and activities that the CISO is responsible for performing and overseeing.

5 Recommended Next Steps

For organizations and CISOs considering using the guidance presented in this report, we recommend the following next steps:

- Map your current CISO structure to this recommended structure, departments, subfunctions and activities. Identify where you have full coverage of the current structure, partial coverage, and gaps (no or minimal coverage). For partial or minimal/no coverage, determine if these activities are being performed elsewhere in the organization.
- Determine which organizational units can continue as is, which ones need to change (i.e., expand, contract), and if new units need to be created. Consider insourcing and outsourcing solutions as well as encouraging more active collaboration with existing units that perform cybersecurity activities.
- Develop an implementation roadmap. Consider using defined maturity indicator levels to measure progress, derived from, for example, CERT-RMM. This model has been successfully used by the U.S. Department of Energy (Cybersecurity Capability Maturity Model [DOE 2014]) and by the U.S. Department of Homeland Security (Cyber Resilience Review [DHS 2015]) to assess and improve the cybersecurity programs of their constituents. Example maturity indicator levels include incomplete, performed, planned, managed, measured, and defined (also referred to as optimized) [Butkovic 2013].

During 2015, the authors have used the concepts and approaches described in this report with the U. S. Postal Service to help improve their cybersecurity programs, plans, and processes.

Appendix A: Mappings of Functions, Departments, Subfunctions, and Activities

This section presents full mappings of functions to departments to subfunctions to activities, with supporting sources. Appendix B contains a full list of acronyms from all sources.

Table 7: CISO Function to Source Mapping

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Protect/Shield	Security Engineering (all asset lifecycle related activities)	Security requirements	Specify and allocate/assign confidentiality, integrity, and availability requirements		Confidentiality, Integrity, Availability, Security Administration	KIM, TM, RRD, RRM	SA	ACM-1c	ID.BE	#19	OM:SA
Protect/Shield	Security Engineering	Security architecture	Develop and maintain a security architecture		Security Architecture	KIM, TM, RRD, RRM	PL, PM, SA	CPM-3	PR.DS	#19	SP:SS
Protect/Shield	Security Engineering	Secure lifecycle	Address security throughout the development lifecycle	Development organization	Development Security, Operations Security	RTSE, TM	CM, SA	CPM-2f, CPM-4	PR.DS, PR.IP	#6, #19	SP:SD, SP:SR, SP:SS
Protect/Shield	Security Engineering	Secure lifecycle	Address security throughout the acquisition lifecycle	Acquisition organization	Development Security for third parties, Operations Security for third parties	EXD	SA	CPM-2f, EDM-2	PR.DS, PR.IP	#6, #19	SP:SS
Protect/Shield	Security Engineering	Certification and accreditation (CandA)	Perform certification and accreditation prior to releasing new systems to production	Testing/CandA organization	Release Management, CandA	RTSE, TM	CA, SA, PM	ACM-3	PR.DS		SP:IA
Protect/Shield	Identity Management	Identity and access management	Define and manage identities and access controls based on identities (password management, single sign on, two factor authentication, PIN management, digital signatures, smart cards, biometrics, Active Directory, etc.)	IT?	Authorization, Accountability, Identification, Authentication	ID, AM	AC, IA	IAM	PR.AC, PR.PT	#11, #12, #15 #16	OM:SA
Protect/Shield	Application Security (operations, not development lifecycle)	Software and application inventories	Develop and maintain software and applications inventories	IT	Operations Security (Software and Applications)	ADM, KIM	CM	ACM-1	ID.AM, PR.MA	#2	OM:CS

