THE INTERNATIONAL JOURNAL OF BUSINESS & MANAGEMENT

A Design of Information Security Maturity Model for Universities Based on ISO 27001

Daniel Makupi
Lecturer, Department of Information Technology Security,
School of Computer Science and Bioinformatics, Kabarak University, Kenya

Abstract:
Information infrastructure is one of the most critical assets in organizations. With continued and rapid advancement in technology especially brought by the need for employees to use their personal devices, it presents a major opportunity and challenge for enterprises, it poses a challenge as adversaries have taken advantage of widening cyber space to attack information and information systems. Our study provides a solution by designing a prototype of a web-based implementation prototype of an information security maturity model for universities. The research was based on ISO 27001 by involving specific clauses relevant to universities because of its unique organizational ecocentric nature having varied categories of user's and extensive research allowing it to serve as a plausible area for study compared to other organizations. The cumulative factors having being considered statistically varied towards contribution towards the maturity model. The model is then implemented using a web-based prototype. The study adopted design research approach to come with the model design.

Keywords: *Model, design, security, ISO 27001*

1. Background

Today's organizations do not hesitate to invest their share in the fields of Information Technology due to benefits accrued in utilization of technology infrastructure. This is done as an effort to get the convenience and benefits of the use of information technology, which is expected to help the performance of the company to conduct a competitive business strategy (Clinton, 2019). Information technology is a very important requirement for all enterprise organizations because it helps in improving the effectiveness and efficiency of enterprise business processes (Singla, 2019).

Because of the benefits accrued in adoption and use of technology and the need to gain competitive advantage Organizations have begun to realize and start doing information security performance evaluation. In not more than two decades ago organizations have begun Identifying, planning, scheduling and implementing information security management as an organizational framework (Kerzner, 2019). In evaluation of information technology, there have been several frameworks that have been widely accepted and proven such as The British Standard for information security management (BS7799) later, International Standards Organization (ISO 27001 & ISO 17799), IETF security architecture (Internet Engineering Task Force), the National Institute of Standards and Technology (NIST 800 series special publications), Control Objectives for Information and related Technologies (COBIT), and Committee of Sponsoring Organizations (COSO) are some of the most prominent initiatives in management of information security and risk management systems (Rhodes-Ousley, 2013; Veljkovic, & Budree, 2019, 2012; Information Systems Audit and Control Association (ISACA), 2012; The ISO 27000 directory, 2007; Yost, 2007; Bowen et al., 2006).

The different standards and information security frameworks that are already existing have been helpful to organizations for efficiency in information security risk management (Khouja et al., 2018). However, because of proliferation of the cyber space and more continued reliance on information and related technologies in operations of organizations, has led to elevated levels of information security requirements (Moulton & Coles, 2003; Posthumus & Solms, 2004; Kooper, Maes, & Lindgreen, 2011; Bahl & Wali, 2014; Edwards, 2018) in view of continued information security needs and ever changing information security landscape, the existing processes and governance structures still appear to be unfit, unstructured, and unreliable.

1.1. Statement of the Problem

The need for organizations to adopt information security so as to thrive in today's business environment that is highly technical is indisputable. There are only a few studies focusing towards achieving the right blend of factors that contribute to achieving a secure information technology infrastructure and gaining towards maturity especially in a dynamic organizational environment. Despite such many certification standards and information security frameworks in place, concerns have been raised on the effectiveness of such alignment and information security audit and governance being viewed as an unmanageable mechanism (Laeeq, & Memon, 2018), because individually none of them, on their own, are standalone frameworks but they all have a useful role in the efficient management of IT operations. In addition, there has not been a mechanism in form of a model to cumulatively come up with the threshold inform of status level as a result of risk exposure by organizations, therefore, this research will serve to inform the status level of information security maturity.

1.2. Objective of the Study

To design an information security maturity model to aid universities in determining the level of maturity in regard to information security based on ISO 27001 standards. It serves to inform organization on the level of information security maturity position.

