Information Security Management Systems

Dietrich Lehr

lehrd12@students.ecu.edu

East Carolina University

ABSTRACT

Information has always been a vital part of any business. Today, information is shared globally in an instant and able to be accessed remotely. This has brought about the need for a method of ensuring that this information can be protected securely and unauthorized access and data loss is mitigated. There are several organizations in existence today that have sought to create a set of universal standards that can be tailored and applied to a company, regardless of size, in pursuit of information security. This paper will examine the International Organization for Standardization 27001 standard that exist today to assist companies in creating their own information security management systems. I will also examine digital commercial solutions that are designed to accelerate and automate the implementation of information security management systems used to secure information assets in the workplace.

As defined by the International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC), an “information security management system is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.”(ISO/IEC 27000 family) ISO/IEC has developed a set of standards that businesses, large or small, can use in order aid in managing assets securely. This issue is addressed by the 27000 family of standards, but this paper will focus primarily on ISO/IEC 27001 as it pertains directly to suggested requirements for implementing an information security management system. (ISO/IEC 27000 family)

ISO 27001 is one of the most well known standards when it comes to information security management systems and this framework enables a business to perform a security risk assessment based on common needs in today’s corporate world. These things include financial information, employee personally identifiable information (PII), and even third party information shared between companies. New controls have been implemented that address various security domains, such as human resource security, information security incident management, and information security policies. (*A. Aginsa) In all, there are 148 mandatory controls in the ISO/IEC 27001:2013 standard. (Terroza, A. S.) Using ISO/IEC 27001 as a guide, a company can easily display its commitment to potential clients and partners that they are committed to protecting sensitive data. This standard is so effective and widely used, that “66% of companies using it noticed an increase in quality control of information security processes and

procedures and 40% decrease in risk" according to BSI America.(Terroza, A. S.) They also saw their number of information technology systems decrease their downtime by 39%. (Terroza, A. S.) Perhaps one of the most promising statistics is that 87% of those that implemented the ISO/IEC 27001 standard had a positive outcome. (Terroza, A. S.) The business friendly ISO/IEC 27001 framework not only provides the business the ability to ensure proper protection of its assets, but also servers as a market differentiator if the company becomes certified against the standard. (ISMS Home)

Looking back to the ISO/IEC 27001:2005 standard, we see the implementation aspect of Plan, Do, Check, and Act. The 2013 update has modified this with the steps of context of the organization, leadership, planning, support, operation, performance evaluation, and improvement. (*M. Nancylia)

In the context of the organization control, there are several sub controls. The first is to understand the organization and its context. (Terroza, A. S.)This means that those creating the plan need to understand what business it is that they are in and how they perform. The next is to understand the needs and expectations of interested parties. (Terroza, A. S.) This is in reference to understanding what the requirements of the business' customers are and possible any 3rd party companies that they work together with in pursuit of their organizational goals. The scope of the information security management system must also be determined in this control. (Terroza, A. S.) This includes which departments and employees will participate. The last sub category is the

actual information security management system itself, which will be determined by the members during the planning phase.

Under the leadership control, the primary and most important sub category is the commitment by leadership. (Terroza, A. S.) This is where leadership offers their support behind the security policies to be made in order to help enforce them. Leadership includes the board of directors, the executive staff, the management staff, and the operations groups. (New Books) The policy sub category comes next. (Terroza, A. S.) This is where the guidance and substantiating rules are drafted that the business will follow. The last sub category under the leadership control is to define the organizational roles, responsibilities, and authorities. (Terroza, A. S.) This involves putting in writing, who is in charge of what sections, what those sections will do, and who has the ability to authorize certain things, such as security system modifications, purchases, etc.

With leadership on board, ISO/IEC 27001 moves into the planning control phase with the first sub category being to determine the actions to use in addressing risks and opportunities. (Terroza, A. S.) These could include actions such as accepting a contract in the best interest of the company, or even purchasing a new piece of network security equipment to mitigate risks factors. The team must also come up with their information security objectives and how they will attain them. (Terroza, A. S.)