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Protect/Shield	Application Security	Software and application controls	Define, implement, assess, and maintain controls necessary to protect software and applications in accordance with security requirements (operating systems, applications, database management systems, web-based PCI applications, COTS; maintenance)	IT	Operations Security (Software and Applications)	CTRL, KIM, TM, VAR	SA	TVM-1c, TVM-2c, IAM-2	PR.DS		SP:SA
Protect/Shield	Application Security	Configuration management	Manage configurations for software and applications	IT	Configuration Management (Software and Applications)	KIM, TM	CM	ACM-2	PR.IP, DE.CM	#3	OM:SA
Protect/Shield	Application Security	Change management	Manage changes for software and applications	IT	Change Management (Software and Applications)	KIM, TM, VAR	CM, MA	ACM-3	PR.IP		OM:SA
Protect/Shield	Host and Network Security	Host and network inventories	Develop and maintain network, hardware, device, and system inventories (including wireless)	IT	Operations Security (Hosts and Networks)	ADM, TM	CM	ACM-1	ID.AM, PR.MA	#1	OM:CS
Protect/Shield	Host and Network Security	Host and network controls (mainframes, network devices, servers, workstations, mobile devices; maintenance)	Define, implement, assess, and maintain controls necessary to protect networks, hardware, and systems in accordance with security requirements (intrusion prevention/detection)	IT	Operations Security (Hosts, Networks, Mobile Devices)	CTRL, TM, EC, VAR	SC	TVM-1c, TVM-2c, IAM-2	PR.AC, PR.DS, PR.PT, DE.AE		OM:NS, PD:DS

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Protect/Shield	Host and Network Security	Network perimeter controls	Define, implement, assess, and maintain controls necessary to protect the network/Internet perimeter in accordance with security requirements (firewalls, DMZ, network connections, third-party connectivity, remote access, VPNs)	IT	Operations Security (Network Perimeters)	CTRL, TM, EC, EXD, VAR	SC	TVM-1c, TVM-2c, IAM-2	PR.AC, PR.PT	#7, #10, #13	OM:NS, PD:DS
Protect/Shield	Host and Network Security	Configuration management	Manage configurations for networks (including wireless), hardware, and systems	IT	Configuration Management (Hosts, Networks, Mobile Devices)	TM	CM	ACM-2	PR.IP, DE.CM	#3, #10	OM:NS, SP:SS
Protect/Shield	Host and Network Security	Change management	Manage changes for networks, hardware, and systems	IT	Change Management (Hosts, Networks, Mobile Devices)	TM, VAR	CM, MA	ACM-3	PR.IP		OM:NS
Protect/Shield	Information Asset Security	Information asset categorization	Designate and categorize information and vital assets (including PII) (includes privacy requirements)	CPO and others	Information Designation and Categorization	ADM, KIM	FIPS 199, 200, RA, SI		ID.AM		SP:SR
Protect/Shield	Information Asset Security	Information asset inventories	Develop and maintain information asset inventories	??	Operations Security (Information Assets)	ADM, KIM	FIPS 199, 200, SI	ACM-1			OM:CS

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Protect/Shield	Information Asset Security	Information asset controls	Define, implement, assess, and maintain controls necessary to protect information and vital assets (including media) in accordance with security requirements (includes privacy requirements, PII, encryption, PKI, backups, DLP, data retention/destruction)	IT, CPO	Operations Security (Information Assets)	CTRL, KIM	MP, SI	TVM-1c, TVM-2c, IAM-2	PR.DS, PR.IP, PR.PT	#8, #17	SP:SD, SP:IA
Protect/Shield	Physical Access Control	Access to facilities; access to hosts and networks	Define and enforce access controls for facilities and other physical assets (such as networks and hosts)	CPI/CSO; IT	Physical Access Controls; Physical Protection of Information Assets	EC, TM	PE	IAM-2	PR.AC		OD:SP
Monitor/Hunt	Security Operations Center	Intelligence collection and threat management	Collect, analyze, triage, and disposition information from all threat sources		Intelligence Collection; Threat Management		PM, SI	TVM-1	ID.RA		AZ:AS, AZ:EA, AZ:TG, CO:CY
Monitor/Hunt	Security Operations Center	Situational Awareness and Common Operating Picture	Collect, analyze, and report information in (near) real time that provides situational awareness and a common operating picture		Situational Awareness		PM, SI	SA-3	DE.AE		PD:DA
Monitor/Hunt	Security Operations Center	Logging	Perform audit logging (includes review and retention) of users, applications, networks, systems, access to physical assets	IT	Logging	MON	AU	SA-1, MA-a, MA-d	PR.MA, PR.PT, DE.CM	#14	PD:DA, PD:DS

