Enterprise IT Security Management by the Numbers

Using NIST and FIPS to Develop a Management Framework

We take for granted that everybody reading this magazine probably knows that Information Security is about ensuring the Confidentiality, Integrity, and Availability (CIA; called the CIA Triad) of your organization's information. However, for the average person Information Security can be an overwhelming concept to grasp. Mention it in the local shopping mall and you will get a mixed set of reactions ranging from fear to confusion to amusement. Yet for those of us who spend time reinforcing our tin-foil hats with chicken wire (after all, everybody KNOWS that Faraday cages are the best way to stop signals from leaking) the everyday duties required to keep an enterprise computing environment safe is a staggering ballet of firewalls, intrusion detection, policies, and encryption algorithms. The correct answer to what Information Security is will depend on whom you ask - the firewall administrator sees it as a set of complex and interlaced rules, while all the Active Directory team may see is users and their associated groups.

For the new manager of an Information Security program, you must ask which of those answers is correct. The answer to your question is that both of them are right. Each of these answers are but parts of the greater system consisting of an interlocked series of layered controls which provide 'defense-in-depth' against all potential threats to your computing environment. As cryptologist Bruce Schneier said, "Security is... more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together. "

Unfortunately, Information Security solutions are complex, diverse, and are not usually of the 'plug-and-play' variety. How do you make all of these processes, technologies, and products fit together? How do you make sure that your Information Security plan is comprehensive? Deciding how to start a program is one of the most fundamental complexities of managing an Enterprise Information Security Program (EISP). According to the International Information Systems Security Certification Consortium, Inc., (ISC)²®, there are ten domains[1] in Information Security:

1. Access Control
2. Application Development Security
3. Business Continuity and Disaster Recovery Planning
4. Cryptography
5. Information Security Governance and Risk Management
6. Legal, Regulations, Investigations and Compliance
7. Operations Security
8. Physical (Environmental) Security
9. Security Architecture and Design
10. Telecommunications and Network Security.

Covering all of these areas with an effective and systematic strategy is complicated and can be overwhelming.

NIST INFOSEC DOCUMENTS

The **Federal Information Processing Standards** (FIPS) Publication Series is the official series of publications relating to standards and guidelines adopted and promulgated under the pro-visions of the Federal Information Security Management Act (FISMA) of 2002.

The **Special Publication 800-series** reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

ITL Bulletins are published by the Information Technology Laboratory (ITL). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis.

Source: Guide to NIST Security Documents [2]

Fortunately there is help. The United States (US) National Institute of Standards and Technology (NIST) Special Publications (SP) 800 series and the US Federal Information Processing Standards (FIPS), which are also published by NIST (which is part of the U.S. Department of Commerce) provide a solid basis for any security program, whether in-side or outside of government space that can scale to meet the unique needs of your organization. NIST currently has about 300 documents which are the security guidelines used by most U.S. Federal agencies. These documents are provided free to the public at the NIST Computer Security Division's Computer Security Resource Center (CSRC), at **http://csrc.nist.gov** [3].