2. Literature Review

2.1. Information Security Challenge

Information security being a collection of strategies and processes that formally manages information technology risks (Englbrecht, et al., 2019; Chan et al., 2018), there appears to be drawbacks in organizational efforts relating to well defined and enhanced processes, sound standardization, and the lack of adequate security awareness, analysis, support, implementation, and maintenance. Moreover, their exist a gap on modeling information security maturity models given that there is inadequate attention to what should be treated as adequate security and how information security controls can be considered as effective. It's therefore difficult for organizations to optimize their security requirements and inhibits realization on threats facing them including the likelihood and possible impact. Without a requisite model that fits the organization process it proves difficult for organizations to measure performances, ensure compliance to regulations, validate sufficiency in security, and identify improvements in information security. Information security management is a very important requirement for all enterprise organizations today because it has proved to help in improving the effectiveness and efficiency of enterprise business processes (Aydiner et al, 2019).

2.2. Technologies Used by Web-Based Models

Determination of information security maturity entails all efforts that are brought together in order to compute information security risks facing institutions. Information security maturity in a context of a web-based model occurs in the sense that information maturity level issues can be captured for auditing purposes. Typical web-based application follows a model view controller pattern which has three parts Fig. 1 (Qazi et al, 2018).

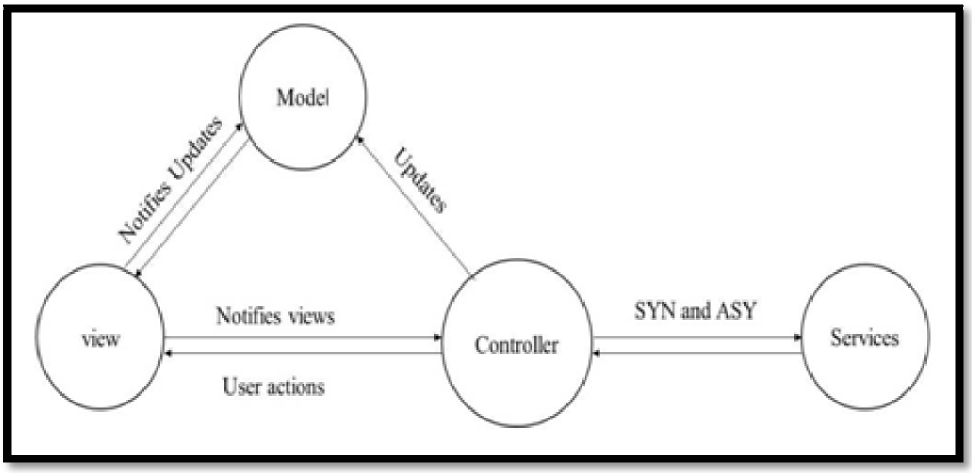

Figure 1: Modified Basic Components of MVC Architectural Pattern & Information Flow (Qazi Et Al, 2018)

The view renders the interfaces where the user interacts with and normally made up of web-based tools with languages such has HTML. Therefore, the HTML page sends information to the controller. The controller responds and process events, which are the user actions and typically invokes changes to model and view. The model is the domain layer which contains the application logic layer, which adds meaning to raw data. It also contains a storage mechanism with a resource management layer underneath. The storage mechanism can be facilitated by database such as MySQL, which is a free open source software and widely available in search engine that can be used has a fast, reliable DBMS with modular engine architecture. It has been used in capturing information for further analysis in various systems like Electronic Database System, the Internet and web programming. It can be used to develop a system for evaluating impacts generated in experiments using a software or and hardware prototype (Wong et al, 2019).

3. Methodology

A design of solution requiring a web-based application is thus proposed to provide an accessible and a reliable mechanism to compute information security maturity based on ISO 27001. The design comprises of four parts; institution registration and deregistration, supplying information security maturity factors and determining maturity of organization. An overview of the design is discussed below.

3.1. User Registration Process

The registration process is the entry point into the system and caters for the registration of organizations. Users supply information on behalf of their organization. The users are then able to enter information security details of their organizations.

3.2. Maturity Determination Process

Determination of information security maturity is based on pre-entered data by organizational in charge on behalf of the organization. Upon filling inn of the necessary information then information security maturity will be computed based on the model coefficients weights as per the information security factor as obtained from statistical analysis.