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Monitor/Hunt	Security Operations Center	Monitoring	Monitor users, applications, networks, systems, access to physical assets (includes intrusion prevention/detection, email/spam filtering, web filtering)	IT	Monitoring	TM, MON	AU	SA-2, MA-a, MA-l40d	DE.CM	#11, #14, #17	CO:CO, PD:DA, PD:DS
Monitor/Hunt (previously Protect/Shield)	Security Operations Center	Vulnerability management	Scan for, analyze, and disposition vulnerabilities	IT	Vulnerability Management	VAR	RA, SA, SI	TVM-2	ID.RA, PR.IP, DE.CM, RS.MI	#4	OM:SA, PD:VA
Monitor/Hunt (previously Protect/Shield)	Security Operations Center	Virus and malicious code management	Detect, analyze, and eliminate viruses and malicious code	IT	Virus Management; Malicious Code Management	KIM, TM	SC, SI	TVM-1	DE.CM	#5	OM:SA, PD:VA
Monitor/Hunt	Security Operations Center	Information Security Help Desk (a.k.a. CIRT)	Accept, triage, assign, and disposition all reported suspicious events and security incidents		Incident Management (Detect)	IMC	IR, NIST 800-61	IR-1, IR-2, IR-3	DE.AE, RS.CO, RS.AN		OM:CS, PD:IR
Monitor/Hunt	Security Operations Center	Incident management and response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents		Incident Management	IMC	IR, NIST 800-61	IR-1, IR-2, IR-3	DE.AE, DE.DP, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP	#18	PD:DS, PD:IR
Recover/Sustain	Emergency Operations and Incident Command Centers	Incident management and response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents		Incident Management	IMC	IR, NIST 800-61	IR-1, IR-2, IR-3	DE.AE, DE.DP, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP	#18	PD:IR
Recover/Sustain	Emergency Operations and Incident Command Centers	Business continuity	Plan for business continuity	BC	Business Continuity Management and Planning	SC	CP	IR-4, MA-a, MA-d	PR.IP		OD:SP, SP:SD
Recover/Sustain	Emergency Operations and Incident Command Centers	IT disaster recovery	Plan for disaster recovery	IT DR	IT Disaster Recovery Management and Planning	SC	CP	IR-4	PR.IP		OD:SP, SP:SD

