Organization Security Controls for Effective Cyber Defense

Anne Kohnke, PhD
Assistant Professor

Lawrence Technological University
21000 West Ten Mile Road
Southfield, MI 48075
akohnke@comcast.net

Abstract - Even the most technically savvy organizations cannot stop hackers and the risk of poorly implemented IT security controls can be devastating. Technical solutions need to work in harmony with formal security controls, informal organizational culture, and the overriding mission and goals of the organization. With the exponential growth of security breaches and the increasing dependency on external business partners to achieve organizational success, the effective use of enterprise-wide frameworks and implementation of integrated security controls are critical in order to mitigate data theft. Surprisingly, many organizations do not have formal processes or policies to protect their assets from internal or external threats. This paper gives an overview of why an organization should consider using, or tightening up their organizational security controls, an overview of the most widely used frameworks, and a comparative discussion of the various IT security frameworks to assist managers in assessing their own IT security efforts.

Keywords*: cybersecurity, IT governance, enterprise security frameworks, security controls, risk management*

INTRODUCTION

C-level suite executive emails should never be made available for public consumption. The recent humiliation of Sony Pictures Entertainment's executives may have many corporate executives reflecting before they craft another email or seriously inquiring into the security of their own corporate security controls. The Sony security breach included not only thousands of emails but documents that

included US Social Security numbers, personal information, copies of passports, salaries and home addresses of current and former employees, contracts, termination dates and reasons with additional sensitive information—nearly all stored in Microsoft Excel files with no password protection (Fritz, 2014; Dipietro, 2014). And the financial devastation has yet to be calculated for the films not yet officially released that were leaked online or lacking distributors. After the attack, Sony shut down its network for more than a week (Clark & Olivarez-Giles, 2014). The hackers were after much more than credit cards as in the security breaches of Home Depot, Target, JP Morgan Chase, and Pf Changs—they threatened to reveal additional information if their demands were not met (Seals, 2014). This escalates IT data security hacking to a new level.

Firewalls and perimeter security are not enough. Technical solutions need to work in harmony with formal security controls, informal organizational culture, and the overriding mission and goals of the organization (LeVeque, 2006). If sensitive data is found on multiple devices it increases the opportunities for hackers to steal information. And the demand on organizations to allow employees to use their own devices such as smartphones, iPads, tablets, etc., not only increases the opportunity for a breach but also adds to the complexity of the IT security requirements. Effective information security requires employees to comply with established security policies and procedures (ISACA, 2012; Kim & Solomon, 2014). As a former Chief Information Security Officer, I have often observed that employees follow their day-to-day routines and habits and resist the behavioral changes required to abide by security policies and procedures. In more than 1,300 data breaches and 63,400 security incidents in 95 countries, a 2014 Data Breach Investigations Report found basic lapses at the heart of many of them such as employee mistakes, the use of weak and default passwords, system configuration issues, and inadequate system monitoring (Verizon, 2014). Based on actual data breaches versus self-reporting surveys that can be unreliable, the Data Breach Investigations Report gives an accurate picture of cyber-crime activity. Although corporate espionage is on the rise, employee negligence and posting non-public information to a public resource are the second most frequently occurring computer security incidents behind virus and malware infections. And although the internal

employees cited in the report were end-users, sysadmins, and developers, a significant number of incidents were caused by partner errors.

With the exponential growth of security breaches and the increasing dependency on external business partners to achieve organizational success, the effective use of enterprise-wide frameworks and implementation of integrated security controls are critical in order to mitigate data theft (Berson & Dubov, 2011; Davis & Schiller, 2011; ISACA, 2012). It is also important that organizations are structured and staffed with the appropriate roles and responsibilities to ensure risk assessment, risk mitigation, and the implementation of security controls are effective (Shoemaker & Conklin, 2012). This paper gives an overview of why an organization should consider using, or tightening up their organizational security controls, an overview of the most widely used IT security frameworks, and a comparative discussion of the various frameworks to assist managers in assessing their own IT security efforts.

THE NECESSITY OF ORGANIZATIONAL SECURITY CONTROLS

Even the most technically savvy organizations cannot stop hackers and the risk of poorly implemented IT security controls can be devastating (Tarala, 2013). Between April and when Home Depot finally noticed in September 2014, hackers stole 56 million credit card numbers and 53 million email addresses. Contact information for 76 million households and 7 million small businesses were hacked from JPMorgan and personal information on 110 million plus 40 million credit and debit cards from Target shoppers were also stolen. Organizations are experiencing an array of security issues from denial of service (DOS) attacks to web application attacks and from cyber espionage to insider threats (Verizon, 2014). Any part of a computing system whether it be hardware, software, storage media, data, and people can be the target of a crime and any system is most vulnerable at its weakest point (Pfleeger & Pfleeger, 2007).

