AN EXTENDED SECURITY MEASUREMENT FRAMEWORK FOR OPEN-SOURCE ENTERPRISE RESOURCE PLANNING SOFTWARE SECURITY

Jane Wanjiru Njuki, Geoffrey Muchiri Muketha and John Gichuki Ndia

School of Computing and Information Technology,
Murang'a University of Technology, Kenya

ABSTRACT

Modern organizations are adopting new ways of measuring their level of security for compliance and justification of security investments. The highly interconnected environment has seen organizations generate lots of personal information and sensitive organizational data. Easiness in automation provided by open-source enterprise resource planning (ERP) software has accelerated its acceptability. The study aimed at developing a security measurement framework for open-source ERP software. The motivation was twofold: paradigm shift towards open-source ERP software and the need for justified investment on information security. Product quality evaluation method based on ISO 25010 framework guided the selection of attributes and factors. A security measurement framework with security posture at the highest level, attributes and factors was developed presenting a mechanism for assessing organization's level of security. Security posture promotes customers' confidence and gives management means to leverage resources for information security investment. The future work includes definition of metrics based on the framework.

KEYWORDS

Measurement framework, Attributes, Factors, open-source ERP software, security posture

1. INTRODUCTION

Modern organizations are adopting new ways of measuring their level of security for compliance and justification of security investments. The highly interconnected environment has seen organizations generate lots of personal information and sensitive organizational data [1] Easiness in automation provided by open-source enterprise resource planning (ERP) software has accelerated its acceptability [2] [3]. The rigidity and hefty costs associated with proprietary ERPs has prompted adoption of open-source ERP software by small, medium and large organization[4]. Large organizations are moving from their legacy IT systems by integrating open-source ERP modules such as customers' relations management (CRM) and human resource management (HRM) [5] [6] [7]. The information security concerns of modern organizations is therefore in the realm of ERPs.

Enterprise resource planning software is implemented under highly internetworked environment with real-time interactions between functions. These interactions involve a three tier interface setup with a database, network and user interface [6]. This technical and module architectures complicate the security of the ERPs by presenting a wider attack surface since each of these interfaces could be an entry point for intruders intending to harm the system [8]. Organizations implementing ERPs are prone to vulnerabilities, threats and attacks which get into these systems via the broadened attack surface. Proprietary ERPs have the advantage of developers taking

responsibility to address and resolve bugs reported in their software through their system support team [7]. These support teams provide users with security updates in the form of patches and sometimes software upgrades. However, some of the bugs published in the national vulnerability database (NVD) and common vulnerabilities scoring systems (CVSS) affecting the said proprietary ERPs may remain unattended for a long duration. On the other hand, open-source ERP published bugs are addressed by the community of developers as soon as they are announced [4]. Sometimes organizations miss on the updated patches or versions depending on the adoption mode.

Security measurement enables quantification of security in a manner that aids in comparison, contrast and ability to make decisions on where organizational resources should be spent [9]. Security measurement framework presents an essential way to understand and manage information security based on security attributes or factors. To this end open-source ERP software has been widely adopted and hence its security needs a measurement framework that will aid in assurance of security posture for the adopting organizations. The motivation to design this proposed framework was due to a lack of any existing security measurement framework targeting open-source ERP software.

The following sections presents background, section three presents methods, section four results, section five discussion, section six framework operationalization and section seven conclusion and future work.

2. BACKGROUND

2.1. Characteristics of Security Measurement Framework

In order to design a security measurement framework, there is need for understanding the kind of measures to be taken in the system under investigation. According to measurement theory, there must be an object or an entity whose measurements are taken. This object must possess some measurable attributes or characteristics. Measurement is the process of assigning numbers or symbols to the identified attributes of an entity in the real world according to clearly defined rules [9] [10] [11]. Measuring something means having knowledge about it and being able to express it in numbers. Security is an important element in the performance and sustainability of any organization as it provides a basis for trust and confidence, hence the need for assurance of security posture.