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Recover/Sustain	Emergency Operations and Incident Command Centers	Test/exercise/drill response plans	Test and exercise BC, DR, and incident management plans (penetration testing, etc.)		Test/Exercise Incident, BC, and DR Plans	SC, IMC	CP, IR, NIST 800-61	IR-3e, IR-3j, IR-4f	PR.IP, DE,DP	#20	OM:SS
Recover/Sustain	Emergency Operations and Incident Command Centers	Problem management, root cause analysis, and post mortem reports	Perform problem management, analyze root causes, and develop after action reports for high-profile, high-impact incidents		Problem Management; Incident Post Mortem/Lessons Learned	TM		IR-3h	DE.AE, RS.AN		PD:IR
Recover/Sustain	Emergency Operations and Incident Command Centers	Investigations	Perform forensic analysis and support investigations (includes interfaces with law enforcement)		Forensic Analysis; Investigations	IMC	IR, NIST 800-61	IR-3i	RS.AN		IN:DF, IN:IV
Govern/Manage	Program Management Office	Information security program/plan	Develop, implement, and maintain an information security program and plan		Information Security Program/Plan	GP2	PL, PM	CPM			OD:SO
Govern/Manage	Program Management Office	Information security program/plan	Define, implement, maintain, and improve information security processes		Information Security Processes	OPD, OPF	PL, PM		PR.IP, DE.DP		OD:ST
Govern/Manage	Program Management Office	Information security program/plan	Define information security roles/responsibilities		Information Security Program/Plan (roles, responsibilities)	GP4	PL, PM	WM-1, MA-h	ID.AM, ID.GV, DE.DP, RS.CO		OD:SP, OD:ST
Govern/Manage	Program Management Office	Information security program/plan	Allocate adequate trained/skilled resources to implement the information security program and plan		Information Security Program/Plan (trained, skilled resources)	GP3	PL, PM	CPM-2d, MA-i			OD:SP, OPME
Govern/Manage	Program Management Office	Information security program/plan	Identify, manage, and maintain the work products required to implement the information security program and plan		Information Security Program/Plan (work products)	GP6	PL, PM	CPM-1			OD:SO

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Govern/Manage	Program Management Office	Information security program/plan	Reporting and communications		Information Security Program/Plan (reporting, communications)	COMM	PL, PM	SA-3a, ISC			OD:SP
Govern/Manage	Program Management Office	Information security program/plan	Allocate and manage funding for the information security activities		Information Security Program/Plan (funding)	FRM	PL, PM	MA-c			OD:SP,OPME
Govern/Manage	Program Management Office	Information security program/plan	Measure and monitor cost, schedule, performance		Information Security Program/Plan (measure cost, schedule, performance)	MA, GP8	PL, PM	CPM-2i, CPM-2j			OD:SP, OPME
Govern/Manage	Program Management Office	Information security program/plan	Identify and involve relevant stakeholders (internal and external)		Information Security Program/Plan (stakeholders)	GP7	PL, PM	MA-b	PR.AT, PR.IP, RS.CO, RC.CO		OD:ST
Govern/Manage	Program Management Office	Information security program/plan	Review the status of the security program with higher level managers		Information Security Program/Plan (review status with executives)	GP10	PL, PM	CPM-1f			OD:SP
Govern/Manage	Program Management Office	Information security program/plan	Identify, review, assess, and enable business services/functions that rely on/impact information security (mergers and acquisitions, SAAS services, cloud services, mobile security strategy/guidelines, new mail applications)		Information Security Program/Plan (enable business services)	EF	PM, SA	CPM-1c	ID.BE		OD:SP, SP:SR
Govern/Manage	Governance, Risk, and Compliance	Information security program/plan	Define, implement, and enforce information security policies		Information Security Program/Plan (policy)	EF, GP1	PL, PM	MA-e, MA-f (MA-d in CPM), CPM-2g	ID.GV		OD:SP, OD:ST

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Govern/Manage	Governance, Risk, and Compliance	Risk management	Establish an information security risk management strategy, process, and program		Risk Management	RISK	RA, NIST 800-39	RM	ID.GV, RS.MI, RC.CO		OD:ST, SP:IA
Govern/Manage	Governance, Risk, and Compliance	Governance and compliance	Govern/oversee the information security program and plan (includes CCB and other oversight boards/groups)		Governance	EF, GP1	PM	CPM-1. CPM-2			OD:SP
Govern/Manage	Governance, Risk, and Compliance	Governance and compliance	Ensure that controls are adequate to meet legal, regulatory, policy, standards, and security requirements (PCI, SOX, etc.)		Compliance	COMP, TM, VAR, GP8, GP9	AU	IAM-2	ID.GV, PR.IP		SP:IA
Govern/Manage	Governance, Risk, and Compliance	Governance and compliance	Ensure that controls are adequate to meet privacy requirements	CPO	Compliance	KIM	AP, AR, DI, DM			#17	SP:IA
Govern/Manage	Governance, Risk, and Compliance	Governance and compliance	Conduct audits		Audit	COMP, GP9	AU	TVM-2k, CPM-2j, EDM-2i, MA-g			SP:IA
Govern/Manage	Personnel and External Relationships	External relationship management	Manage relationships with third parties (vendors, suppliers, contractors, partners, critical infrastructure owners/operators))		Third Party Relationship Management	EXD	PS, SA	EDM	ID.AM, ID.BE, ID.GV, PR.AT, PR.IP		OD:SP, OPME
Govern/Manage	Personnel and External Relationships	External relationship management	Manage relationships with external stakeholders (for example, NCCIC, NSA, DHS, US-CERT, FBI, the press)		External Stakeholder Management	EXD, GP7	PM	MA-b	PR.IP, RS.CO, RC.CO		IN:IV, OD:SP