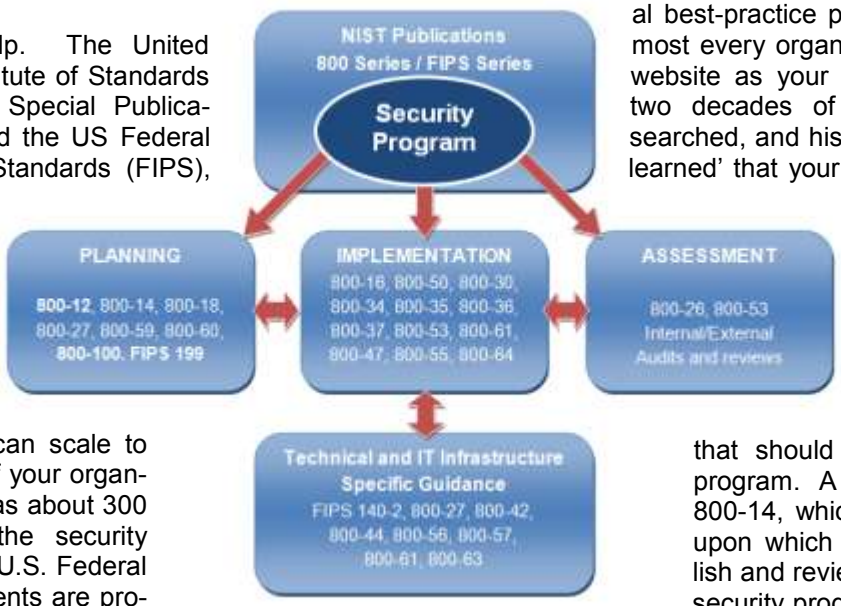

Figure 1. *NIST Information Security structure*

It is important to note that the NIST framework is based on a Data-Centric Security Model (DCSM). DCSM operates on the principle that all information is not created equal; this is because some has more inherent value to your organization than does others. According to IBM's experts, "the primary goal of data-centric security is to drive security controls from a business requirements perspective [4]." Effectively this level of security is driven by questions that determine the significance of data in context of its use within the agency, or an information risk management approach.

> **"Knowing where the data is helps us close the gaps."**
>
> **ISABELLE THEISEN**
> Chief Security Officer,
> First Advantage Corp. [5]

There are a number of guidelines and frameworks which provide direction on how to categorize information. For example, FIPS 199 is the definitive guideline for Federal organizations to determine data classification, and it bases information's value on its value compared to inherent threats to determine the risk to the organization [6]. Regardless, DCSM should drive the decisions that determine appropriate security controls: physical restriction, encryption, least-privileged access, logging, etc.

One additional general note on NIST documentation: many of the documents are aging (for example, 800-12 was written in 1995!)... do not let this fool you. Where NIST or FIPS publications get into specific technological concepts, they are updated. However, many of them are tech-agnostic, choosing instead to provide sets of general best-practice principles that apply to almost every organization. Consider NIST's website as your own resource for almost two decades of time-proven, highly researched, and historically effective 'lessons learned' that your organization may benefit from - starting with your EISP strategy.

Planning

When beginning the strategic planning process, there are some practical issues that should be considered for your program. A great place to start is SP 800-14, which "provides a foundation upon which organizations can establish and review information technology security programs. The eight Generally Accepted System Security Principles in SP 800-14 are designed to provide the public or private sector audience with an organization-level perspective when creating new systems, practices, or policies. [6]"

Another key resource is SP 800-12 *An Introduction to Computer Security* [7]. 800-12 is a great reference regardless of your security experience and background, because it provides technology-neutral concepts, security program structure guidance, common-sense considerations, as well as supporting resources that you might use to develop security controls. For example, section 2 details the eight elements which are the foundation of the document's general approach to computer security:

1. Computer security should support the mission of the organization.
2. Computer security is an integral element of sound management.
3. Computer security should be cost-effective.
4. Computer security responsibilities and accountability should be made explicit.
5. System owners have computer security responsibilities outside their own organizations.
6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer security is constrained by societal factors.

Other guidance can be found in other documents like SP 800-27 Revision (rev) A, *Engineering Principles for Information Technology Security (A Baseline for Achieving*

Security)[8] which provides security management principles in six categories:

- Security Foundation
- Risk Based
- Ease of Use
- Increase Resilience
- Reduce Vulnerabilities, and;
- Design with Network in Mind

800-27 goes into greater detail about each category, providing a total of 33 'sub' principles which have a lower level of detail about each of the six categories. Each of these discusses the system development life-cycle, at which stage of the principles applies, and a discussion about the importance of each item.

It is all about Risk!