4. System Design

Based on the model proposed in the previous section, a prototype was designed. The system flowcharts are presented in Figs. 1 – 4.

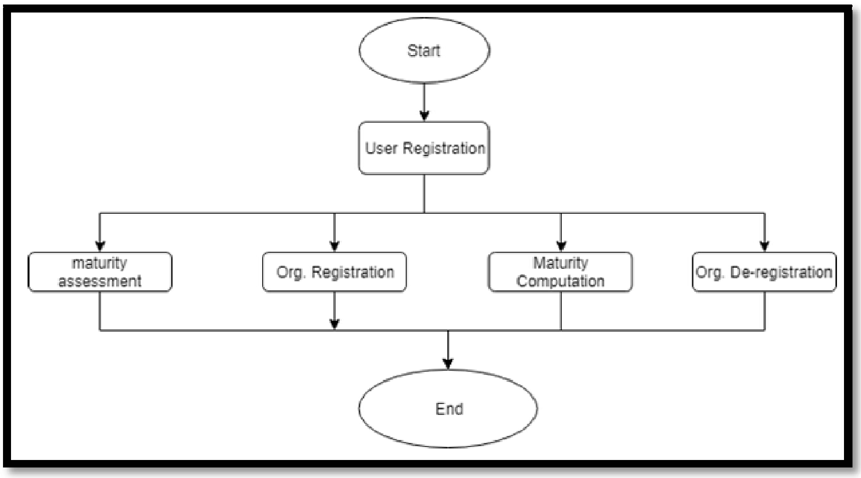

Figure 2: Flow Chart of WBRM Prototype

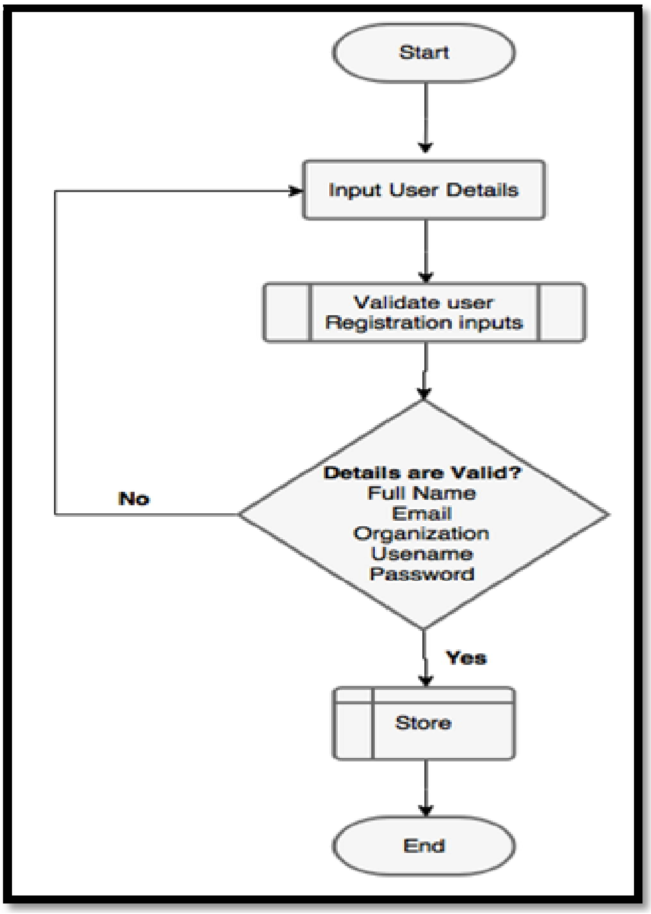

Figure 3: Registration Process Flowchart (Author, 2018)

