https://doi.org/10.48009/1_iis_2020_22-29

Issues in Information Systems
Volume 21, Issue 1, pp. 22-29, 2020

MANAGING CYBER SECURITY COMPLIANCE ACROSS BUSINESS SECTORS

Kevin J. Slonka, University of Pittsburgh, slonka@pitt.edu

ABSTRACT

Cyber security is a key consideration in ensuring the privacy and safety of organizational data. This need extends beyond individual business sectors up to, and including, national security. Due to the varying regulatory requirements for cyber security, a Western PA IT firm had the need to create a cyber security management strategy that allowed them to manage compliance for their customers, which span most major industries, in such a way that is time and cost effective. The IT firm solved this problem by creating a master database that contains all necessary regulations (plus many additional details) mapped to a master set of security controls. This cyber security management strategy not only allows the IT firm to bring customer networks into compliance by finding and remediating deficiencies but also manage and maintain their compliance throughout the years.

Keywords: cyber, security, management, compliance, CUI, PHI, FTI, IRC, CJIS, PCI, GDPR, GLBA

INTRODUCTION

In the threat landscape of 2020, cyber security is of the utmost importance. The average cost of a security breach is approximately $225 per record and, with companies taking an average of 46 days to remediate, the average breach costs companies $21,155 per day (Krishan, 2018). While some are taking cyber security strategy to the government/national level (Ibrahim et al., 2018; Kovacs, 2018) others are proposing various tactics and techniques to protect individual networks (Arlitsch & Edelman, 2014; Edelman, 2019; Lee & Kang, 2015). This far reach of cyber security necessity cannot be better expressed than by the myriad of laws and regulations from different business sectors requiring companies operating within those sectors to enforce some basic level of cyber security hygiene on their business' networks. A quick (and incomplete) list of some of the well-known regulations is as follows:

- US Government Controlled Unclassified Information (CUI) - 48 CFR § 252.204-7012 (NIST SP 800-171)
- Protected Health Information (PHI) - Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 CFR § 164)
- Federal Tax Information (FTI) - IRS Internal Revenue Code (IRC) (IRS Publication 1075)
- FBI Criminal Justice Information Services (CJIS) - FBI CJIS Security Policy
- Payment Card Information (PCI) - PCI Data Security Standard (DSS)
- European Union (EU) Individuals' Privacy - General Data Protection Regulation (GDPR) 2016/679
- Automotive Dealer Financing - Gramm-Leach-Bliley Act (GLBA)

Even business sectors that do not work with what is typically considered sensitive information (e.g., medical records, government data, etc.) have the need for a basic level of cyber security hygiene (Shelhart, 2018). In Pennsylvania, the Supreme Court ruled that companies "owe a duty to Employees to use a reasonable care to safeguard their sensitive personal data [including, but not limited to, names, birth dates, social security numbers, addresses, tax forms, and bank account information] in collecting and storing it on an internet-accessible computer system" (Dittman v. UPMC, 2017, p. 32). While some companies do not have a literal law requiring them to implement cyber security controls, all companies in Pennsylvania now have a legal precedent that essentially requires such controls in order to protect people's personal information stored on their network. The bottom line is that all companies have some sort of responsibility to protect sensitive data.

As a small cyber security/information technology (IT) firm operating in Western Pennsylvania (herein, the IT firm), many clients fit into one or more of the aforementioned regulation categories. Each regulation is comprised of security controls that aim to mitigate the most common cyber security risks, such as trojans, denial of service, cloud security, spyware, and phishing

among others (Jenab & Moslehpour, 2016). Additionally, cyber security not only includes technical configurations but also organizational and critical infrastructure elements. This introduced the need for a way to manage the implementation and maintenance of cyber security regulations in such a way that a single process could support all regulations while balancing the costs and benefits (Dutta & McCrohan, 2002). Having a single process would ensure that the IT firm does not need its employees to manage and maintain seven, or more, different programs, which would severely increase the cost of operating in this space.

This paper offers a case study of the IT firm's journey developing an efficient, manageable, and replicable process for managing cyber security regulations across business sectors.

FINDING COMMON GROUND

In order to achieve a single process that can handle the existing, and any future, cyber security requirements, common ground must be found between all sets of requirements. Upon a reading of each set of requirements one can notice that each has very similar goals in mind. While each document explains the specifications using different words, the spirit of the goal is the same. Take, for example, the following security controls in Table 1 from four of the major regulations:

Table 1: Comparison of similar security controls

Regulation	Security Control Text
NIST 800-171	3.5.1 Identify system users, processes acting on behalf of users, and devices (SP 800-171r1, 2016, p. 28)
HIPAA	164.312(a)(2)(i) Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity ("HIPAA", 2013, p. 66).
IRS 1075	9.3.7.2 Identification and Authentication (Organizational Users): The information system must: a. Uniquely identify and authenticate agency users (or processes acting on behalf of agency users) (Publication 1075, 2016, p. 88).
FBI CJIS	5.5.1 Account Management: The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. […] Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges ("Criminal Justice", 2019, p. 41).