Function	Department	Subfunctions	Activities	Subcontracted To	IS Policy Topics	RMM	NIST 800-53	C2M2	NIST CSF	SANS Top 20	NICE CWF
Govern/Manage	Personnel and External Relationships	Personnel management	Manage the employment lifecycle and performance of personnel in accordance with security requirements (background checks, vetting, transfers, risk designations, succession planning, disciplinary action, termination)	HR	Personnel Management (lifecycle, performance)	HRM, PM	PS	WM-2 a-h			OD:SP, OPME
Govern/Manage	Personnel and External Relationships	Personnel management	Manage knowledge, skills, capabilities, and availability of the information security team	HR	Personnel Management (knowledge, skills, capabilities, availability)	HRM, PM	PS	WM-3	PR.AT, PR.IP	#9	OD:SP, OPME
Govern/Manage	Personnel and External Relationships	Personnel management	Implement an enterprise-wide role-based information security awareness and training program		Personnel Management (awareness, training)	OTA, GP5	AT	WM-4	PR.AT	#9	OD:ET
Govern/Manage	Personnel and External Relationships	Personnel management	Define and enforce acceptable use	IT	Personnel Management (acceptable use)	AM, ADM, KIM	SC		PR.AT, PR.IP		OD:ST, OPME

Appendix B: Complete List of Source Acronyms

Appendix A presents full mappings of functions to departments to subfunctions to activities, with supporting sources. This section contains a full list of acronyms from all sources.

Table 8: Complete List of Source Acronyms

Acronym	Definition	Source
ACM	Asset, Change and Configuration Management	C2M2
CPM	Cybersecurity Program Management	C2M2
EDM	Supply Chain and External Dependencies Management	C2M2
IAM	Identity and Access Management	C2M2
IR	Event and Incident Response, Continuity of Operations	C2M2
ISC	Information Sharing and Communications	C2M2
MA	Management Activities	C2M2
RM	Risk Management	C2M2
SA	Situational Awareness	C2M2
TVM	Threat and Vulnerability Management	C2M2
WM	Workforce Management	C2M2
ADM	Asset Definition and Management	CERT-RMM
AM	Access Management	CERT-RMM
COMM	Communications	CERT-RMM
COMP	Compliance	CERT-RMM
CTRL	Controls Management	CERT-RMM
EC	Environmental Control	CERT-RMM
EF	Enterprise Focus	CERT-RMM
EXD	External Dependencies Management	CERT-RMM
FRM	Financial Resource Management	CERT-RMM
GP1	Establish Process Governance	CERT-RMM
GP10	Review Status with Higher Level Managers	CERT-RMM
GP2	Plan the Process	CERT-RMM
GP3	Provide Resources	CERT-RMM
GP4	Assign Responsibility	CERT-RMM
GP5	Train People	CERT-RMM
GP6	Manage Work Product Configurations	CERT-RMM
GP7	Identify and Involve Stakeholders	CERT-RMM
GP8	Monitor and Control the Process	CERT-RMM
GP9	Objectively Evaluate Adherence	CERT-RMM
HRM	Human Resource Management	CERT-RMM
ID	Identity Management	CERT-RMM
IMC	Incident Management and Control	CERT-RMM
KIM	Knowledge and Information Management	CERT-RMM
MA	Measurement and Analysis	CERT-RMM
MON	Monitoring	CERT-RMM