Of the 100,000 security incidents that were analyzed from data collected during the last 10 years, the Data Breach Report identified nine distinct attack patterns that vary according to industry (Verizon, 2014). The nine patters were: point-of-sale

intrusions, web application attacks, insider misuse, physical theft, miscellaneous errors (sending confidential emails to the wrong recipient), malware, payment card skimmers, cyber espionage, and DOS attacks. In order to protect information, organizations need to implement rules and controls around the protection of sensitive data, intellectual property, and the systems that store and process the information. Surprisingly, many organizations do not have formal processes or policies to protect their assets from internal or external threats (Whitman, Mattord, and Green, 2014). Establishing and running an IT security program can be challenging as there are numerous areas to address—from application security, to encryption, to disaster recovery. Additionally, there are regulatory requirements such as PCI DSS, Sarbanes-Oxley, and HIPAA that add a layer of complexity. For an IT security system to be effective and add value, a well-defined organization-wide security framework needs to be incorporated that involves all levels of the organizational structure and fine-tuned over time (Davis & Schiller, 2011; Whitman, Mattord, and Green, 2014).

IT GOVERNANCE FRAMEWORKS – AN OVERVIEW

An enterprise security framework is an overarching structure that identifies interlinked key elements, which collectively contribute to a consistent approach to managing risk. The interlinked key elements or principles often include processes to identify the current state of the organization, levels of risk the organization is willing to accept, security requirements, priorities, strategic goals and mission, resource availability and competencies, compliance, security controls, implementation of security controls, best practices, authorization levels, assessment, financial budgets and costs, governance, disaster recovery, and ongoing monitoring. From a holistic perspective, the absence of a planned approach can result in a rather piecemeal approach or a series of reactionary implementations to satisfy those in the organization whom have the loudest voice. The following is an overview of most widely-used enterprise security frameworks.

COSO

The *Foreign Corrupt Practices Act of 1977* (FCPA) made bribery illegal in foreign countries and was the first regulation requiring organizations to implement internal control initiatives and keep extensive records of transactions for disclosure purposes. With the collapse of the savings and loan industry in the mid 1980's, the demand for governmental oversight of accounting standards and the auditing profession paved the way for the creation of formal standards and frameworks. In an attempt to avoid governmental intervention, five private accounting organizations created the Committee of Sponsoring Organizations (COSO) and funded the *National Commission on Fraudulent Financial Reporting* (also known as the *Treadway Commission*, named after the chairman) in 1985. COSO is credited with formalizing the concepts of *internal control* and *framework*. Their aim was to improve the quality of financial reporting and issued a comprehensive guideline called *Internal Control-Integrated Framework* in 1992. By establishing a common definition for *internal control* and a framework, the intention was that public companies could self-regulate and apply the voluntary industry guidelines and thus avoid the need for governmental regulation. They viewed internal control as a *process* designed to provide effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations (COSO, 2004). Figure 1 below shows the updated *COSO Enterprise Risk Management—Integrated Framework (2004)*.

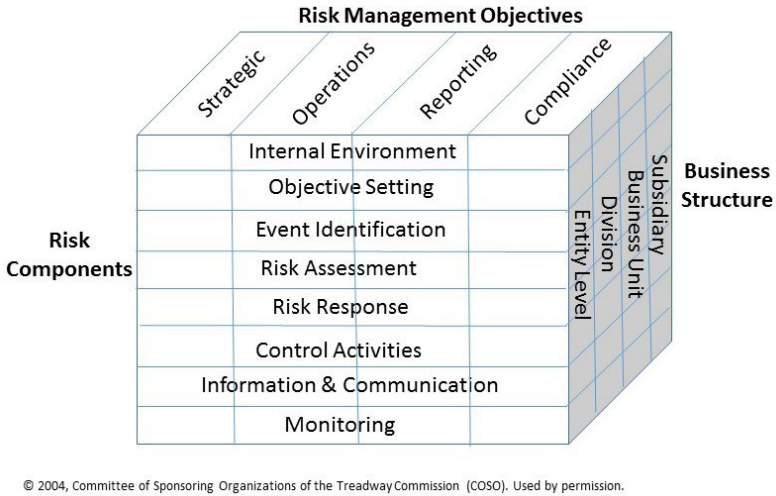

Figure 1. The COSO Enterprise Risk Management—Integrated Framework.

This framework has been updated from the original cube to emphasize the importance of identifying and managing risks across the enterprise (COSO, 2004). The new COSO framework consists of eight components:

1) *Internal control environment* - sets the tone of an organization providing discipline and structure on how risk is viewed and addressed.

2) *Objective setting* - the chosen objectives must support and align with the organization's mission and are consistent with its risk appetite

3) *Event identification* - all events that impact the achievement of an organization's objectives must be identified and distinguished between risks and opportunities.