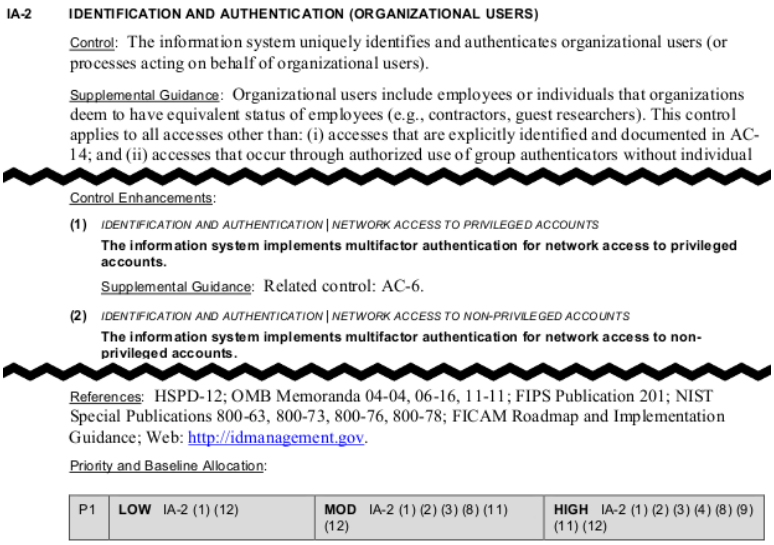
Each regulating body uses different words to express each specific control. Some are more verbose than others. The spirit of all four of these controls, however, is the same: every person must be uniquely identifiable on the network, meaning that everyone has their own user account and the sharing of user accounts is prohibited. Some regulations tend to combine multiple atomic specifications into a single control, but the point remains that each regulation is essentially attempting to accomplish the same goal.

It should be easy to see from Table 1 that if every control in every regulation document (there are hundreds of controls in each) varies widely in how it is written it would be extremely costly, in every form of the word, and nearly impossible, for an IT firm to build an efficient, manageable, and replicable process around the implementation and maintenance of such security controls.

Luckily, there is common ground between these regulations. The industry standard for security controls is the NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. This 462-page document is used by the United States Federal Government to secure systems housing data critical to national security. This means it is more complex, more restrictive, and contains more security controls than necessary for any other business sector, if taken as a

whole. The good news, however, is that due to its complexity it can be picked apart in order to arrive at a smaller list of security controls that are relevant to varying business sectors.

In the above security control example of Table 1, each control exhibited the same spirit through different words. Looking through the 800-53 document, one can find security control IA-2, which discusses the identification and authentication of users. IA-2, like most security controls in this document, has five sections: Control (lays out the literal wording of what is to be accomplished), Supplemental Guidance (expounds upon the control, giving various examples and items to consider when attempting to implement the control), Control Enhancements (takes more complex controls and breaks them into sub-controls so that each individual specification can be accurately tracked and managed), References (lists various approved documents that contain more information that may be useful when implementing this control), and Priority and Baseline Allocation (lists the priority of the control as well as which of the sub-controls are required to be implemented on federal systems of varying security levels: Low, Moderate, and High). Figure 1 shows portions of IA-2 in order to gain an understanding of the level of detail in the 800-53 document.



IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual

Control Enhancements:

(1) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for network access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

(2) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for network access to non-privileged accounts.

References: HSPD-12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-2 (1) (12)	**MOD** IA-2 (1) (2) (3) (8) (11) (12)	**HIGH** IA-2 (1) (2) (3) (4) (8) (9) (11) (12)

Figure 1. Condensed view of the IA-2 security control (SP 800-53r4, 2013)

It is clear that each of the controls in Table 1 can be mapped to IA-2 in the 800-53 document, thus proving that 800-53 can be used as the master source for security controls.