Acronym	Definition	Source
OPD	Organizational Process Definition	CERT-RMM
OPF	Organizational Process Focus	CERT-RMM
OTA	Organizational Training and Awareness	CERT-RMM
PM	People Management	CERT-RMM
RISK	Risk Management	CERT-RMM
RRD	Resilience Requirements Development	CERT-RMM
RRM	Resilience Requirements Management	CERT-RMM
RTSE	Resilient Technical Solution Engineering	CERT-RMM
SC	Service Continuity	CERT-RMM
TM	Technology Management	CERT-RMM
VAR	Vulnerability Analysis and Resolution	CERT-RMM
AZ:AS	Analyze: All Source Intelligence	NICE CWF
AZ:CT	Analyze: Cyber Threat Analysis	NICE CWF
AZ:EA	Analyze: Exploitation Analysis	NICE CWF
AZ:TG	Analyze: Targets	NICE CWF
CO:CO	Collect and Operate: Collection Operations	NICE CWF
CO:CY	Collect and Operate: Cyber Operations	NICE CWF
IN:DF	Investigate: Digital Forensics	NICE CWF
IN:IV	Investigate: Investigations	NICE CWF
OD:ET	Oversight and Development: Education and Training	NICE CWF
OD:SO	Oversight and Development: Information Systems Security Operations	NICE CWF
OD:SP	Oversight and Development: Security Program Management (CISO)	NICE CWF
OD:ST	Oversight and Development: Strategic Planning and Policy Development	NICE CWF
OM:CS	Operate and Maintain: Customer Service and Technical Support	NICE CWF
OM:DA	Operate and Maintain: Data Administration	NICE CWF
OM:KM	Operate and Maintain: Knowledge Management	NICE CWF
OM:NS	Operate and Maintain: Network Services	NICE CWF
OM:SA	Operate and Maintain: System Administration	NICE CWF
OM:SS	Operate and Maintain: Systems Security Analysis	NICE CWF
OPME	Cybersecurity Supervision, Management, and Leadership	NICE CWF
PD:DA	Protect and Defend: Computer Network Defense Analysis	NICE CWF
PD:DS	Protect and Defend: Computer Network Defense Infrastructure Support	NICE CWF
PD:IR	Protect and Defend: Incident Response	NICE CWF
PD:VA	Protect and Defend: Vulnerability Assessment and Management	NICE CWF
SP:IA	Securely Provision: Information Assurance Compliance	NICE CWF
SP:SA	Securely Provision: Software Assurance and Security Engineering	NICE CWF
SP:SD	Securely Provision: Systems Development	NICE CWF
SP:SR	Securely Provision: Systems Requirements Planning	NICE CWF
SP:SS	Securely Provision: Systems Security Architecture	NICE CWF
SP:TE	Securely Provision: Test and Evaluation	NICE CWF
AC	Access Control	NIST 800-53
AT	Awareness and Training	NIST 800-53
AU	Audit and Accountability	NIST 800-53
CA	Security Assessment and Authorization	NIST 800-53

