SS

by Ss Ss

Submission date: 02-Jun-2021 10:22AM (UTC-0400)
Submission ID: 1599055563
File name: evaluating_framework.edited.docx (24.23K)
Word count: 830
Character count: 4953

Evaluating Framework Alignment

Name

Institution

Course

Instructor

Date

Evaluating Framework Alignment

Many organizations and companies utilize frameworks because they are guaranteed to use the observe the relevant laws and protect their network in a conformant way. One of the frameworks used is COSO. Chiu & Wang (2019) stated that COSO is an acronym for Committee of Sponsoring Organization of Treadway Commission and was intended to develop a robust internal control system to safeguard shareholders and clients from fraud. Therefore, this framework is essential in the banking industry because credit deception can be stopped. COSO utilizes the COSO cube, which integrates three internal controls objectives, including the reporting, processes and compliance. The framework is easy to execute hence good for the organization to start with; nonetheless, it is broader and can result in challenges, especially to complex companies.

Information Technology Infrastructure Library (ITIL) is another framework that comprises volumes of libraries explaining the foundation of best practices for offering information technology services. ITIL aims to establish IT services in the whole lifecycle (Gërvalla et al., 2018). The framework can be used in every sector that needs to control their information Technology, for example, hospitals and banks. ITIL can aid business in managing the dangers, reinforce customer association, develop cost-effective activities and create a steady information technology ecosystem which provides a chance for growth. Nevertheless, this framework is expensive to execute because extensive training is needed.

NIST 800-53 is the next framework which is a governing standard that describes the least foundation of security controls for all American federal information systems, excluding those associated with national safety. Sandoval (2017) emphasized that this framework is utilized by several things, including consciousness, access control and training. Therefore, it is widely used

in healthcare organizations, especially when implementing their systems, including electronic health records. The purpose of NIST 800-53 is to create procedures that will evaluate risk and protect the assets that are under threat. The benefits of this framework are to enhance information security and develop a foundation for cybersecurity preparation. However, it has a challenge because of many requirements and the acquittance needed to execute.

The purpose of the COBIT framework is to help companies in information technology governance and management. Therefore, COBIT can be utilized in every sector; however, it is appropriate for information technology managers, risk committees, and other high-level executives. Astuti et al. (2017) claimed that to execute COBIT, an organization needs to observe a lifecycle method from starting the program to evaluating its efficiency. Also, COBIT has more benefits because it causes countless risk minimization, ascendency, effectiveness and output. On the other hand, implementing COBIT is not easy as it requires more equipment and skills.

Lastly is the ISO 27001 framework. This framework is the most recognized standard for handling information technology protection to maintain data safe in government organizations and private companies. Hsu WT AL. (2016) stated that the purpose of ISO 27001 is to safeguard the central intelligence agency triad. This framework is vital because of the advantages it has for the company. It assists the organizations in observing laws, attaining competitive advantage through obtaining certification and reducing the cost of information technology by eradicating dangers. Nonetheless, it has the disadvantage of insufficiency in risk evaluation processes as well as inadequate direction on controls.

The explained frameworks work on enhancing protection, confidentiality, risk management and planning. Therefore, the access control archetypal can achieve several roles performed by frameworks. Nevertheless, a security framework summarizes the methods of

executing security procedures, while an access control approach is a method that can be utilized to execute an outline. Also, access control is restricting the admission to data, specific individuals or systems. Moreover, access control models and frameworks can be united to develop a clearer procedure because they all focus on verifying and approving data.

Furthermore, because information system is controlled by elements in the framework, the framework will be utilized in justifying dangers and susceptibilities in information security, everyday work to achieve this and the break that can happen. similarly, access control has restrictions on an individual that needs to access information security. However, it can also result in challenges in openness.

References

Astuti, H. M., Muqtadiroh, F. A., Darmaningrat, E. W. T., & Putri, C. U. (2017). Risks assessment of information technology processes based on COBIT 5 framework: A case study of ITS service desk. *Procedia Computer Science*, *124*, 569-576.

Chiu, T., & Wang, T. (2019). The COSO framework in emerging technology environments: An effective-in-class exercise on internal control. *Journal of Emerging Technologies in Accounting Teaching Notes*, *16*(2), 1-10.

Gërvalla, M., Preniqi, N., & Kopacek, P. (2018). IT Infrastructure Library (ITIL) framework approach to IT Governance. *IFAC-PapersOnLine*, *51*(30), 181-185.

Hsu, C., Wang, T., & Lu, A. (2016, January). The impact of ISO 27001 certification on firm performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848). IEEE.

Sandoval, R. (2017). Information systems development (ISD) and the national institute of standards and technology (NIST) risk management framework.

SS

ORIGINALITY REPORT

1%	1%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	markets.ft.com Internet Source	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		