Micah Wieburg - Week 3 - Research Paper

Micah L Wieburg

School Of Computer Information Sciences

ITS835 - A01 Enterprise Risk Management

Dr. Jimmie Flores

January 27, 2023

Embracing and successfully implementing the information security standards and frameworks available to organizations is a significant step in creating a holistic risk management system. There can often be an absence of standardization across organizations concerning risk management practices, information security, and security guidelines which could allow for security flaws that can have devastating effects. To aid corporations in these issues, The International Organization for Standardization (ISO) has created a suite of frameworks to guide and certify entities that meet its standards. ISO is focused primarily on developing and monitoring technical standards, making them an excellent source of security certifications, as information technology is a crucial sector in almost every enterprise. One of the ISO's most recognized and used standards is ISO 27001. ISO 2007 has been embraced on an international level by enterprises of all sizes and markets. Research and results lead to the belief that ISO 27001 would work well as a framework in my current organization. My current organization handles a decent amount of sensitive data. My research revealed that ISO 27001 would be a great addition to the current information security management system.

ISO 27001 is a technology and vendor-neutral management system designed to provide confidence to an organization's information security procedures and effectiveness (Freeman, 2007). Designed to define the necessary actions to establish, implement, maintain, and regularly improve information security management systems, ISO 27001 is the third most certified standard on a global scale (Culot et al., 2021). Using this framework will allow my organization to ensure we are developing an information security management system (ISMS) that connects risk assessment, treatment, and administration into one holistic approach. Options for handling risks are also plentiful within the ISO 20071 framework. The ability to either treat risks via risk avoidance, risk acceptance, risk mitigation, or risk transference provides a level of diversification necessary for contemporary organizations (Brenner, 2007). ISO 20071 certification will also benefit from incorporating the Plan, Do, Check, and Act (PDCA) methodology into our ISMS. This methodology is designed to be a repeated circular process that encourages regular evaluation of the principles of the ISO 27001 framework. This approach to an ISMS is critical due to the necessity to establish and risk evaluation process that is on par with how frequently threats to organizations change.

By regularly visiting the Plan portion of the PDCA model, my organization would identify and analyze risks and develop risk mitigations against these risks in this model step. After that, the Do phase of the PDCA model is visited as an opportunity to create responsibilities within the organization and define managerial behaviors and priorities. Enacting controls, characterizing metrics for control effectiveness, and applying the defined actions for negative event discovery should be handled in the Do phase of PDCA. The Check phase of the PDCA is critical as this is the phase responsible for monitoring and reviewing the configuration of the ISMS. In this step, the benefits are spawned from taking actions to gauge ISMS effectiveness and reviewing procedures and risk assessments. Ultimately, this step is where gaps and improvements are to be discovered to improve the ISMS. Administering the discovered improvements to our ISMS would occur in the Act phase of the PDCA model. Once the improvements have been implemented, taking the necessary reformative behaviors should occur in addition to reviewing the learnings from this cycle of the PDCA model and informing the appropriate parties of the actions taken.

A certification of this magnitude would be a valuable asset to my organization's commitment to information security. There is also a competitive advantage yielded by obtaining ISO 27001 certification as it displays that the organization is committed to protecting its customers' data. Cyber-attacks have caused significant damage to organizations' infrastructure and integrity which ultimately devalues the organization and causes mistrust and frustration among its customers. By subjecting ourselves to the process required to obtain ISO 27001 certification, we protect our systems and the data it encompasses to avoid the aforementioned negative impact. While the ISO 20071 framework is an excellent option for ensuring an efficient ISMS, other standards and frameworks could benefit my organization.

Another widely accepted and sought-after framework is the ISO 9001 standard which defines rudimentary necessities for a quality management system. Over one million certificates for ISO 9001 have been granted. This framework focuses heavily on advancing an organization's internal operations. ISO 9000 certification has been noted to help an organization achieve greater productivity, advanced sales, lower costs, and better control over business operations (Khanai & Bharamanaikar, 2019). Organizations that seek and obtain ISO 9001 certification operate with fewer mistakes due to the focus on quality management, which ultimately increases customer contentment. With the ISO 9001 framework, many organizations witnessed benefits related to their ability to document work methods, giving employees of the organization better insight into their responsibilities. As a result of the control and improvement in quality products, the organizations bolstered an improved image in the eyes of their customers. Employee engagement and incentive is another benefit fostered by all of the internal quality improvements of ISO 9001. A competitive advantage is also documented as a benefit of ISO 9001-certified organizations as they tend to outperform organizations that still need to implement quality management systems to meet the ISO 9001 standard. The competitive advantage is in ISO 9001's ability to enhance internal business processes (Tarí et al., 2012). ISO 9001 execution subjects organizations to the principle of continual improvement (Chountalas et al., 2020). This focus on continual improvement is a key benefit that will give organizations an essential change in mindset in how their processes are approached. Ultimately, holders of the ISO 9001 certification see long-term benefits related to process improvement as the workplace setting is centered on the idea that continual process improvement must be performed to achieve critical objectives.

ISO 14001 is a framework that would work in conjunction with ISO 20071. Key benefits of the ISO 14001 standard are related to a reduction in resource usage and an improved image to the organization's stakeholders (Martí-Ballester & Simon, 2017). Organizations also observed a better image and customer satisfaction with increased environmental rendition, profitability, and effectiveness. (Tarí et al., 2012) classifies ISO 14001 benefits into three groups. The groups are labeled as internal performance, external marketing, and relations benefits. Internal performance benefits were related to reductions in cost and increased productivity and motivation among employees. External marketing benefits included an increase in market share and greater customer satisfaction. The relations benefits create a separation between ISO 14001 and ISO 9001. This benefit group highlights an enhanced relationship with local communities, primarily through the environmental performance exhibited by ISO 14001-certified organizations. Using the ISO 14001 and the ISO 20071 would prove to be a powerful combination for any organization as the benefits of information security and quality of operations and products are fused to create solidified internal procedures that met the expectations of two of the most rewarding frameworks.

We could also see benefits to our information security structure by implementing ISO 27002 standards. ISO 27002 places its focus on the protection of key assets of an organization. The security controls put in place by an organization are required to fulfill regulatory, legal, and contractual requirements (Topa & Karyda, 2019). Security controls within ISO 27002 include cryptography and standards for implementing physical security. Physical security topics are covered by security training for an organization's employees to teach them their responsibility to avoid breaches of organizational resources. Security training importance is reinforced to staff by establishing the devastating outcomes that can occur for the organization in the event of a security transgression.

This security training is one of the key benefits of ISO 27002, as the human aspect of information security can be the target of attackers suspecting that employees do not have the proper training. ISO 27003 can work in tandem with ISO 27001 in creating an ISMS as it places its structure on defining the scope of the ISMS, identifying security requirements, and carrying out risk assessments and treatments (Topa & Karyda, 2019). Adding requirements from ISO 27005 framework will bolster our risk management process due to this framework centering on the necessities substantiating an ISMS as it relates to security controls and the restrictions required to ensure ease of use for the ISMS.

Security standards are an excellent opportunity to improve security and business practices. ISO 27001, ISO 27002, ISO 27005, ISO 9001, and ISO 14001 are world-renowned frameworks that can be leveraged by any organization seeking to improve its operations. The frameworks discussed in this paper can serve as guidelines for organizations to create an efficient and secure ISMS, increase product quality, and improve performance in their respective markets. While these standards offer numerous benefits individually, an ideal configuration would include the usage of multiple standards to harness the various advancements related to each.

References

Brenner, J. (2007). Iso 27001: Risk Management and Compliance. Risk Management, 54(1), 24-26,28-29.

Chountalas, P. T., Magoutas, A. I., & Zografaki, E. (2020). The heterogeneous implementation of ISO 9001 in service-oriented organizations. TQM Journal, 32(1), 56–77. https://doi.org/10.1108/TQM-02-2019-0053

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. TQM Journal, 33(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Freeman, E. H. (2007). Holistic Information Security: ISO 27001 and Due Care. Information Systems Security, 16(5), 291–294.

Khanai, S. N., & Bharamanaikar, S. R. (2019). Effect of ISO 9001 Standard on Organisational Performance. Abhigyan, 36(4), 47–56.

Martí-Ballester, C. P., & Simon, A. (2017). Union is strength: The integration of ISO 9001 and ISO 14001 contributes to improve the firms' financial performance. Management Decision, 55(1), 81–102. https://doi.org/10.1108/MD-09-2015-0414

Tarí, J. J., Molina-Azorín, J. F., & Heras, I. (2012). Benefits of the ISO 9001 and ISO 14001 standards: A literature review. Journal of Industrial Engineering and Management, 5(2), 297. https://doi.org/10.3926/jiem.488

Topa, I., & Karyda, M. (2019). From theory to practice: Guidelines for enhancing information security management. Information and Computer Security, 27(3), 326–342. https://doi.org/10.1108/ICS-09-2018-0108