4) *Risk assessment* - risks are analyzed as a basis for determining how they should be managed.

5) *Risk response* - management defines risk responses and develops a set of actions to align risks with the organization's risk tolerances.

6) *Control activities* - policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

7) *Information and communication* - relevant information is communicated in a form and timeframe that enable people to carry out their responsibilities.

8) *Monitoring* - the enterprise risk management is monitored and modified as necessary and accomplished through ongoing management activities and/or separate evaluations.

Due to widespread reliance on information systems, COSO introduced controls for IT and classified them into to broad groupings: 1) *General computer controls* to include controls over IT management, infrastructure, security management, software acquisition, development, and maintenance and 2) *Application controls* (Singleton, 2007).

ITIL

Also in the mid-1980's, the UK Government's Central Computer and Telecommunications Agency developed its own set of recommendations to address the growing dependence on IT. The UK government recognized that "utilizing consistent practices for all aspects of an IT service lifecycle could assist in driving organizational effectiveness and efficiency, as well as achieving predictable service levels" (Arraj, 2013, p. 3). Originally called the *IT Infrastructure Library*, the ITIL as it is now called, originated as a collection of books, each covering a specific practice within IT management. ITIL V3 was published in 2007 with updates made in 2011. Although a substantial amount of content has been added to ITIL 2011, no entirely new concepts were added. Figure 2 shows the ITIL 2011 lifecycle and its components:

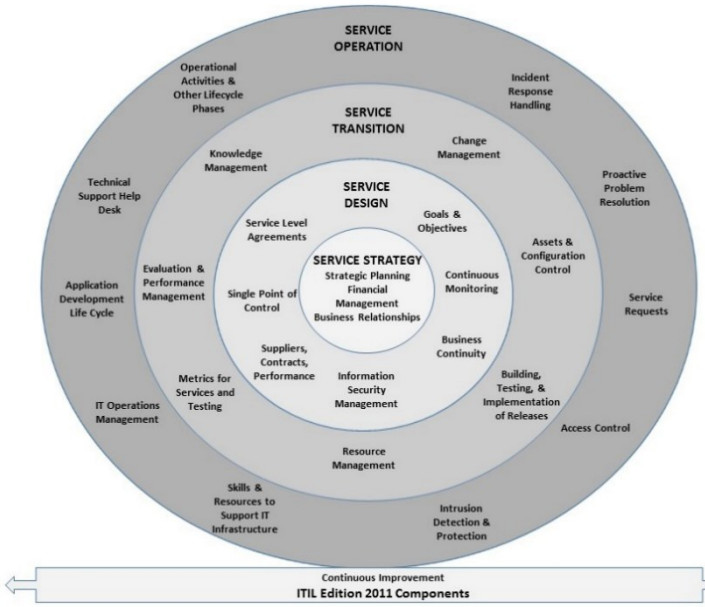

Figure 2. ITIL Edition 2011 Components.

ITIL 2011 is organized around a *service lifecycle* which includes service strategy, service design, service transition, service operation, and continual service improvement. ITIL 2011 can be adapted and used in conjunction with other frameworks such as COBIT and ISO 27000.

ISO 27001

The International Organization for Standardization (ISO) officially began in 1947 and is an independent, non-governmental membership organization. The ISO 27001 is the international standard that describes best practices for an information security management system (ISMS). First published in mid-1990 as a code of practice, the British Standard 7799-2, as it was called, morphed into ISO Standard 17799 by December 2000. The standard was updated in 2005 [ISO 27002:2005] and emphasized a model to structure the processes called PDCA, *Plan-Do-Check-Act*. The latest version was jointly published in 2013 with the *International Electrotechnical Commission* (IEC) and no longer emphasizes the PDCA model. The

ISO/IEC 27002:2013 standard focuses more on measuring and evaluating how well the organization's overall ISMS is performing and has added a section on outsourcing and new controls to reflect changes in technology such as cloud computing. The updated standard now includes 14 groups that have 114 controls, the previous standard had 11 groups with 133 controls (ISO/IEC, 2013). Figure 5 below shows the ISO/IEC 27001 & 27002:2013 framework components with the 14 groups of control objectives.

