A Brief Overview & Comparison of ISMS Frameworks

Saptarshi Laha
M.Sc. Cybersecurity
School of Computing
National College of Ireland
Dublin, Ireland
x18170081@student.ncirl.ie

***Abstract*—The primary goal of this document is to introduce its readers to the concept of Information Security Management Systems and study the various frameworks available in today's date for the same in brief, which will further help us draw a comparison between them.**

Keywords—ISMS, comparison, standards, frameworks

I. Introduction

Every business, irrespective of how small or large it is, if online by any means, could be a potential victim to cyber-attacks. Hence companies in today's world using the internet to perform any level of activity should cut costs by implementing safe data protection and cybercrime prevention mechanisms from the very beginning. To incorporate essential and functional security in a business project, the need for an Information Security Management System (ISMS) arises.

An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach[1].

There are many standards set for ISMS, which are often known as frameworks. These frameworks regulate the policies and procedures to be followed for secure development and deployment of an application but, most importantly, uphold the three primary principles of security – Confidentiality, Integrity, and Availability. Every organization leans towards different frameworks when it comes to the implementation of software for their projects due to multiple reasons such as development cost, audit cost, etc. We first list the frameworks available for the audience to choose to incorporate in their business project and then compare them briefly to highlight the benefits as well as shortcomings of each of them.

The most commonly followed ISMS frameworks as of 2019 are[2]:

A. *The CIS Top 20 Critical Controls.*
B. *The NIST Cybersecurity Framework.*
C. *Cyber Essentials.*
D. *ISO 27001:2013.*
E. *PCI DSS.*

II. The CIS Top 20 Critical Controls

The top 20 list from CIS (earlier known as SANS top 20) emphasizes on some of the significant topics related to cybersecurity with clear and concise methods to implement the same during the development phase or mentioning the incorporation mechanism to follow to have usable security. The CIS top 20 controls include specifications of inventory and control of hardware and software assets, controlled use of administrative privileges, maintenance, monitoring and analysis of audit logs, malware and boundary defenses, data protection, penetration testing, and red team exercises, etc.[3] This framework is, however, limited in terms of defining the entire security of the application and merely serves as a focal point of security based on recent attacks. The CIS cybersecurity manual fills in the gaps left by the top 20 by delving into the detail of the unmentioned policies and mechanisms to be incorporated or secured in a project.

III. The NIST Cybersecurity Framework

NIST is a U.S. government initiative at incorporating usable security in applications at every stage, starting from identifying potential vulnerabilities, protecting vulnerable points from exploits, detecting malicious activity, responding to intrusions and threats, and recovery from the safe, hence defining a fail-safe standard. Currently, the framework version 1.1 is used to describe and highlight a variety of areas where security measures should be incorporated, such as data protection schemes during storage to data protection during secure delivery, safeguarding of assets, etc.[4]

This is a much more detailed specification document than the CIS TOP 20 Critical Controls and focuses on a plethora of other essential security points and security attributes with clear and concise explanations on how to incorporate them into the project and activities that should be performed to maintain the standard of security obtained.

IV. Cyber Essentials

Just like NIST, Cyber Essentials is a U.K. government initiative at providing rather basic guidelines at securing an application or digital environment. It gives a fundamental set of standards and sets shallow requirements or is often ambiguous in its style of representation when it comes to detailing the security aspects to be incorporated in its essential advice section. However, the rigor comes into play with the audits and certification authorities, when they validate and verify applications to certify them and add them to the Cyber Essentials certified database on their website[5].

Compared to the other two standards mentioned above, the lack of openness to information regarding incorporating basic security needs before applying for an audit or verification seems very limited. To add to this, the critical points mentioned under the advice section barely highlights significant issues based on recent or trending attacks. Instead, it suggests some fundamental tasks one should follow on every system to keep it secure to a certain extent. This, however, makes it audience-friendly and does a decent job of spreading awareness instead of setting security standards, for which it should be appreciated.

V. ISO 27001:2013

This is by far the most structured and comprehensive manual on information security standards addressing issues from the very grassroots level to the absolute essential security principles needed in place. Topics covered in the previous sections just form a sub-section of ISO's manual. It addresses critical subjects such as the context of the organization, leadership and planning, support and operation, performance evaluation, and improvement[6].

Where ISO lacks is in the payment handling department, which is taken care of by PCI DSS and PA DSS, as mentioned in the next section. ISO standards are by far the most extensively used and most trusted framework concerning a variety of standards, not just pertaining to information security, which is clearly seen by the extensiveness of coverage of the standards manual.

VI. PCI DSS

PCI DSS is primarily focused on securing card payments and storing of sensitive financial and identity information such as credit card details in a secure format. They are the pioneers in providing a certificate for authentic and secure payment gateways and credential storing units. PCI DSS focuses on a variety of aspects related to safe storage and usage of financial credentials such as building and maintaining a secure network and systems, protecting cardholder data, maintaining a vulnerability management program, implementing active and robust access control measures, regular monitoring and testing of networks and maintaining an information security policy[7].

Since the scope of PCI DSS is very limited compared to the previously mentioned information security standards, it is quite challenging to compare the same with the others. However, financial data being the most valuable data and PCI DSS being a top certifier in the field only explains the stringent policies it has in place to prevent financial fraud, data leak, and the best threat detection policies in place in its vulnerability management program.

CONCLUSION

Most of the frameworks mentioned have a well detailed and specified standard that they follow available publicly for implementation by developers in their projects. Some of them are limited in scope, such as PCI DSS, and others are too ambiguous in their definitions and descriptions, such as Cyber Essentials. Even though their extent is somewhat limited, they do their part in providing specific standards in an individual subdomain of activities performed online or help spread awareness about cybersecurity in general, which is beneficial, respectively. The different ups and downs of each of the standards, if any, are, in general, covered for by the other frameworks in place. Hence, it is a good business practice to get covered by two or more certificate issuing authorities than just one. Although this would require two or more audits and cost the business more in its capital expenditure, it will be well worth the added security in the long run by attracting potential cyber security-aware customers to their portal.

ACKNOWLEDGMENT

I want to thank the authors of the referred links for providing me with relevant information for me to be able to complete this CA Assignment well within time.

I would also like to thank my lecturer Mr. Vikas Sahni for allotting me this assignment that encompasses multiple frameworks of information security management system. This assignment helped get me up to speed with the security implementation standards followed in the cybersecurity world.

REFERENCES

[1] M. Rouse, "What is information security management system (ISMS)? - Definition from WhatIs.com", WhatIs.com, 2019. [Online]. Available: https://whatis.techtarget.com/definition/information-security-management-system-ISMS. [Accessed: 15- Nov- 2019].

[2] "Information Security Management Framework | IT Security | Integrity360", Integrity360.com, 2019. [Online]. Available: https://www.integrity360.com/cyber-risk-advisory/information-security-management-framework. [Accessed: 15- Nov- 2019].

[3] "The 20 CIS Controls & Resources", CIS, 2019. [Online]. Available: https://www.cisecurity.org/controls/cis-controls-list/. [Accessed: 15- Nov- 2019].

[4] "Cybersecurity Framework", NIST, 2019. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: 16- Nov- 2019].

[5] "Homepage", Cyber Essentials, 2019. [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/. [Accessed: 16- Nov- 2019].

[6] Iso.org, 2019. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. [Accessed: 17- Nov- 2019].

[7] "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards", Pcisecuritystandards.org, 2019. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1574022799239. [Accessed: 17- Nov- 2019].