Measurement entails identification of an attribute's acceptable behaviour, collection of data about the attribute and presentation of a quantification measure for the attribute as described in the measurement theory and echoed by several scholars including [9] [12] [13] [14]. This attribute must be measurable either directly or indirectly [15] [16] [17] [18] [19]. Quantification of measurement requires consideration of precision which is the limit of details that can be measured and distinguished, concerns of repeatability (accuracy), integrity of measurement data, systems and processes of measurement, and utility which is about measuring things that matter [1] [14].

Measurements are mainly used for assessment or prediction and there is a need for measurement activities to have clear objectives as to whether the measures are intended for assessment or prediction [10] [14]. A measure can be sufficiently determined by three parameters namely attribute, scale and unit of measure [16] and it is important to ensure validity, precision and accuracy of the said measure [20]. An attribute refers to the aspect of the entity that is being measured, a scale of measurement is the quantitative yardstick that provides measuring unit and

scope for the attribute [16]. Five types of measurement scales have been identified as nominal, ordinal, ratio, interval and absolute [21] [22]. These scales provide a mechanism for quantifying the attribute's measure. Hence the kind of security measurement framework designed should provide a means to clearly identify attributes, scales and units of measurement.

Information security in an organization is greatly influenced by the interactions between technology, environment and individuals. Thus any security measurement framework must take into consideration the role each plays. A system is deemed to be as secure as its weakest link [9]based on the interactivity of its components. Operational security of any software depends mainly on the technological environment and behavioral aspects of the system users.

2.2. Security Attributes Based on Various Frameworks

This section presents measurement of information security and attributes as identified in some of the existing frameworks. The identified attributes and concepts will be used in conceptualization of the extended security measurement framework.

2.2.1. Software Product Quality Framework - ISO/IEC 25010

This is a software product quality framework which identifies eight software quality attributes and their sub-attributes [23]. Software products are required to comply with quality standards in ISO 25010 during the development process. The attributes are categorized as functional and non-functions with a need to consider both in the software development lifecycle. Functional attributes are directly measured to ascertain the quality of the software while the non-functional attributes are indirectly measured. ISO 25010 identifies security as a non-functional software quality attribute with confidentiality, integrity, non-repudiation, authenticity and accountability as security sub-attributes [24] [25].

The Consortium for IT Software Quality (CISQ) framework extends the ISO 25010 framework and adds the compliance attribute for the purpose of CISQ certification. On matters of security the framework included SQL injection, cross-site scripting and buffer overflow as architectural considerations for CISQ measures [23] based on the severity of their impact on operational problems or cost of ownership. Software certification under this framework requires compliance with reliability, security, performance efficiency and maintainability. Weaknesses in the mentioned characteristics are identified and assigned numbers using the common weakness evaluation (CWE) method.

ISO 25000 which is an extension of ISO 9126 series has been adapted severally to define software quality metrics [25]. It extended the six factors and twenty-one sub-factors to eight attributes and thirty-one sub-attributes by including security and compatibility sub-attributes. Further extension has been done to specifically address quality of ERP software [25] by adding supportability, search ability and archive ability sub-factors. This gave rise to a framework with eight attributes as per ISO 25010 and thirty-four sub-attributes. The three sub-attributes were placed under usability (supportability and search ability) and security (archive ability). The general system properties that are used to determine the security level are identified as secure user management, session management, access management, unique identification, logging completeness, strength of proof, input/out verification, secure authorization, authorized data access, authorized data storage and secure data transport.

2.2.2. A Reference Measurement Framework of Software Security Product Quality (SPQNFSR)

This reference measurement framework was developed based on ISO/IEC software quality requirement evaluation (SQuaRE) 25000 series and common software measurement international consortium (COSMIC) ISO/IEC 19761 [26]. The purpose of the framework was to identify the software security requirement at the early stage of software development by considering functional and non-functional security requirement (NFR) of the software quality. The framework identifies entities or attributes for measurement based on three objectives namely; measurement objective of security requirements, measurement point of view of security and the intended use of measurement results [26]. Further, software security requirement concepts to be measured have been categorized into external security entities (auditability, integrity and confidentiality) and internal security entities (data encryption).

2.2.3. Security, Privacy and Dependability (SPD)

The security, privacy and dependability software evaluation framework takes into considerations the vulnerabilities that affect these three aspects of a software. The framework allows for computation of an SPD composite score and identifies control measures for each of the identified attribute for the three aspects [27]. The framework provides security controls and measures for confidentiality, integrity and availability. In privacy aspect, controls for collection, access and usage are considered and in dependability controls for reliability, maintainability and safety. Attack surface size based on each aspect and damage potential effort resulting from exploitation of vulnerabilities and anomalies affect the SPD value.

The SPD framework implements security, privacy and dependability existing standards like common vulnerability evaluation (CVE), open source security testing methodology manual for security, ISO/IEC 29100, 27018 standards, European Data Protection Directive 95/46/EC for privacy, and IEC 60300 standard for dependability [27]. Using these standards an SPD surface is established using security, privacy and dependability. An SPD value is computed based on systems porosity, controls and dependability. On the part of security confidentiality, integrity and availability controls are used as indicators. This underscores the importance of these aspects of information security. On the other hand, personal identification information (PII), reliability and maintainability cover for privacy and dependability respectively. It is worth noting that privacy is an aspect of confidentiality while dependability is an aspect of availability.

2.2.4. Towards A Framework for Security Measurement

This framework provides a means to quantify security of computer systems and determine how resources would be utilized to secure these systems by obtaining attribute measurements. Measuring any component starts with knowing what to measure by selecting security properties to be measured [9] in terms of security concerns. These concerns can be identified as confidentiality, integrity and availability of information in the systems. These are security attributes which are affected by several factors for which measurable controls are instituted. To measure these factors, scales and units must be selected in order to determine how measurement can be achieved [9]. Plausibility and accuracy of units and scales should be put into consideration if meaningful measures are to be attained. It is also important to have a way of estimating the values since factors affecting security may be a single component in the system or as result of the system's interaction. These attributes are not directly measurable and a good estimation methodology should be applied.

High level security attributes are broken down into individual low-level measurable components [9]. This gives rise to the attribute, factor criteria model where the factors affecting an attribute are identified and a criterion for measuring each factor's security established. The framework presents a method of measuring confidentiality using cryptographic protection, physical security and software access control as factors. These factors are further decomposed to measurable criteria into algorithm and keys & secrets, physical media and accessibility, effectiveness and reliabilities. Integrity, non-repudiation and authenticity are also treated to a similar decomposition.

The security attributes are measured in terms of qualities hence they cannot be directly measured. Therefore, each of the security attributes is associated with a measurable factor for which some criteria for measurement is formulated.

3. METHOD

This section presents the methods used in designing a security measurement framework.

3.1. Research Questions

The research questions addressed in this study include the following:

RQ1. Which characteristics should be considered when designing a security measurement framework?
RQ2. How would these characteristics aid in the design of the security measurement framework?
RQ3. What components should the security measurement framework constitute and how are the components interlinked?

3.2. Identification of Characteristics

The product quality evaluation method (PQEM) is used to analyse, study, measure and assess the quality of a software product in five steps [28]. This method was applied to analyse characteristics for measuring security of the open-source ERP software. The process involved identification of security attributes requirements (SARs) through selection of security attribute, factors and specification of attribute requirement. Attributes selected map to ISO 25010 and ISO/IEC 27001, while factors selected were selected from the vulnerabilities identified for open-source software.

Characteristics show essential open-source ERP software components in the environment that affect its ability to perform tasks correctly, accurately and completely within the specified time [26]. The components in the environment include factors that present vulnerability to the software. Exploitability of loopholes in these factors causes software insecurity. Review of existing literature helped in identifying factors that contribute to open-source ERP software insecurity.

3.3. Linking Security Measurement Framework Components

Systems attack surface determines security measurement framework components. A system's attack surface is described as the set of ways in which an adversary enters a system and potentially causes damage. Resources utilised in an attack include system entry and exit points, channel used and the data [29]. An attack surface measure indicates the susceptibility of a system to attacks [27] [16].

Existing security frameworks and models were analysed to help identify the various causes of insecurity. Identified causes were treated as factors with a mapping to the security attributes in ISO 25010 and ISO/IEC 27001. To determine the attack surface component analysis and analytical process methods were used with the identified factors.

3.4. Mapping the Security Measurement Framework Components

Mapping of security attributes presented in ISO 25010 and ISO/IEC 27001 with the factors that cause software insecurity was done through categorization. Data protection and privacy regulations require adherence to confidentiality, integrity and availability principles of information security. The categorization identified factors affecting each of these attributes. These factors were further linked to controls instituted to mitigate against exploitation.

The extended security measurement framework constitutes of attributes in the ISO 25010 and ISO/IEC 27001; confidentiality, integrity and availability with an addition of auditability and trackability. This has given rise to an extended security measurement framework (ESMF) with eight attributes. Factors causing open sources software insecurity include delayed software updates, inadequate training, insufficient control of access rights, single authentication, unauthorized software, failure to comply, inadequate documentation, and unlimited trust boundary. The ESMF therefore, constitutes eight attributes and eight factors. Security posture is attained through effectiveness of controls instituted to mitigate against vulnerabilities emanating from exploitation of attack surface resulting from these factors. Hence, to enable measurement, technical, logical and administrative controls were included in the framework.

4. RESULTS

This section presents the results of the study.

4.1. RQ1: Which Characteristics should be Considered When Designing the Security Measurement Framework?

The proposed extended security measurement framework (ESMF) integrates security and privacy requirements for information security compliance. The extended framework attributes include confidentiality, integrity, availability, non-repudiation and authentication from ISO 25010 software quality framework and ISO/IEC 27000 information security model [9] [30]. The real-time transactions aspect of the open-source ERP software necessitated addition of two more attributes namely auditability and trackability.

Security posture of an organization is determined through measurement of effectives of controls instituted against vulnerabilities caused by identified factors. These factors include delayed software updates, insufficient control of access rights, single authentication, inadequate training, use of unauthorized software, failure to comply, inadequate documentation and unlimited trust boundaries. Exploitation of any vulnerability presented by these factors causes loss of information confidentiality, integrity and availability. Non-repudiation, authenticity auditability and trackability were considered as integral parts of the principles. Mitigation against vulnerabilities involves institution of administrative, logical and technological controls.

The architecture comprises of three levels; at the highest level we have security posture, followed by attributes in the second highest level, then we have the identified factors followed by the type of controls and at the lowest level. This relationship is shown in Table 1.

Table 1: Relationship between factors, controls and security attributes

Factor	Type of control	Categorization of Effect		
		Confidentiality	Integrity	Availability
Delayed software updates	Technical/ Logical	√	√	√
Insufficient control of access rights	Technical/ Logical	√	√	
Single authentication	Technical/Logical/Administrative	√	√	
Inadequate training	Administrative	√	√	√
Use of unauthorized software	Administrative		√	√
Failure to comply	Administrative		√	√
Inadequate documentation	Administrative	√	√	√
Unlimited trust boundaries	Administrative	√	√	√

4.2. RQ2: How would these Characteristics Aid in Designing a Security Measurement Framework?

Secure software is characterized by security of information in terms of confidentiality, integrity and availability. Security posture score informs the management of the level of security and forms a basis for informed decision making in terms of security investment. Security posture answers the questions like “are we secure?”, “how secure are we?”, “for how long will we remain secure?”. To answer these questions among others requires measurements and metrics. ESMF will help in answering these questions by pointing out where the problem is and guiding on what should be done. This is achieved through identification of factors that introduce vulnerabilities and control measures necessary to mitigate the vulnerabilities. The effectiveness of the instituted controls determines the security posture.