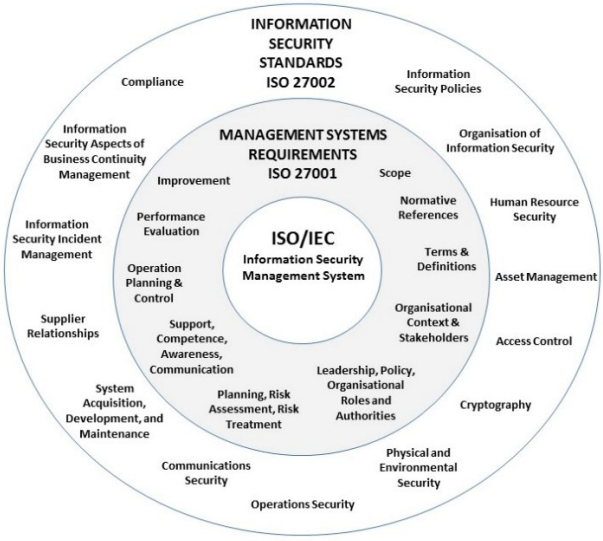

Figure 5. The ISO/IEC 27001 & 27002:2013 Components

The comprehensive group of control objectives focus more on the organizational context of information security and how an organization can respond to risks by choosing the appropriate controls. Annex A of the Requirements lists the following control groups (ISO/IEC, 2013):

1) A.5: Information security policies (2 controls)

2) A.6: Organization of information security (7 controls)

3) A.7: Human resource security - 6 controls that are applied before, during, or after employment

4) A.8: Asset management (10 controls)

5) A.9: Access control (14 controls)

6) A.10: Cryptography (2 controls)

7) A.11: Physical and environmental security (15 controls)

8) A.12: Operations security (14 controls)

9) A.13: Communications security (7 controls)

10) A.14: System acquisition, development and maintenance (13 controls)

11) A.15: Supplier relationships (5 controls)

12) A.16: Information security incident management (7 controls)

13) A.17: Information security aspects of business continuity management (4 controls)

14) A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

COBIT 5

In 1998, the *IT Governance Institute* (ITGI) was formed by the *Information Systems Audit and Control Association* (ISACA) as a nonprofit, independent research entity to advance international thinking on governance and management of enterprise IT. ITGI developed COBIT, *Control Objectives for Information and Related Technology*, the foremost internationally recognized framework for IT governance and control. COBIT 5, released in 2012, provides a comprehensive framework to "help enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resources use" (ISACA, 2012, p. 13). Figure 3 below shows the five key principles for governance and management of enterprise IT:

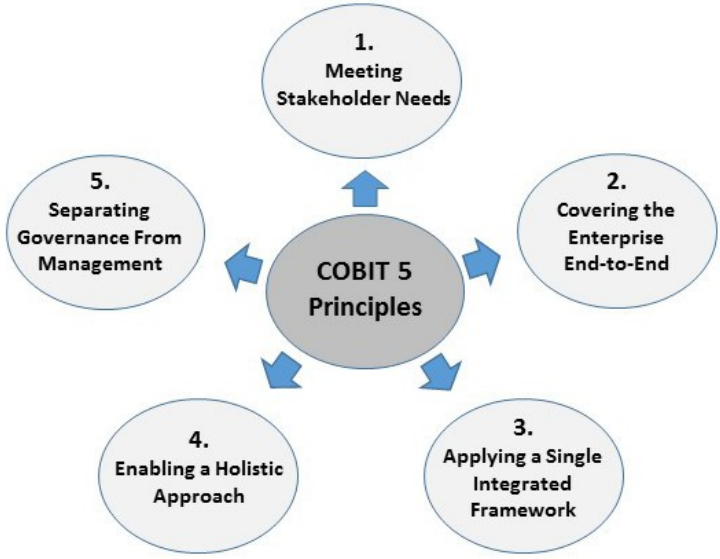

Figure 3. COBIT 5 framework for governance and management of enterprise IT.

The COBIT 5 framework consists of the following five key principles (ISACA, 2012):

1) *Meeting Stakeholder Needs* - the governance system should consider all stakeholders and the enterprise goals for IT are used to formalize and structure the stakeholder needs.

2) *Covering the Enterprise End-to-end* - covers all functions and processes within the enterprise and is inclusive of everything and everyone that is relevant to governance and management of IT.

3) *Applying a Single, Integrated Framework* - aligns with other latest relevant standards and frameworks.

4) *Enabling a Holistic Approach* - identifies seven categories of enablers to include principles, policies, and frameworks; processes; organizational structures;

culture, ethics, and behaviour; information; services, infrastructure, and applications; and people, skills, and competencies.

5) *Separating Governance from Management* - provides a clear distinction between these two disciplines.

The COBIT 5 includes a *process reference model*, representing all of the IT processes normally found in an enterprise and designed to be understandable to operational IT and business managers (ISACA, 2012). Figure 4 below shows the COBIT 5 *Process Reference Model*.