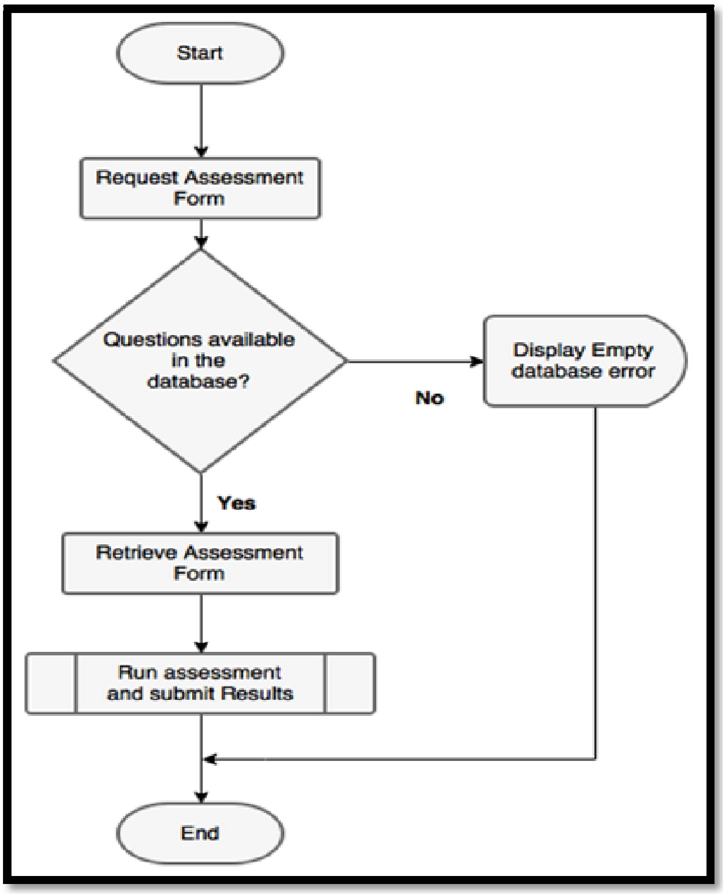
Start
Request Assessment Form
Questions available in the database?
No
Display Empty database error
Yes
Retrieve Assessment Form
Run assessment and submit Results
End

Figure 4: Maturity Computation Logic Flowchart (Author, 2018)

5. Model code logic

The maturity regression equation implementation logic is realized in a prototype for overall goal realization. Also, it conforms accordingly to simulation modelling that takes the form of computer programs, where logical arithmetic operations are performed in a prearranged sequence. This provides an added flexibility in model formulation and permits a high degree of realism to be achieved, which is particularly useful when uncertainties are an important aspect of decision making. The code logic was realized in the web-based prototype. The flowchart depicting the program logic is shown below in Figs. 5 – 6.

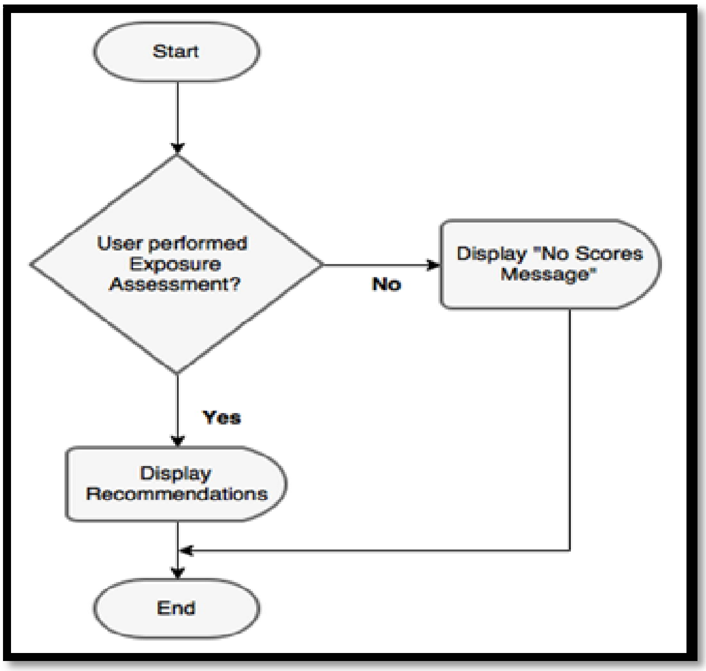
Start
User performed Exposure Assessment?
No
Display "No Scores Message"
Yes
Display Recommendations
End

Figure 5: Maturity Score Flowchart (Author, 2018)