MAPPING TO THE MASTER

Now that NIST SP 800-53 has been identified as the master document, each of the other regulation documents must have their security controls mapped to the controls in 800-53. In the above example, the four controls were mapped to IA-2 in 800-53. An astute reader can notice that some of the controls in Table 1 were more complex than others and thus would not be fulfilled by IA-2 alone. Some controls will map to multiple controls in the 800-53 document in order to meet the requirements. The key, however, to streamlining every regulatory document onto a common playing field is mapping every control to the necessary controls in 800-53. At the end of the mapping process, the original regulatory documents can be set aside and IT firms can simply work from the new, mapped document.

Initially this seems like a daunting task. Each regulatory document must be thoroughly read, understood, and have each control mapped to the corresponding control, or controls, in the master document. The good news is that the majority of the work has already been completed: most regulatory documents have sections dedicated to the mapping of their particular controls to the controls in NIST SP 800-53. Those documents that do not have a dedicated section usually have some other way of achieving the mapping without the need for an IT firm employee to sift through hundreds of pages and spending weeks

of time manually completing the mapping. This is evident with HIPAA, where the regulatory document itself makes no mention of mapping to NIST SP 800-53; however, the NIST has released SP 800-66, which contains more specific information on how to implement HIPAA, including a mapping of HIPAA security controls to 800-53 security controls. Table 2 details some of the aforementioned regulations and the specific location in their documents where the 800-53 mapping can be found, or other instructions when it cannot be found.

Table 2. *Mapping regulations to NIST SP 800-53*

Regulation	Location of NIST SP 800-53 Mapping (* denotes separate document)
NIST 800-171	NIST SP 800-171 Appendix D (Mapping) & Appendix E (Tailoring)
HIPAA	NIST SP 800-66 Appendix D (Crosswalk)*
IRS 1075	IRS Publication 1075 Section 9.3 (NIST SP 800-53 Control Requirements)
FBI CJIS	FBI Security Control Mapping of CJIS Security Policy*
PCI DSS	Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1*

While most of the tedious work has been completed, it is important to note that the mapping is not yet finished. NIST SP 800-53 does not contain everything necessary to completely fulfill the requirements of each and every regulation from all industries. The 800-53 document was written for federal organizations. The requirements of federal organizations differ from those of medical organizations, financial organizations, etc. While the core security requirements might be the same, such as the need for passwords, screensavers, encryption, etc., other requirements might differ wildly. One example of this is in cyber incident reporting. Table 3 lists some of the specific requirements organizations must follow when they have detected a breach.

Table 3. *Breach reporting requirements*

Regulation	Summarized Breach Reporting Requirements
NIST 800-171	Report the breach to DIBNet within 72 hours and preserve all associated systems/data for 90 days
HIPAA	If less than 500 patients were affected, notify HHS within 60 days after the calendar year in which the breach occurred. If more than 500 patients were affected, notify HHS within 60 days of the breach and notify media outlets (typically via press release). In both cases, individual notice must be sent to all affected patients.
IRS 1075	Within 24 hours of a possible breach, contact the Treasury Inspector General for Tax Administration and the IRS Office of Safeguards with the applicable incident information.
FBI CJIS	Complete and send the FBI CJIS breach reporting form to the FBI CJIS Division ISO via both email and USPS Certified Mail.

It is clear from Table 3 that while all industries have requirements to report breaches, they differ significantly in their scope and timeframe. These reporting requirements typically map to IR-6 from NIST SP 800-53; however, the text of IR-6, as is the case with most controls, is extremely general (see Figure 2).

IR-6 INCIDENT REPORTING

Control: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time period*]; and

b. Reports security incident information to [*Assignment: organization-defined authorities*].

Figure 2. IR-6 security control showing extremely general wording (SP 800-53r4, 2013).

Due to these instances where the text in 800-53 leaves much to the will of the specific organization or the requirements imposed upon said organization from other regulatory bodies, the process of mapping all regulatory documents to the 800-53 controls is not an easy one despite having much of the actual mapping previously completed. A simple spreadsheet that lists the requirements of each regulation and the matching security control from 800-53 will not suffice due to the large number of controls that need edited to include specific text, such as in IR-6. The only way for the IT firm to have a single master database of security controls that can be used to keep multiple organizations in compliance that deal with multiple regulatory bodies is to create a literal database.

Figure 3 depicts one of the queries from this database. The database contains a table for each regulation with a single column: the list of controls that link to the master table. The master table (800-53) contains four columns: the control ID, the control name, the summarized text of the control that has been edited to reflect all necessary requirements in a single location, and a suggested implementation procedure that details how organizations can meet the particular control (e.g., specific Group Policy settings, additional paper log sheets that need created/used, etc.). The suggested implementation is comprised of industry best practices combined with the expert judgement (Holm, et al., 2014) of the IT firm's cyber personnel to produce an implementation that meets the regulation while managing cost to the client. The IT firm can simply run the query for the specific regulation they need and receive a complete list of all applicable controls and implementation text required to fully comply with the regulation. This makes the life of the cyber personnel much easier when it is time to complete a Security Controls Assessment (SCA) for an organization.