Acronym	Definition	Source
CM	Configuration Management	NIST 800-53
CP	Contingency Planning	NIST 800-53
IA	Identification and Authorization	NIST 800-53
IR	Incident Response	NIST 800-53
MA	Maintenance	NIST 800-53
MP	Media Protection	NIST 800-53
PE	Physical and Environmental Protection	NIST 800-53
PL	Planning	NIST 800-53
PM	Program Management	NIST 800-53
RA	Risk Assessment	NIST 800-53
SA	System and Services Acquisition	NIST 800-53
SC	System and Communications Protection	NIST 800-53
SI	System and Information Integrity	NIST 800-53
DE.AE	Detect: Anomalies and Events	NIST CSF
DE.CM	Detect: Security Continuous Monitoring	NIST CSF
DE.DP	Detect: Detection Processes	NIST CSF
ID.AM	Identify: Asset Management	NIST CSF
ID.BE	Identify: Business Environment	NIST CSF
ID.GV	Identify: Governance	NIST CSF
ID.RA	Identify: Risk Assessment	NIST CSF
ID.RM	Identify: Risk Management Strategy	NIST CSF
PR.AC	Protect: Access Control	NIST CSF
PR.AT	Protect: Awareness and Training	NIST CSF
PR.DS	Protect: Data Security	NIST CSF
PR.IP	Protect: Information Protection Processes and Procedures	NIST CSF
PR.MA	Protect: Maintenance	NIST CSF
RC.CO	Recover: Communications	NIST CSF
RC.IM	Recover: Improvements	NIST CSF
RC.RP	Recover: Recovery Planning	NIST CSF
RS.AN	Respond: Analysis	NIST CSF
RS.CO	Respond: Communications	NIST CSF
RS.IM	Respond: Improvements	NIST CSF
RS.MI	Respond: Mitigation	NIST CSF
RS.RP	Respond: Response Planning	NIST CSF
1	Device Inventory	SANS CSC
2	Software Inventory	SANS CSC
3	Secure Configurations for Hardware and Software	SANS CSC
4	Continuous Vulnerability Assessment and Remediation	SANS CSC
5	Malware Defenses	SANS CSC
6	Application Software Security	SANS CSC
7	Wireless Access Control	SANS CSC
8	Data Recovery Capability	SANS CSC
9	Security Skills Assessment and Training	SANS CSC
10	Secure Configurations for Network Devices	SANS CSC

Acronym	Definition	Source
11	Limitation and Control of Network Ports, Protocols and Services	SANS CSC
12	Controlled Use of Administrative Privileges	SANS CSC
13	Boundary Defense	SANS CSC
14	Maintenance, Monitoring and Analysis of Logs	SANS CSC
15	Controlled Access	SANS CSC
16	Account Monitoring and Control	SANS CSC
17	Data Protection	SANS CSC
18	Incident Response and Management	SANS CSC
19	Secure Network Engineering	SANS CSC
20	Penetration Tests and Red Team Exercises	SANS CSC

Bibliography

URLs are valid as of the publication date of this document.

[Aubuchon 2010]
Aubuchon, Kurt. "How Many Information Security Staff Do We Need?" September 2010. http://www.infosecisland.com/blogview/8327-How-Many-Information-Security-Staff-Do-We-Need.html

[Butkovic 2013]
Butkovic, Matthew & Caralli, Richard. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale* (CMU/SEI-2013-TN-028). Carnegie Mellon University: Software Engineering Institute, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69187

[Caralli 2011]
Caralli, Richard A.; Allen, Julia H.; & White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011. http://www.informit.com/store/cert-resilience-management-model-cert-rmm-a-maturity-9780321712431

[DHS 2015]
U.S. Department of Homeland Security US-CERT Cyber Resilience Review website, September 2015. https://www.us-cert.gov/ccubedvp/self-service-crr

[DOE 2014]
U. S. Department of Energy. *Cybersecurity Capability Maturity Model (C2M2) Version 1.1*. U. S. Department of Energy and U. S. Department of Homeland Security, February 2014. http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

[EYGM 2014]
"Security Operations Centers - helping you get ahead of cybercrime." EYGM Limited, EYG no. AU2689, October 2014. http://www.ey.com/GRCinsights