After the business team has drafted a plan, they need foster it through the support control. (Terroza, A. S.) This requires resources (Terroza, A. S.), which can come in the form of human or capital depending on the needs of the business. The subcategory of competence (Terroza, A. S.) requires knowledgeable members to be placed in appropriate positions throughout the process. Awareness (Terroza, A. S.) is obtained by informing members of the organization and can come in the form of guidance as to who supports who, and what they are responsible for doing. Communication (Terroza, A. S.) not only applies to ensuring people and departments talk, but also can be used to determine how they will talk, whether it's via email, meetings, or video teleconferencing systems. The final subcategory is to document the information. (Terroza, A. S.) Some examples are through policy letters, memorandums, or system's configuration documentation.

The operation control consist of the 3 key features of operational planning and control, information security risk assessment, and information security risk treatment. (Terroza, A. S.) Operational planning and control follows the criteria of previous planning but with the added emphasis of creating controls to see the plan through. Information security risk assessments are accomplished by a method of the team's choosing, while addressing the company's specific business practices. Information security risk treatment defines how a company will treat a risk once identified. The general options are to accept that risk and press on with operations, mitigate it by implementing a control such as a badging system, or to transfer it to a third party

through an agreement similar to the way an insurance company will cover the corporate headquarters building in the event of an earthquake.

Despite the best efforts of a company to plan for everything, they will inevitably miss critical items throughout the lifecycle of the company's existence. That is where the performance evaluation control is useful. (Terroza, A. S.) Through performance evaluation, there are three subcategories of monitoring, measurement, analysis and evaluation; internal audit, and a management review. The first with monitoring and evaluating is done by gathering metrics that the company has deemed important key indicators as to whether or not their information security management system is performing as intended. This can be done through various automated systems that report back to administrators. Internal auditing is done in a similar fashion, but more meticulously and much more focused. It can be performed on the information security management system itself in an effort to identify weaknesses. The management review is the final step in the performance evaluation control. In this subcategory step, management reviews their company's findings and makes the final decision on the next course of action to remedy the issues identified.

The final mandatory clause in ISO/IEC 27001 is the improvement control, which contains the two subcategories of nonconformity and corrective action, and continual improvement. (Terroza, A. S.) This is where areas that do not comply with the business policies are identified and an action to curb them is considered and implemented. The

final step is simply to continuously improve, which means to repeat the process over and over in this case.

Looking back to the Plan, Do, Check, Act process of 2005, (Information Security Management System (ISMS)) within the planning phase, the organization must establish how they want their information security management system to operate. This includes the creation of corporate rules as well as creating corporate policies and processes that are aligned with the goal of minimizing risk, or risk management. The planning phase should involve senior members in the organization. Without management's buy in and support, the remaining steps would surely fail. (*M. Nancylia)

After the plan is created, the business moves onto the "Do" phase. This is the point in which the company begins to execute the plan and create their information security management system. Policies can be enforced automatically through the use of rules or access control measures. Process work flows would also be implemented through a system of the company's choosing. (*M. Nancylia)

Once the information security management system has been implemented, the company must perform the "Check" phase. This requires continuous monitoring and validation of the system against the policies created in the initial phase. Reports can alert employees, as well as management, to any potential areas of interest in need of rework within the information security management system.

With problematic areas identified, the company can then “Act” on them. In the Act phase, the company uses the information gathered during the Check phase and takes action to correct the issue. Depending on how large or serious the issue is, this could force a rework of the original policies and rules established in the first step of the Plan, Do, Check, and Act model, which is why the is a continuous and looping process as companies and their requirements can change over time.

Although the 2013 standard has come up with a considerably longer process, the steps in it align very closely and in some cases mirror the Plan, Do, Check, and Act process of its 2005 predecessor.

As important as the adoption of widely accepted standards like ISO/IEC 27001 and the iterative process of Plan, Do, Check, and Act is, there is one security vulnerability that is still virtually unpredictable, and that is the user themself. After an information security management system has been adopted, enacted, maintained and updated, it still relies heavily on the assumption that the users in the business will behave in a secure manner. In computer systems, this is known as a trust relationship, where users are given certain access levels under the assumption that they can be trusted to act accordingly. This is a socio psychological aspect of information security that has made the need for user education in the field so vital for companies today. (*K. U. Loser) Companies can not rely on automation and advanced technology alone to

protect their information. One group of researchers suggest that information security management systems be complemented with a socio-technical walkthrough (STWT). (*K. U. Loser) The socio-technical walkthrough purpose is to bring the people involved into the process more thoroughly for a better and more effective overall system. The researchers even found that their STWT system was integratable with technically centric fields, such as cryptography and other forms of computational validation. (*K. U. Loser) The Blackboard program in use by many universities today can create a better image for how the socio-technical process works with so many different users. The Blackboard system is used heavily by students to submit assignments, but is also used by professors to upload and download content. System administrators grant access to Blackboard while also ensuring it is kept up to date with the latest patches and software changes. It is a veritable digital eco system teeming with users all focused on different aspects of its capabilities. It is important that each user understand their permissions and what is allowed from the user perspective, but it is also as important that their permissions do not creep into areas where they shouldn't have been granted from the technical perspective.

The process of accurately documenting, planning, and implementing an effective information security management system can be a daunting task for the uninitiated, and more so when smaller companies that has employees that are dual hatted in multiple roles. In order to address this issue, some vendors have begun the process of automating the creation and documentation behind an information security management

system. The RSA company has one such tool that a company can use to create “a complete representation of this system of interrelated elements requires a comprehensive understanding of the security infrastructure, the various assets being protected, and potential risks to those assets.“(RSA Archer Information Security Management) The product is called RSA Archer Information Security Management System and it “allows you to quickly scope your information security management system and document your Statement of Applicability for reporting and certification. You can also catalog individual resources related to your information security management system, including information assets, applications, business processes, devices, and facilities, and document and maintain related policies, standards, and risks. This centralized view of your information security management system makes it easier to understand asset relationships and manage changes to the infrastructure. Issues identified during assessments can be centrally tracked to ensure remediation efforts for gaps are consistently documented and monitored and effectively addressed.” (RSA Archer Information Security Management) The Archer system addresses the main issues in aiding to identify all the areas of a business that should be considered under the information security management system. With the all applicable areas mapped, and all non-included areas removed, the business can appropriately address the areas of concern identified.

The RSA Archer information security management system has several key features noted in their data sheet. The first key feature is that of having the ability to see

just how far the scope of your information security management system goes. (RSA Archer Information Security Management) The Archer system also allows the company to easily document a company's Statement of Applicability. The Statement of Applicability is a critical document and first step, in that it is the primary document that defines how to implement the information security program in the business and can serve as a quick reference overview on the company's information security management system. (ISO 27001 Statement of Applicability) The Statement of Applicability letter serves as the primary correlation between a company risk assessment and the treatment options by defining exactly how the company will implement the control options laid out in ISO/IEC 27001 and which ones they will utilize. (ISO 27001 Statement of Applicability) The Statement of Applicability is a mandatory document in order to comply with the ISO/IEC 27001 standard and is used to not only identify which controls the company will use, but also why they were chosen to be used. Those reasons can range from contractual obligations, legal requirements, or any other reason deemed necessary by the business. (ISO 27001 Statement of Applicability) The Statement of Applicability document can also be used to explain why certain controls were chosen to be implemented by the company, or also why they were not chosen to be implemented by the company. (ISO 27001 Statement of Applicability) It can even include the reference of other controls from another source option besides ISO/IEC 27001. (ISO 27001 Statement of Applicability) This document is also written in a much shorter format than other documents of the same nature, where a single line on the page is dedicated to each of the 114 control options afforded in the ISO standard,

making it much quicker to reference during a company's daily operations. (ISO 27001 Statement of Applicability) This doubles down as a checklist for leadership and others involved in the process to know, at a glance, whether or not the controls listed and chosen have been implemented already or not. It can also include exactly how the controls that are implemented are currently being used. (ISO 27001 Statement of Applicability) This document also serves a pivotal role in the ISO/IEC 27001 standard certification process as auditors validate your claims made in the Statement of Applicability. (ISO 27001 Statement of Applicability)