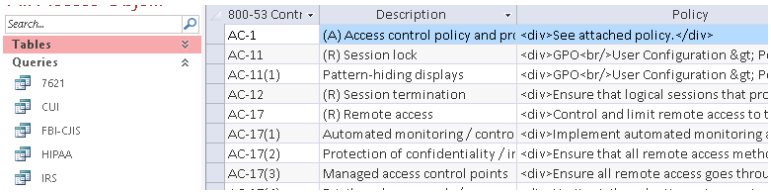


Figure 3. Snippet of the CUI query from the master database.

MANAGING THE SCA

Now that a complete database is available with all required information, the last phase of this process is to actually conduct a SCA for an organization. A SCA may be conventionally understood as an audit, where an organization's network is documented in order to determine its level of compliance. Nothing on the network is altered, or remediated, during a SCA. It is simply a read-only assessment.

In order to conduct a SCA, the complete list of controls, policies, and implementations must be exported from the database into some format that can be used as a checklist. For the IT firm, SCAs are being performed for multiple clients. Using the master database as the documentation/storage repository as well does not make sense. As seen in Figure 4, the completing of a SCA requires the collection of much more information than the master database was designed to hold; therefore, the master database will remain just that, the master copy of security controls. Those controls will need to be exported out of the database and imported into a system that can keep track of separate SCAs for separate clients.

Figure 4 shows a single security control, AC-11, in the documentation system for a specific client. It is apparent that the first few items (800-53 Control, Description, Policy, and Implementation) came from the database export while the remaining fields are specific to the documentation system so that each individual security control can be properly documented. Minimally, each security control will have a status, the date the status was last verified, and an attached artifact with proof of the security control being properly implemented (in the case of AC-11, this proof would be screenshots of the GPO being applied to the entire domain). In the case where an organization does not properly implement a control, there is an additional field where the auditor can list the security gaps, or the specific ways in which the organization does not meet the particular control.

At the end of a SCA, all of this data can be turned into a single report showing the client how their organization fared. This document serves two purposes: it is a complete list of every deficiency that needs to be remediated in order for their network to become fully compliant and it is a document that can be given to the regulatory bodies when proof of compliance is

requested. It is typical for clients to want their reports to list zero deficiencies, so, if approved, the IT firm can use this document to plan and begin work on the client's network in order to achieve full compliance.

Figure 4. Snippet of a single security control in the documentation system.

LIMITATIONS AND FUTURE RESEARCH

While this method had worked for the IT firm for many years, changes are on the horizon. In mid- to late-2020, the Department of Defense (DoD) is planning to alter the cyber security requirements for government contractors handling CUI. Until now, such organizations were bound by DFARS 252.204-7012, which required compliance with NIST SP 800-171 ("Safeguarding", 2016, (b)(2)(i)). By the end of 2020 the DoD is set to move away from 800-171 in favor of a new set of requirements, built upon an update to the original requirements noted 800-171B ("Regulatory Update", 2019), called the Cybersecurity Maturity Model Certification (CMMC), which can be better tailored to suit the level of sensitivity of the data processed by an organization. The CMMC is not a single set of requirements like its predecessor, it is a 5-tier behemoth, depicted in Figure 5.

Level 1 of the CMMC is a tiny set of security controls that every business should have implemented, Level 3 is approximately a full implementation of 800-171, and Levels 4 and 5 add extra controls onto those found in 800-171 to reach a level of cyber hygiene worthy to protect our nation's most sensitive data, including such requirements as a 24x7 Security Operations Center (SOC), regular department staff to perform penetration testing and threat hunting, and custom practical/scenario-based security awareness exercises to ensure all employees are properly trained.

The key to this shift is that many of the security requirements above CMMC Level 3 are brand new and not found in the current NIST SP 800-53. The method of cyber security management described in this paper will need to be altered to account for security requirements not in the master database. Although such a change should be trivial given the flexible nature of the database and process, time and care need to be given in order to properly assimilate the new controls after the CMMC is finalized.