[Guevara 2013]
Guevara, Jamie; Hall, Linda; Stegman, Eric. "IT Key Metrics Data 2014: Key IT Security Measures: Current Year." Document Number G00258905, Gartner, Inc., December 2013. https://www.gartner.com/doc/2633841/Fit-key-metrics-data-&usg=AFQjCNGQWseSdTT4lUWq7eP4miuj4Z1Z0A&sig2=80E6Ub69MHoNEOBclpJgsg

[Kark 2010]
Kark, Khalid and Dines, Rachel A. "Security Organization 2.0: Building a Robust Security Organization." Forrester Research, Inc., May 10, 2010. http://eval.symantec.com/mktginfo/enterprise/articles/b-article_security_organization_20_building_a_robust_security_organization.en-us.pdf

[NICE 2013]
National Initiative for Cybersecurity Education (NICE). *The National Cybersecurity Workforce Framework Version 1.0*. National Initiative for Cybersecurity Education, March 2013. http://csrc.nist.gov/nice/framework

[NIST 2014]
U. S. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*. U. S. National Institute of Standards and Technology, February 2014. http://nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[NIST 2015]
Joint Task Force Transformation Initiative. *Security and Privacy Controls for Federal Information Systems and Organizations NIST Special Publication 800-53 Revision 4*. U. S. National Institute of Standards and Technology, January 2015. http://csrc.nist.gov/publications/PubsSPs.html

[OPM 2014]
U.S. Office of Personnel Management. "Cybersecurity Category/Specialty Area," *The Guide to Data Standards, Part A: Human Resources*, Update 16, November 15, 2014, pg. A-109. https://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf

[Rehman 2013]
Rehman, Rafeeq. "CISO Job Responsibilities v3." Information Security and Cloud Computing blog, January 8, 2013. http://rafeeqrehman.com/?attachment_id=576

[Rolfe 2003]
Rolfe, Andy. "Calculating Security Staffing Requirements." CSOonline.com, August 2003. http://www.csoonline.com/article/2116162/data-protection/calculating-security-staffing-requirements.html

[SANS 2015]
SANS. "Critical Security Controls Version 5.0." SANS, 2015. http://www.sans.org/critical-security-controls/

[Scholtz 2011]
Scholtz, Tom. "Information Security Organization Dynamics." Document Number G00213579, Gartner, Inc., June 2011.

[Scholtz 2014]
Scholtz, Tom. "Tips and Guidelines for Sizing Your Information Security Organization." Document Number G0023971, Gartner, Inc., April 2014. https://www.gartner.com/doc/1723715/information-security-organization-dynamics

[UW 2015]
"Information Security Program." The Office of the CISO, University of Washington, 2015. http://ciso.washington.edu/about-us/information-security-program/

[Wood 2012]
Wood, Charles Cresson. “Information Security and Data Privacy Staffing Survey 2011: Benchmarking the Information Security Function.” Information Shield, Inc., January 2012. http://www.informationshield.com/papers/2011SecurityPrivacyStaffingSurvey.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	September 2015	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Determining a Structure for the Chief Information Security Officer (CISO) Organization	FA8721-05-C-0003

6. AUTHOR(S)

Julia H. Allen, Gregory Crabb, Pamela D. Curtis, Brendan Fitzpatrick, Nader Mehravari, David Tobar

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2015-TN-007

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Chief Information Security Officers (CISOs) are increasingly finding that the tried-and-true, traditional information security strategies and functions are no longer adequate when dealing with today's increasingly expanding and dynamic cyber risk environment. Many opinions and publications express a wide range of functions that a CISO organization should be responsible for governing, managing, and performing. How does a CISO make sense of these functions and select the ones that are most applicable for their business mission, vision, and objectives?

This report describes how the authors defined a CISO team structure and functions for a large, diverse U.S. national organization using input from CISOs, policies, frameworks, maturity models, standards, codes of practice, and lessons learned from major cybersecurity incidents.

14. SUBJECT TERMS	15. NUMBER OF PAGES
CISO, chief information security officers, cyber security, information security	48

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL