Pushing for better Cybersecurity Education and Awareness Training in the ISMS: How the ISO/IEC 27001 is the Most Important To Learn

Alexander Abou Khir

Old Dominion University

IT425W Cyber Strategy and Policy

Professor Hamza Demirel

January 25th , 2025

Everywhere we go we rely on technology from not leaving our home without our phones, and having our information posted to the internet on social media or for important transactions like sensitive information to bank companies. The outside world is dangerous like just as how a robber could steal your wallet or purse, the threat actors on the internet can do the same through digital means. With increasing reliance on the internet, companies, government agencies and organizations across the world have been implementing policies to prevent leaks of sensitive information, breaches, and other different types of attacks and exposure attempts. These policies involve training, awareness, or certain cybersecurity infrastructure that must be set in place to be more protected from threat actors, insider threats and even accidental actions. The Cybersecurity policy I have chosen is ISO/IEC 27001 because it guidelines are very vast, in detail and can be used across any organization, company or even governmental body. The standard coincides with the ideology that an efficient Information Security Management System (ISMS) is supported by several topics that provide beneficial guidance to employees within the workforce (Fonseca-Herrera, 2021). These topics can be identified as security policy and objectives, risk assessment methodology, risk treatment plan, and procedures and guides. These topics all integrate to support a healthy management system by allowing for employees to train and educate on these topics. This is a great supporting factor for the idea of implementing this policy into the workplace environment employees. The standard coincides with the ideology that an efficient ISMS is supported by several topics that provide beneficial guidance to employees within the workforce (Fonseca-Herrera, 2021). These topics can be identified as security policy and objectives, risk assessment methodology, risk treatment plan, and procedures and guides.

These topics all integrate to support a healthy management system by allowing for employees to train and educate on these topics. This is a great supporting factor for the idea of implementing this policy into the workplace environment for all employees.

The origin of ISO/IEC 27001 date back to 1987 developed through several stages of different versions and is still being improved upon to this day. These developments were backed by environmental advantages and learning from disaster recovery while also trying to internationally cooperate with other countries standards. For example, the ISO 14001 series was created to align with the standards in other worldwide environments (Vladislav). The current version, used in the workplace, was developed solely on the British BS 7799-2 Standard. The ISO IEC 72001 standard took a route as an updated version of the British standard and was supported from the anticipation from both ISO 9001 and ISO 14001's success. This allowed for base characteristics derived from the two previous versions and allowed for a rather flexible standard that can be easily applied to a lot of security environments (Vladislav). With Vladislav's findings shows proof of years of reliability on complex issues can be used within the workplace as a framework for broadening education, awareness, and training methods. A previous company has already embarked on integrating the ISO 1EC into regular business routines. The company allocated the standards into each department where it would apply best, then would allow for weekly routine observations to oversee the successfulness of the standards (Kovac). Auditing was a method used to observe and derive information from the weekly research. From collaboration with other countries and regions, such as the utilization of the British standard as a developmental tool, the standards were able to be constructed into a global base standard in which collaboration, information sharing, and transparency goes together

to develop a safe global environment for potential threat actors (J. Antilla, 2012). With the idea that standards are performed at the international level to ensure cooperation means that these standards are also performed in the governmental level, showing its relevance within the cybersecurity industry.

References

Anttila, J., Jussila, K., Kajava, J., & Kamaja, I. (2012, August 1). *Integrating ISO/IEC 27001 and other Managerial Discipline Standards with Processes of Management in Organizations*. IEEE Xplore. https://doi.org/10.1109/ARES.2012.93

Fomin, V. V., de Vries, H. J., & Barlette, Y. (2008). ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption. *EuroMOT 2008 - the Third European Conference on Management of Technology*. https://www.researchgate.net/publication/228898807_ISOIEC_27001_Information_Systems_Security_Management_Standard_Exploring_the_reasons_for_low_adoption

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science*, *48*(2), 213. https://www.researchgate.net/publication/362062660_A_Model_of_an_Information_Security_Management_System_Based_on_NTC-ISOIEC_27001_Standard

Kováč, S. (2015, June 26). *Introducing a System for Information Security Management by ISO/SEC 27007*. Muni.cz. https://is.muni.cz/th/ox4nz/?lang=en%3Bzoomy_is