In order to know if you covered your bases when developing your strategy, you must determine (as with all Information Security decisions) where the risk lies. The core of the NIST system is a Risk Management Framework (RMF), which analyzes risk at three tiers: the organization, mission, and Information System view and is described in NIST SP 800-39, *Managing Information Security Risk*[9]. The RMF is focused on the entire security life cycle, and is comprised of six steps:

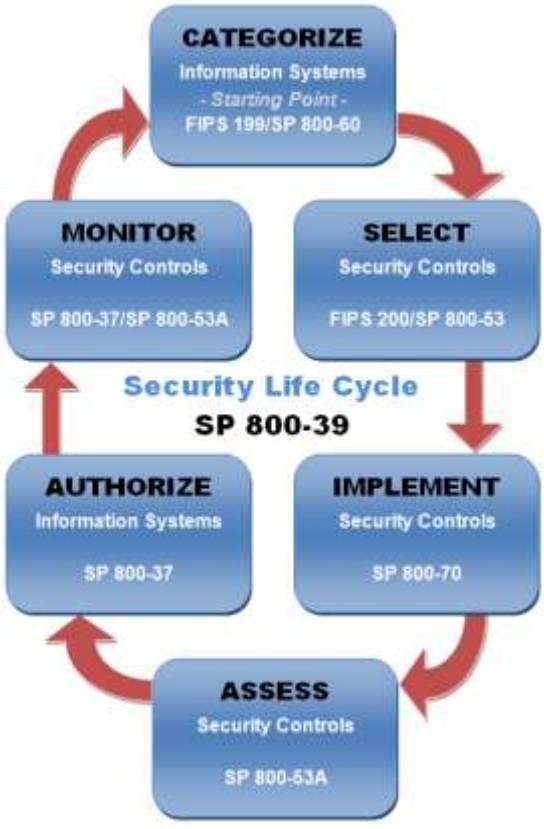

Figure 2. *NIST Risk Management Framework* [10]

1. Security Categorization
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize Information Systems
6. Monitor Security State

Risk is the underlying driver for all Information Security systems, processes, and yes, even budgets. Risk is critical because it explains, in empirical terms, why Information Security activity 'x' matters to the business unit it is designed to support by protecting the CIA of its information resources. In order to better understand this process, let's review each of the NIST RMF steps: categorize, select, implement, assess, authorize, and monitor -- and apply them to your Information Security program.

1. Categorize *FIPS 199, SP 800-60*

As the DSCM concept suggests, categorization is a critical task in Information Security. According to NIST, "Security categorization provides a structured way to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system. The security category is based on the potential impact (worst case) to an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions."[11]

FIPS 199 provides guidelines for the information owner to classify (categorize) your information as High, Moderate, or Low values but you can substitute the appropriate term for your organization (e.g., Public, Internal, and Sensitive) based on the culture, function, and political environment of the company.

Additionally, SP 800-60, Volume 1: *Guide for Mapping Types of Information and Information Systems Security Categories*[12] is practical guidance that explains the categorization process functionally by describing the lower level processes used to categorize enterprise information.

2. Select *FIPS 200, SP 800-53*

One of the documents that has been around for years and constantly updated is NIST SP 800-53 rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*[13]. This has been combined

with FIPS 200, *Minimal Security Requirements for Federal Information and Information Systems*[14] to "ensure that appropriate security requirements and security controls are applied to all Federal information and information systems. An organizational assessment of risk validates the initial security control selection and determines if any additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations" [13].

NIST 800-53 breaks its Information Security requirements into seventeen control "families":

- (AC) Access Control
- (AT) Awareness and Training
- (AU) Audit and Accountability
- (CA) Certification, Accreditation and Security Assessments
- (CM) Configuration Management
- (CP) Contingency Planning
- (IA) Identification and Authentication
- (IR) Incident Response
- (MA) System Maintenance
- (MP) Media Protection
- (PL) Security Planning
- (RA) Risk Assessment
- (SA) System and Services Acquisition
- (SC) System and Communications
- (SI) System and Information Integrity

As with many of these Federal documents, they are largely driven by the Federal Information Security Management Act (FISMA) of 2002. While your organization may not be directly subject to FISMA, do not let this stop you from considering how these guidelines might apply in your environment. 800-53 provides a simplified RMF, revised and updated security controls, security baseline configurations, and a variety of other useful tools.

3. Implement *SP 800-70*

SP 800-70 is deceptive. While it appears to be directed solely on the provisioning and use of Governmental security checklists, this is a very extensible concept for every enterprise. 800-70[15] provides directions on how to use security checklists, as well as a link to the National Checklist Repository (NCR), which is located at **http://checklists.nist.gov** [16]. The NCR is part of the National Checklist Program (NCP).