The next key feature of the RSA Archer information security management system is the ability to catalog resources for better organization. (ISO 27001 Statement of Applicability) This breakdown can be done in numerous ways such as whether or not the area of concern is an information asset. (ISO 27001 Statement of Applicability) It can also differentiate between applications, business processes, and hardware as well as structures. (ISO 27001 Statement of Applicability) The Archer system can even be used to assist in the documentation process for a company's information security risk analysis as well as be used in order to create the information security management system policies while also being able to manage any deficiencies identified while evaluating the information security management system. (ISO 27001 Statement of Applicability) The information security management system dashboard shows the user each control in a line by line layout. Each line can display various fields including why the control was chosen, how well the company complies with the control, what exactly

the risk is that it was chosen for, the level of the risk, and how the company chose to respond to that risk while also providing a quick reference compliance percentage chart. (ISO 27001 Statement of Applicability) This central ability to track and document compliance with the information security management system is extremely convenient and reduces the overhead of formatting when creating an information security management system. It can also be used to quickly generate reports to show key leadership members deficient areas in need of their attention and support. Unfortunately, gathering more detailed information for analysis and comparison of these automated systems is difficult without coordinating demos from the company's that offer them, and the data sheets are limited. (ISMS Home) There will be a need for future research on newer systems as more and more vendors begin to offer advanced and all inclusive automated security compliance tools to their customers in order to ascertain whether they are viable options or not.

The ISO/IEC 27001 standard, specifically the 2013 version, has become the modern day gold standard for those companies wishing to differentiate themselves from their competitors in their dedication to information security. This standard offers a comprehensive list of control options to be implemented in order to comply as well as the Statement of Applicability letter to assist in the auditing process on the road to accreditation. Vendors are offering up digital and automated solutions to reduce the learning curve required and step a business through the process of information security

management system creation, while also allowing for accurate and simplified reporting of compliance.

References

ISO/IEC 27000 family - Information security management systems. (2017, February 27). Retrieved May 19, 2017, from https://www.iso.org/isoiec-27001-information-security.html

*A. Aginsa, I. Y. Matheus Edward and W. Shalannanda, "Enhanced information security management system framework design using ISO 27001 and zachman framework - A study case of XYZ company," *2016 2nd International Conference on Wireless and Telematics (ICWT)*, Yogyakarta, 2016, pp. 62-66.

*M. Nancylia, E. K. Mudjtabar, S. Sutikno and Y. Rosmansyah, "The measurement design of information security management system," *2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Kuta, 2014, pp. 1-5.

*K. U. Loser, A. Nolte, T. Herrmann and H. te Neues, "Information security management systems and socio-technical walkthroughs," *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, Milan, 2011, pp. 45-51.

Terroza, A. S. (2015, May 12). Information Security Management System (ISMS) Overview. Retrieved May 19, 2017, from https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf

Information Security Management System (ISMS). (n.d.). Retrieved May 19, 2017, from http://cnii.cybersecurity.my/main/resources/ISMS.pdf

New Books. (n.d.). Retrieved May 19, 2017, from http://www.infosectoday.com/Articles/ISMS/Information_Security_Management_Systems.htm

ISMS Home. (n.d.). Retrieved May 19, 2017, from https://www.isms.online/

RSA Archer Information Security Management System (ISMS). (2016). Retrieved May 19, 2017, from https://www.rsa.com/content/dam/rsa/PDF/2016/06/Data-Sheet-RSA-Archer-ISMS-H15121-5-2016.pdf

ISO 27001 Statement of Applicability – Why does it matter? (n.d.). Retrieved May 19, 2017, from https://advisera.com/27001academy/knowledgebase/the-importance-of-statement-of-applicability-for-iso-27001/