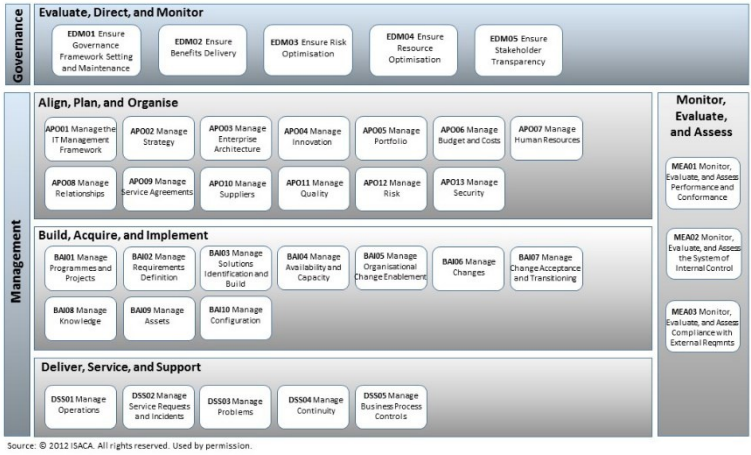

Figure 4. COBIT 5 Process for Governance of Enterprise IT, Process Reference Model.

The COBIT model above divides the governance and management processes of enterprise IT into two main process domains:

1) *Governance* - five processes (at the top of the model) include evaluate, direct, and monitor

2) *Management* - four domains (in blue) include align, plan and organize (APO); build acquire and implement (BAI); deliver, service, and support (DSS); and monitor, evaluate, and assess (MEA). These domains are an evolution of the

COBIT 4.1 process structure and include the Risk IT and Val IT process models as well.

NIST

Founded in 1901, the *National Institute of Standards and Technology* (NIST) is a non-regulatory agency, possessing one of the nation's oldest physical science laboratories, whose mission is to increase the visibility and competitiveness of U.S. innovation by advancing measurement science, standards, and technology. NIST has created standards and controls for numerous disciplines most notably the 800-53 Security and Privacy Controls (NIST SP, 2013). The 800-53 provides a catalogue of security and privacy controls and a process for selecting controls to protect organizational operations, assets, and individuals from hostile cyber-attacks, natural disasters, structural failures, and human errors (NIST SP, 2013). The security controls are designed to be technology-neutral and focus on the fundamental safeguards and countermeasures necessary to protect information during processing, at rest, and during transmission. The security controls are step 2 within the bigger picture of the *Risk Management Framework*. This framework addresses the "security concerns related to the design, development, implementation, operation, and disposal of information systems and environment in which those systems operate" and consists of the following six steps (NIST SP, 2013, p. 8).

1) *Categorize* the information system based on an impact assessment that can be found in FIPS Publication 199.

2) *Select* the applicable security control baseline—this is based on the results of the security categorization in step 1 and has three levels: low-impact, moderate-impact, and high-impact.

3) *Implement* the security controls and document the design, development, and implementation details for the controls.

4) *Assess* the security controls to determine if implemented correctly, operating as intended, and producing desired outcome.

5) *Authorize* information system operation based on determination of risk.

6) *Monitor* the security controls.

Figure 6 below is the Risk Management Framework and shows the various publications for detailed information for each step in the process:

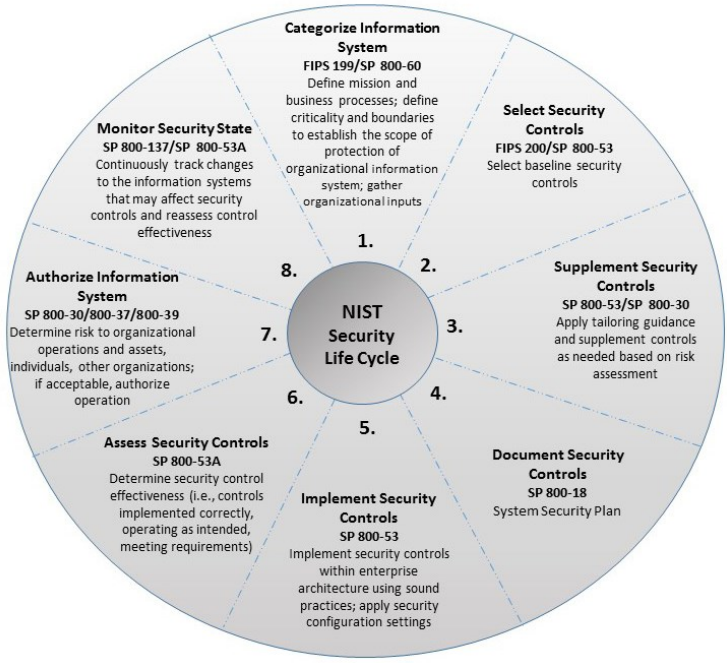

Figure 6. NIST Risk Management Life Cycle: Security Life Cycle

In February 2013, the President issued Executive Order 13636 entitled the *Framework for Improving Critical Infrastructure Cybersecurity* for the creation of a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure. The *Cybersecurity Framework* enables organizations to apply the principles and best practices of risk management to improving the structure and resilience of critical infrastructure regardless of size, degree of cybersecurity risk, or the level of cybersecurity sophistication that exists

within the organization (NIST, 2014). The framework is a risk-based approach and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each component is designed to consider the business drivers and connect them to cybersecurity activities (NIST, 2014). The components are as follows:

1) *Framework Core* - is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure. Consists of five concurrent and continuous functions (identify, protect, detect, respond, recover). When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cyber risk (NIST, 2014). It is not a checklist of actions but presents key cybersecurity outcomes that are identified by industry. The following, Figure 7, shows the four elements of the framework: Functions, Categories, Subcategories, and Informative References. The Category column can include logical groupings of controls such as access control, detection processes, etc. The Subcategory column can include information relevant to each category such as the activities performed to ensure each task within a category is addressed. The Informative References column can include the specific standards, guidelines, procedures, and/or controls that were created to address each subcategory.

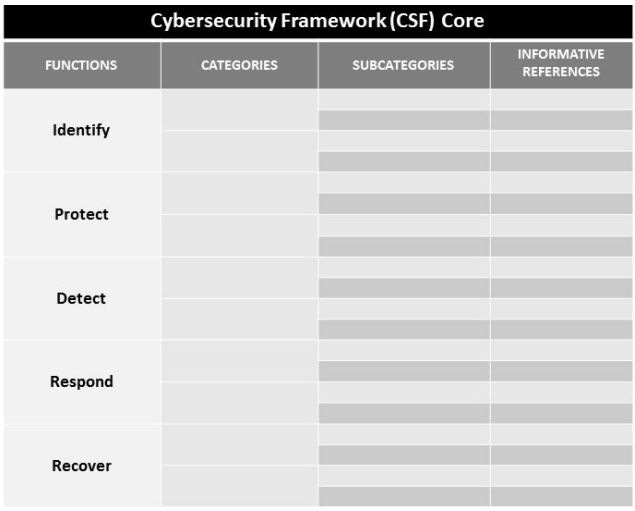

Figure 7: Framework Core Structure

2) *Framework Implementation Tiers* - provides the context on how the organization views risk and the processes in place to manage that risk (NIST, 2014). There are 4 tiers that are characterized by a range of increasing degree of rigor (Partial, Risk Informed, Repeatable, and Adaptive).

3) *Framework Profiles* - represents the outcomes based on business needs and alignment of standards, guidelines, and practices to the Framework Core. Current profiles that represent 'as is' states can be helpful in identifying opportunities to improve rigor and possibly increase to a higher Tier (NIST, 2014).

The goal of the Framework is to provide a common language to increase understanding and assist in the management of both internal and external cybersecurity risks. It can be used to help prioritize cybersecurity risk activities, and to align policy, business, and technological approaches to managing that risk.

SANS INSTITUTE

In 1989, the SANS Institute was founded as a private research and education organization that specializes in training information security professionals on a variety of topics to include cyber and network defenses, incident response, digital forensics, penetration testing, and audit. In 2006, SANS established the SANS Technology Institute which is a graduate school focusing exclusively on cybersecurity. The SANS Institute readily makes available numerous CIS security configuration benchmarks, assessment tools, and security metrics definitions. Although not a framework, they are well known for their top 20 list of critical security controls which are updated and derived from the most common attack patterns and vetted across a broad community of government and industry (SANS, 2013). Originally the Critical Security Controls were recommendations created to provide a prioritized list of controls that would have the greatest impact in improving risk posture against real-world threats as opposed to a requirement framework that risked becoming an exercise in reporting on compliance. The controls work in conjunction with NIST SP 800-53 and the NIST Cybersecurity Framework with the objective of focusing on a smaller number of immediate actionable controls with a high-payoff.

The six widely-used frameworks in this overview (COSO Enterprise Risk Management—Integrated Framework, COBIT 5, ITIL 2011, ISO 27001, NIST 800-53 and NIST Cybersecurity Framework) cover a variety of principles and key elements with the objective of guiding an organization through a consistent approach to managing their cybersecurity risk. There are pros and cons to the various frameworks which will be discussed in the next section.

DISCUSSION

With the advent of web-enabled technologies, outsourcing to strategic partners, and distributed networking, businesses are moving away from a closed business model to a more open model. Managing and protecting the organization's assets has become increasingly complex and the expectation to deliver secure IT solutions can be costly. Many organizations must now comply with regulatory agencies and

laws and prove compliance with either process certifications or risk not being able to compete for new business. IT governance and risk management processes help IT professionals navigate the myriad aspects of corporate cybersecurity. The proliferation of standards, policies, controls, best practices such as COBIT, ITIL, ISO 27001, and NIST create great challenges for organizations to understand these frameworks.