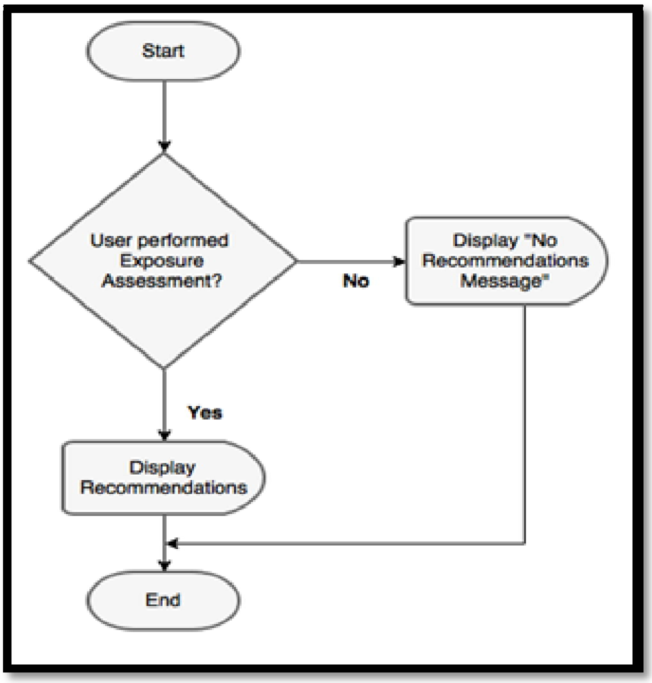
Start
User performed Exposure Assessment?
No
Display "No Recommendations Message"
Yes
Display Recommendations
End

Figure 6: Maturity Report Flowchart (Author, 2018)

6. Entity Relationship Diagram

The entity-relationship diagram (ERD) was used to graphically illustrate the maturity model conceptual implementation. It depicts the entities and relationship between entities in the model. ER modeling is a diagrammatic technique used to represent conceptual model of relational database. The entity is a real-world object or concept described in a database where as attributes are properties of the entity measuring the appropriateness of attribute groupings into relational schemas (Balaji et al, 2018). The Entity relationship diagram (ERD) for university information security maturity with four tables for data storage is as depicted below in Figs. 7.

Organization user registration and login authentication information: user_id, user_name. Email_ID, maturity, and password (SHA1 cryptographic algorithm).

Maturity Questions: category id, category name. System Questions information: Category_id, q uestion_id, recommendation, threshold score. Maturity information: user_id question_id, assessment date, assessment score.

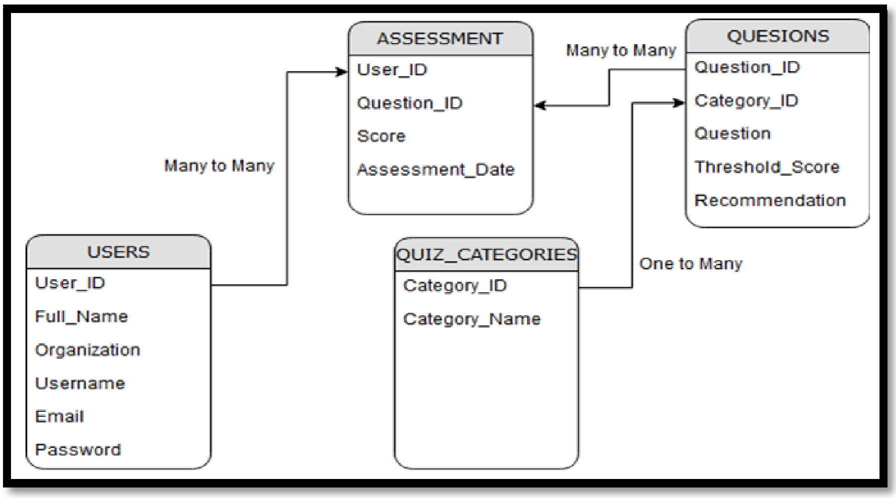

Figure 7: Entity Relationship Diagram (Author, 2018)

7. Recommendation

The proposed design can present a number of advantages towards determining information security maturity, these are:

- Organization User detail capture: These details are captured once, used many times and can be utilized for other incidental utilizations by authorized parties and stakeholders.
- Organization information security level: These is made available to relevant authorities including regulating parties.
- Organizational data availability: The availability of organizational data regarding information security is made available through a comprehensive report generated from the model.