The identified security attributes have been summarized into three security principles, confidentiality, integrity and availability. The attributes were linked to the eight factors, delayed software updates, insufficient control of access rights, inadequate training, single authentication, use of unauthorized software, failure to comply, inadequate documentation and unlimited trust boundaries. Technical, logical and administrative controls whose effectiveness determines security posture were mapped with the factors.

The inter-linking of attributes, factors and controls forms the ESMF architecture as illustrated in Figure 1. Security posture is measured through the effectiveness of technical, logical and administrative controls. Each of the factors has some identifiable characteristic that is measurable. Compliance with requirement for the identified control measure for each characteristic determines the security level hence security posture. Software updates are measured using versioning and patches, so delay in upgrading to a newer version and failure to install available update patches presents a vulnerability. Action or inaction of the part of users while interacting with the system due to inadequate training leads to some level of insecurity. Similarly, insufficient control of access rights, use of unauthorized software, failure to comply, unlimited documentation and unlimited trust boundary have identifiable characteristics which forms the basis for institution of either technological, logical or administrative controls.

The ESMF eight attributes identified earlier have been summarized into three namely; confidentiality, integrity and availability as shown in Figure 1. The attributes were summarized based on the information security principles and the fact that non-repudiation, authenticity,

accountability, auditability and trackability are details associated with the information principles to help in the institution of control measures. The hierarchical illustration in Figure 1 therefore, has three attributes, eight factors and three controls. The architecture informed the ESMF framework shown in Figure 2.

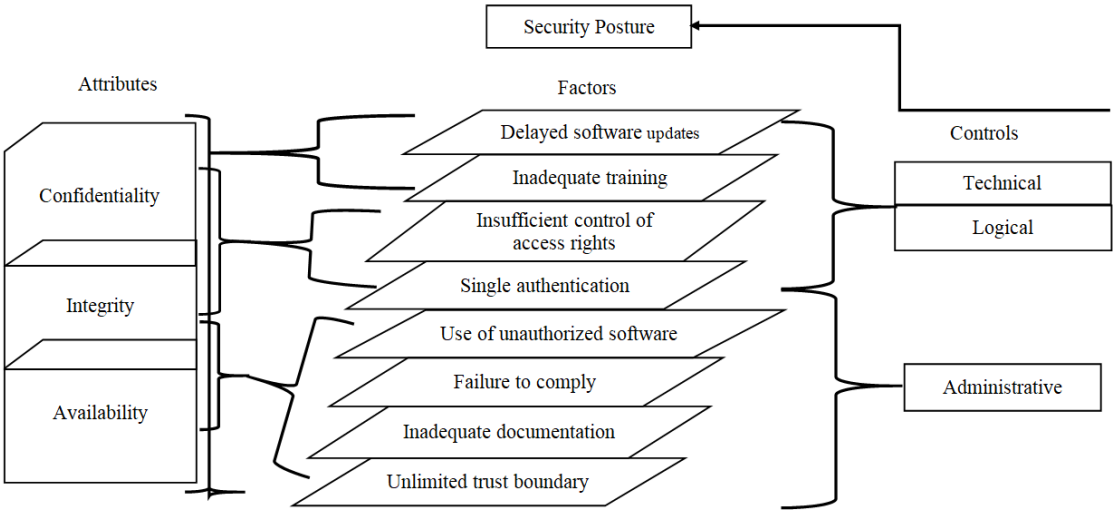

Figure 1: Extended software measurement framework architecture

4.3. RQ3: What Components should the Extended Security Measurement Framework Constitute and How are the Components Interlinked?