Although COBIT has become a widely-used IT control and governance framework, there are few research studies in the academic literature investigating the utilization of COBIT. Several researchers have noted that one of the biggest disadvantage with COBIT is that it requires a great deal of knowledge to understand the framework before it could be applied as a tool (Simmonsson, Johnson, and Wijkstrom, 2007; Van Grembergen & DeHaes, 2005). There are 37 governance and management processes within COBIT 5 and includes a life cycle, maturity model, process reference model, and a process capability model and does require a level of sophistication and knowledge to navigate through all the details. This comprehensive framework and accompanying tools provide a great deal of guidance but will require a team of professionals dedicated to managing all aspects of corporate risk and corporate sponsorship at the top level of the organization. The COBIT framework can work well in large organizations with the right staff who are trained and knowledgeable.

Business process management has been well researched in the IT academic discipline and makes a clear distinction between a *function* and a *process* (Jeston & Nelis, 2006; Harmon, 2003; Rummler & Brache, 1995; Sharp & McDermott, 2009). Although the ITIL framework provides a more holistic perspective on the full life cycle of services, from a true business process perspective, its design confuses processes with functions (Betz, 2001). A general view of ITIL implementation is that it is a demanding activity in need of substantial dedicated resources (Iden & Eikebrokk, 2014). The ITIL philosophy often requires organizations to change their culture in order to embrace the new processes. In a cross-case analysis of four organizations adopting ITIL, researchers found that "*executive support* was unanimously identified as the most important factor, coupled with ITIL training

and staff awareness to gain buy-in across all stakeholders" (Pollard & Cater-Steel, 2009, p. 170).

Many organizations are required to comply with multiple regulations that may have overlapping and conflicting requirements. One advantage of the 2013 NIST Cybersecurity Framework is the attempt to develop controls in one standard format eliminating the need for multiple security compliance documents. After successfully completing a NIST certification process, I have found the NIST frameworks to be very comprehensive requiring extensive knowledge of technical, operational, and management controls and also requiring significant man-hours to achieve certification status. In some cases, organizations have no choice but to use this framework if they want to do business with government entities. The *Patient Protection Affordable Care Act* of 2009 also stipulates that health systems who accept Medicare will have reporting requirements relating to the "meaningful use of electronic health records" and will all at some point be subjected to an audit by the NIST agency (Patient Protection and Affordable Care Act, 2009, p.647). For smaller organizations who are not looking to become certified, the NIST framework can certainly be adapted to smaller businesses and offer a comprehensive list of controls that can be tailored to fit the environment. They provide detailed documentation to assist in understanding each control area with three levels of risk tolerance baselines.

The objective of the international ISO 27001 certification is to ensure that there are adequate confidentiality, integrity, and availability controls in place and some organizations require certification to ISO 27001 as a prerequisite for doing business. ISO 27001 is as comprehensive as the NIST framework and after achieving initial certification, organizations must constantly monitor and make changes as necessary to stay in compliance. If an organization chooses to use the ISO framework they may gain a competitive advantage once they achieve certification as compliance to this standard demonstrates credibility and trust, provides confidence to stakeholders, and shows a commitment that the organization is willing to invest considerable time and effort to safeguard information.

CONCLUSION

Cybersecurity must be addressed as a significant concern since it mitigates business risks and allows for the smooth functioning of daily activities in order for organizations to achieve their strategic goals and carry out their mission. For every organization, senior managers must make the critical decisions as to how much risk they are willing to tolerate and to decide the appropriate security levels. Additionally, they must understand the financial implications of cybersecurity implementation efforts and weigh the risks in relation to the value of assets. With the numerous IT security standards and guidelines that currently exist, they must also determine the ideal approach that addresses regulation and compliance issues, boost performance results, and represent a high level of security for the investment.

Every IT environment is unique in that the organizational culture, strategic goals and mission, and knowledge, wisdom, and availability of resources all impact the ultimate decisions that managers must make to manage risk. With the rise in cybersecurity breaches and increase in corporate espionage, organizations cannot afford to take a piecemeal or reactionary approach to protecting their critical systems and information. The use of a comprehensive framework which may certainly transform the organization in many ways may require dedicated professionals and increased costs but cannot compare to the costs of lost reputation and the humiliation of the inner workings of the organization exposed to public ridicule, not to mention the costs of certain litigation.