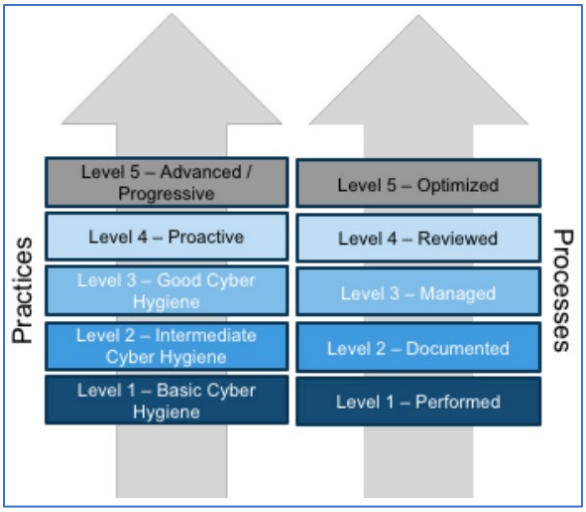


Figure 5. Diagram of the five CMMC tiers ("Cybersecurity Maturity", 2019, p. 5).

CONCLUSION

What started as an IT firm trying to assist their clients with basic cyber security needs turned into an exercise in enterprise-level cyber security management that spanned multiple business sectors. This method has benefited the IT firm for many years, helping them achieve compliance for their various clients, including small government contractors, large government contractors, medium-sized hospitals, and various financial institutions. Although the future offers unknown change with the inception of the CMMC, the method described in this paper is a significant contribution to industry practice and has proven itself flexible and capable of incorporating one more set of cyber security regulations to remain useful for years to come. However, as Miedema (2018) among many others stress, involving the consumer in the cyber security strategy process is necessary if these laws and regulations are to be beneficial. Humans are considered the weakest link when it comes to cyber security due to organizations spending more money protecting computers than training and protecting employees (Spitzner, 2018). Most cyber security regulations include various controls pertaining to employee training and awareness. If those controls are implemented to their fullest extent (and not only the minimum necessary to pass an audit) as part of this paper's cyber security strategy, an organization will be well on its way to proper cyber hygiene.

REFERENCES

Arlitsch, K. & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration, 54*(1), 46-56.

Criminal Justice Information Services (CJIS) Security Policy Version 5.8, Federal Bureau of Investigation Criminal Justice Information Services Division, U.S. Department of Justice: Washington, D.C. (June 2019).

Cybersecurity Maturity Model Certification (CMMC) Version 0.7, Carnegie Mellon University and Johns Hopkins University Applied Physics Laboratory LLC. (December 2019).

Dittman v. UPMC, 43 WAP (Penn. Sup. Ct. 2017).

Dutta, A. & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Edelman, B. (2019). How to prepare for cyber threats in 2019. *Journal of Financial Planning, 32*(4), 26.

HIPAA Administrative Simplification Regulation Text, U.S. Department of Health and Human Services Office for Civil Rights: Washington, D.C. (March 2013).

Holm, H., Sommestad, T., Ekstedt, M., & Honeth, N. (2013). Indicators of expert judgement and their significance: An empirical investigation in the area of cyber security. *Expert Systems, 31*(4), 299-318.

Ibrahim, A., Valli, C., McAteer, I., & Chaundry, J. (2018). A security review of local government using NIST CSF: A case study. *The Journal of Supercomputing, 74*(10), 5171-5186.

Jenab, K. & Moslehpour, S. (2016). Cyber security management: A review. *Business Management Dynamics, 5*(11), 16-39.

Kovacs, L. (2018). National cyber security as the cornerstone of national security. *Revista Academiel Fortelor Terestre, 23*(2), 113-120.

Krishan, R. (2018). Corporate solutions to minimize expenses from cyber security attacks in the United States. *Journal of Internet Law, 21*(11), 16-19.

Lee, S. & Kang, T. (2015). Adaptive multi-layer security approach for cyber defense. *Journal of Internet Computing and Services, 16*(5), 1-9.

Miedema, T. E. (2018). Engaging consumers in cyber security. *Journal of Internet Law, 21*(8), 3-15.

Regulatory Update. *Journal of Internet Law, 23*(1), 9-11.

Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, Internal Revenue Service: Washington, D.C. (September 2016).

Safeguarding covered defense information and cyber incident reporting, 48 CFR § 252.204-7012 (2016).

Shelhart, M. (2018, November). Why cyberdefenses are worth the cost. *Journal of Accountancy,* 1-8.

SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, U.S. Department of Commerce: Gaithersburg, MD (April 2013).

SP 800-171r1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, National Institute of Standards and Technology, U.S. Department of Commerce: Gaithersburg, MD (December 2016).

Spitzner, L. (2018). *This is why the human is the weakest link.* SANS Security Awareness. https://www.sans.org/security-awareness-training/blog/why-human-weakest-link.