These checklists are step-by-step security configuration guidelines for most major technologies, and they are currently being migrated to align with the Security Content Automation Protocol (SCAP). SCAP provides a common standard which allows you to import NCR configuration files and run them natively within many major security tools. With a SCAP-compatible tool and a few clicks, your security program could provide reporting and analysis on the security configurations of most of the organization's technology systems.

While not a NIST publication, security practitioners might also consider the SANS™ (SysAdmin, Audit, Network and Security) resources available to assist in security control implementation. SANS™ provides a wide-array of Information Security resources like their extensive training seminars, the Internet Storm Center (for new patches and alerts), podcasts, and security white papers.

However, one of most popular SANS resources is the SANS™ Top 20 Security Controls[17], which is available online (**http://www.sans.org/critical-security-controls**). This details the 20 most critical security controls based on the research of a consortium sponsored by the Center for Strategic and International Studies. SANS™ provides details on each of the top 20 controls, guidance on implementation, and tested resources proven to be an effective way for organizations to implement continuous monitoring. For example, when the U.S. State Department's CISO John Streufert implemented the SANS™ top 20 cyber-security controls they realized an "80% reduction in 'measured' security risk" [17].

NIST 800-53 may also be useful for reducing your compliance overhead as related to other security requirements that impact your organization (ISO, SOX, CObIT, PCI, etc.). By meeting the NIST requirements, you may be able to address other requirements by cross-referencing to other security controls.

Figure 3. *Sample of the symantec™ IT Controls Reference*

For example, a simple and free resource was created by symantec™, called the *IT Controls Reference*[18]. This document (see Figure 3) can be downloaded as a PDF or even printed at poster size. It cross-references ISO 17799, CObIT 4.0, SOX/COSO, HIPAA, PCI, GLBA, NERC CIP, and PIPEDA. You can download a copy of the *IT Controls Reference* from several online sources.

A more comprehensive solution is the Unified Compliance Framework (UCF)[19], which harmonizes hundreds of authoritative compliance requirements in a cross-referenced "Rosetta Stone" spreadsheet. The UCF allows your organization to select applicable requirements, and creates a single register to clarify control conflict with four updates per year. Paid subscriptions available online at **http://www.unifiedcompliance.com**.

4. Assess *SP 800-53A*

800-53A[20], published in June 2010, is a highly adaptive document wherein NIST describes how to test the effectiveness of the controls listed in 800-53.

More importantly, 800-53A provides guidance on how to provide assurance of the effectiveness of your security controls, including penetration testing, and step-by-step instructions for each of the controls and control enhancements (the number varies between versions, but usually around 200). If you need to have the framework to evaluate your controls, this is the place to look. It provides information on what constitutes successful implementation of the security requirements, what type of documentation would be valid testing evidence, and other useful evaluation tips. These guidelines can be used to establish management self-reporting of controls assigned to management, and even to develop your own repository of 'audit evidence' that can be used to meet audit requests for control documentation.

Also note that recent feedback from FISMA pushes the importance of automated controls. There is no doubt that automation can increase the effectiveness of some controls, but it can also make them very predictable. Keep in mind that automation can be effective, but it cannot totally replace the analysis of a skilled Information Security professional.

5. Authorize *SP 800-37*

This section is easy: if you do not know what it means, it probably does not apply to you. Authorization is the process by which Federal organizations or their contractors certify a system has appropriate Information Security controls in place, and is ready to be authorized. External assessors review and validate the system's controls, and if the agency agrees with the evaluation the system gets officially 'blessed' by the responsible agency. This process is designed to confirm that the system is ready to go into a live or production status.

6. Monitor *SP 800-37, SP 800-53A*

Monitoring is the part of Information Security most EISP programs forget to account for, but is critical in the Total Cost of Ownership (TCO) calculation. You cannot just stand up a piece of equipment in your environment and expect it to work forever; the threats, risks, and even your own environment are far too dynamic for that. The monitoring process should be fully funded to provide for the 'care and feeding' of all of the controls you implemented in steps 1-5. Failure to do so will ultimately result in a failure of your tools to live up to the full functionality you touted during your business justification.