REFERENCES

[1] Arraj, V. (2013*) ITIL: The basics*. A Compliance Process Partners White paper. Retrieved from www.axelos.com

[2] Berson, A. & Dubov, L. (2011). *Master data management and data governance*, 2nd ed. New York: McGraw-Hill

[3] Betz, C.T. (2011). ITIL, COBIT, and CMMI: *Ongoing confusion of process and function*. Retrieved from www.bptrends.com

[4] Clark, D. & Olivarez-Giles, N. (2014, December 27). Hackers hit Sony, Microsoft videogame services. *The Wall Street Journal, Tech*. Retrieved from www.wsj.com

[5] COSO, Committee of Sponsoring Organizations. (2004). *Enterprise Risk Management Framework Reference Copy*. Retrieved from www.coso.org

[6] Davis C. & Schiller, M. (2011). *IT auditing: Using controls to protect information assets*, 2nd Ed. New York: McGraw-Hill

[7] Dipietro, B. (2014, December 22). Crisis of the week: Sony's bad "Interview". *The Wall Street Risk & Compliance Journal*. Retrieved from blogs.wsj.com/riskandcompliance/

[8] Fritz, B. (2014, December 11). Hack of Amy Pascal emails at Sony Pictures stuns industry: Daily messages of studio head leaked. *The Wall Street Journal*. Retrieved from http://www.wsj.com

[9] Harmon, P. (2003). *Business process change: A manager's guide to improving, redesigning, and automating processes*. San Francisco, CA: Morgan Kaufmann Publishers.

[10] Iden, J., & Eikebrokk, T.R. (2014). Using the ITIL process reference model for realizing IT governance: An empirical investigation. *Information Systems Management*, 31, p. 37-58.

[11] ISACA. (2012). COBIT 5: *A business framework for the governance and management of enterprise IT*. Rolling Meadows, IL: ISACA

[12] ISO/IEC. (2013). *Information security management systems: Requirements*. Geneva, Switzerland: ISO/IEC. Retrieved from www.iso.org

[13] Jeston, J. & Nelis, J. (2006). *Business process management: Practical guidelines to successful implementations*. New York, NY: Routledge.

[14] Kim, D. & Solomon, M.G. (2014). *Fundamentals of information systems security*. Burlington, MA: Jones & Bartlett Learning

[15] LeVeque, V. (2006). *Information security: A strategic approach*. Hoboken, New Jersey: Wiley & Sons, Inc.

[16] NIST. (2014). *Executive Order 13636 of February 12, 2013: Framework for improving critical infrastructure cybersecurity*. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from www.nist.gov

[17] NIST SP. (2013). *NIST Special Publication 800-53 Revision 4: Security and privacy controls for federal information systems and organizations*. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from www.nist.gov

[18] Patient Protection and Affordable Care Act. (2009). Retrieved from www.hhs.gov

[19] Pfleeger, C.P. & Pfleeger, S.L. (2007). *Security in Computing*, 4th ed. Upper Saddle River, NJ: Prentice Hall.

[20] Pollard, C., & Cater-Steel, A. (2009). Justifications, strategies, and critical success factors in successful ITIL implementations in U.S. and Austrailan companies: An exploratory study. *Information Systems Management*, 26, p. 164-175.

[21] Rummler, G.A. & Brache, A.P. (1995). *Improving performance: How to manage the white space on the organization chart, 2nd ed*. San Francisco, CA: Jossey-Bass.

[22] SANS, (2013). *The critical security controls for effective cyber defense version 5*. Washington D.C.: Council on CyberSecurity. Retrieved from www.sans.org

[23] Seals, T. (2014, December 5). Sony hack's scope gets much, much worse. *Infosecurity Magazine*. Retrieved from www.infosecurity-magazine.com

[24] Sharp, A. & McDermott, P. (2009). *Workflow modeling: Tools for process improvement and applications development, 2nd ed*. Boston, MA: Artech House.

[25] Shoemaker, D. & Conklin, W.A. (2012). *Cybersecurity: The essential body of knowledge*. Boston, MA: Course Technology Cengage Learning.

[26] Simonsson, M., Johnson, P., & Wijkstrom, H. (2007). Model based IT governance maturity assessments with COBIT. *The 15th European Conference on Information Systems*. Switzerland.

[27] Singleton, T. (2007). The COSO model: How IT auditors can use it to evaluate the effectiveness of internal controls. *Information Systems Control Journal, Volume 6*. Retrieved from www.isaca.org

[28] Tarala, J. (2013). *Reducing risk through prevention: Implementing critical security controls 1 - 4*. A SANS Analyst Program Whitepaper. Retrieved from www.sans.org

[29] Van Grembergen, W., & DeHaes, S. (2005). Measuring and improving IT governance through the balanced scorecard. *Information Systems Control Journal (2)1*, p. 35-42.

[30] Verizon Enterprise Solutions. (2014). *Verizon Data Breach Investigations Report*. Retrieved from www.verizonenterprise.com/DBIR/2014/

[31] Whitman, M.E., Mattord, H.J., & Green, A. (2014). *Principles of Incident Response & Disaster Recovery, 2nd ed*. Boston, MA: Course Technology Cengage Learning.