- Easy to use system: The utilization of the Web based model for determining information security maturity provides a prototype having ease of access and utilization.
- Affordable operation: The use of the Web based model is relatively low cost because it provisions a low-cost facility to audit information security reediness.
- Report generation: The use of this prototype makes it possible to produce summary reports of information security maturity. This information is often not available unless through technical penetration test which is normally expensive.

7.1. Challenges

The main concern of utilizing the model relies on supplying the correct details that reflects the information security reality of the organization. The organization in-charge should enter correct details to get the correct official information security position of an organization.

7.2. Assumptions

Organizations provided accurate position on information security position for model design
Also, organizations should adopt the recommendation report to improve its information security level.
Organizations don't use the recommendation as a replacement of information security improvement program.

8. Conclusions

There's a great potential for a model that is readily accessible and provides a forecast through auditing of information security maturity level of an organisation. The picture of official information security maturity would offer a feasible mechanism for universities to improve their formation security.

9. Areas for Further Study

The model can also be extended and utilized by regulating bodies in coming up with an acceptable level of maturity for organizations. Also, it can serve as a basis for coming up with information security maturity models for other organizations aside from universities.

6. References

i. Accerboni, F., & Sartor, M. (2019). ISO/IEC 27001. In Quality Management: Tools, Methods, and Standards (pp. 245-264). Emerald Publishing Limited.

ii. Aydiner, A. S., Tatoglu, E., Bayraktar, E., & Zaim, S. (2019). Information system capabilities and firm performance: Opening the black box through decision-making performance and business-process performance. International Journal of Information Management, 47, 168-182.

iii. Clinton, L., & Whisnant, R. (2019). Business Model Innovations for Sustainability. In Managing Sustainable Business (pp. 463-503). Springer, Dordrecht.

iv. Curry, M., Marshall, B., Crossler, R. E., & Correia, J. (2018). InfoSec Process Action Model (IPAM): Systematically Addressing Individual Security Behavior. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 49(1), 49-66.

v. Englbrecht, L., Meier, S., & Pernul, G. (2019). Toward a Capability Maturity Model for Digital Forensic Readiness. In Innovative Computing Trends and Applications (pp. 87-97). Springer, Cham.

vi. erzner, Harold. (2019). Using the project management maturity model: strategic planning for project management. Wiley.

vii. Ingla, A., Ahuja, I. S., & Sethi, A. S. (2019). An examination of effectiveness of technology push strategies for achieving sustainable development in manufacturing industries. Journal of Science and Technology Policy Management, 10(1), 73-101.

viii. Laeeq, K., & Memon, Z. A. (2019). Scavenge: an intelligent multi-agent-based voice-enabled virtual assistant for LMS. Interactive Learning Environments, 1-19.

ix. Malik F. Saleh Management Information Systems, Chair Prince Mohammad Bin Fahd University Al Khobar, 31952, Saudi Arabia, 2011

x. Qazi, N., McElholm, M., & Maguire, L. (2018). A Model-View-Controller (MVC) architecture for contextual visualisation of task-based multi-dimensional energy KPIs in a manufacturing process. International Journal of Ambient Energy, 39(4), 406-413.

xi. Suwito, M. H., Matsumoto, S., Kawamoto, J., Gollmann, D., & Sakurai, K. (2016). An Analysis of IT Assessment Security Maturity in Higher Education Institution. In Information Science and Applications (ICISA) 2016 (pp. 701-713). Springer, Singapore.

xii. Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-Device Risk Management Model: A Case Study from a South African Organisation. The Electronic Journal of Information Systems Evaluation, 22(1).

xiii. Wong, H., Neary, D., Jones, E., Fox, P., & Sutcliffe, C. (2019). Pilot capability evaluation of a feedback electronic imaging system prototype for in-process monitoring in electron beam additive manufacturing. The International Journal of Advanced Manufacturing Technology, 100(1-4), 707-720.