This is particularly true for staffing concerns. Many Information Security managers keep buying all-encompassing, enterprise-class tools, yet maintain the same level of staffing. These 'solutions' eventually reach a point of diminishing returns as your staff may become so overworked that they end up being ineffective with any of the tools they administer. Shepherding your staff's time helps not only ensure that you do not get blindsided during your next audit, but may also help you make sure you don't get owned by the next hacker or virus.

Conclusion

In conclusion, as the manager of your EISP there are a few items you should keep in mind. Firstly, while all of these concepts are really important the *most* important factor not discussed in your program is culture. Create a culture of Information Security aware employees, who understand that compliance with security rules and regulations is not the Information Security department's role alone - it is the charge of every employee. The corollary to this rule is that culture is driven by the 'tone at the top'. Without the support of your executive leadership, your Information Security program will develop a 'Russian' culture (characterized by 'check-offs' and 'mark-offs').

Secondly, keep in mind that all of these security controls are not the pole that you must jump *over*, but the floor your organization jumps *from*. They represent the minimum you *must* do, but not necessarily everything that you *should* be doing to your company's information. By implementing your program and being an 'evangelist' for a data-centric & risk-based security, you should ensure that risk management becomes an inextricable part of your organization's culture.

Finally, for all of this guidance remember: your expert opinion IS THE KEY. Unless you are legally bound to NIST's guidelines, they should only be guidelines; use them where they make business sense in your organization and drop anything that does not 'fit' with your business, unique risks, or technology footprint. Every dollar you spend or packet your program inspects should be based on ensuring the CIA of your organization's information in order to fully support your business operations. Use the NIST and FIPS documents in order to help provide a standard framework that is the backbone of your company's robust EISP strategy.

SHAYNE CHAMPION

References:

[1] Common Book of Knowledge (CBK)®, Information Systems Security Certification Consortium, Inc., (ISC)²®. http://www.isc2.org

[2] Guide to NIST Information Security Documents, Pauline Bowen. National Institute of Standards and Technology, US Department of Commerce, December 2009.

[3] *Computer Security Resource Center (CSRC)*, Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology. http://csrc.nist.gov.

[4] Data Centric Security. Mike Bilger, Luke O'Connor, Matthias Shunter, Morton Swimmer, and Nev Zunic; IBM Global Services; December 2006.

[5] Compliance 2.0, Elizabeth Horwitt. TechTarget; 2009.

[6] FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; February 2004.

[7] NIST SP 800-12: An Introduction to Computer Security: The NIST Handbook. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; October 1995.

[8] NIST SP 800-27A: Engineering Principles for Information Technology Security. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; June 2004.

[9] NIST SP 800-39: Managing Information Security Risk. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; March 2011.

[10] NIST SP 800-37 R1: Guide for Applying the Risk Management Framework to Federal Information Systems. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; February 2010.

[11] Categorize Step FAQs: NIST Risk Management Framework. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; January 2009.

[12] NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; August 2008.

[13] NIST SP 800-53 R3: Recommended Security Controls for Federal Information Systems and Organizations. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; August 2009.

[14] FIPS PUB 200: Minimal Security Requirements for Federal Information and Information Systems. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; March 2006.

[15] NIST SP 800-70 R2: National Checklist Program for IT Products—Guidelines for Checklist Users and Developers. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; February 2011.

[16] National Checklist Repository (NCR). Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; http://checklists.nist.gov

[17] *SANS™ Top 20 Security Controls*. System Administration (SysAdmin), Audit, Network and Security (SANS)™ Institute. http://www.sans.org/critical-security-controls

[18] IT Controls Reference, Symantec™.

[19] *Unified Compliance Framework (UCF)*. IT UCF: The Science of Compliance; Network Frontiers LLC and Latham & Watkins LLP. http://www.unifiedcompliance.com.

[20] NIST SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Computer Security Division, Information Technology Laboratory; National Institute of Standards and Technology; June 2010.