The extended security measurement framework (ESMF) constitutes confidentiality, integrity and availability information security principles as defined in ISO/IEC 27001 and stated as quality attributes in ISO 25010. The principles have integrated non-repudiation, authenticity, accountability, auditability and trackability. The level of compliance with these principles determines the security posture of an organization. Figure 2 presents the extended security measurement framework by stating eight security sub-attributes under the security attribute of the software product quality. To measure the attributes eight factors have also been identified. The framework highlights the components in terms of attributes and factors with no direct causal effect established between each attribute and the factors.

Figure 2: Extended security measurement framework

5. DISCUSSIONS

5.1. Relationship of the Security Measurement Framework Components

Security posture of an organization is determined by effectiveness of controls instituted to safeguard against exploitation of loopholes in identified factors. Delayed software updates may result from either delayed upgrades of software versions or software security update patches. This situation is managed through version and patch management which is made possible through the ESMF. Organization should have mechanisms to control access right assigned to internal and external users since ERP systems allow use of intra and extra nets. Proper management of access rights through tracking of users' access rights and regular reviews reduces the vulnerability emanating from the inadequate control of access rights and single authentication. User management in terms of training and monitoring of user activities provides a solution to vulnerabilities caused by inadequate training, use of unauthorized software and unlimited trust boundaries. Auditing the organization's security activities ensures proper documentation and reveals any weaknesses in the open-source ERP software. This helps in addressing compliance and inadequate documentation issues.

Security assurance is achieved through measures and metrics that show the security status or posture. To measure compliance with confidentiality, integrity and availability (CIA), the level of system vulnerability is determined by effectiveness of controls instituted for identified factors. The extended security measurement framework presents a means to identify factors, controls and link them to security attributes. The three components form the basis for development of extended security framework for open-source ERP software.

5.2. Security Measurement Framework Architecture

The security measurement framework architecture comprises of attributes which are affected by exploitation of vulnerabilities presented by identified factors. Controls instituted to mitigate the identified factors ensure security of software. The effectiveness of the controls determines the security posture. Open-source ERP software has known vulnerabilities as any other open-source software. Extended security measurement framework assists organizations implementing open-source ERP software in mapping attributes, factors and controls. Utilization of the framework would lead to improved security posture hence increased customer confidence and enhanced decision making of investment in information security.

5.3. Extended Security Measurement Framework Design

Extended security measurement framework for open-source ERP software has been developed to assist in establishment of security posture. Compliance with confidentiality, integrity and availability by any organizations leads to adherence to data protection and privacy as required by several global authorities. The extended security measurement framework brings to light vulnerabilities associated with open-source software that can be exploited due to their public nature. The framework defines main attributes affected by the determined factors of open-source ERP software security and determines requisite controls. Exploitation of any vulnerability presented by identified factors leads to modification and fabrication of information which are confidentiality and integrity issues. Also unavailability of services through ineffective of instituted controls affects all the three principles meaning a breach in information security.

6. FRAMEWORK OPERATIONALIZATION

The ESMF can be used by small, medium, large organization using open-source ERP software. This section presents scenarios where the framework would be applicable with the three categories of organizations.

6.1. Case 1: Small Organizations

Small organization is defined as an entity with employees ranging from 1 to 50 in number for the purpose of this study. These organizations are mostly characterized by lack of necessary management structures with main focus being the entity's business operations. Secondly, there are never enough resources to fully integrate the requisite ICTs with the daily operations hence the inclination towards open-source software which has lower capital investment except for the hardware components. Depending on the selected adopted mode the entity may be confronted by some insecurity issues.

Let us take a case of an organization which has decided to download the open-source ERP software and customize it through their IT department. One of the problems such an organization may face is lack of requisite skills to fully customize the software.

The open-source software community keeps on working on the said software and by the time the IT team finalizes with customization the software may have evolved to several versions and security patches. This is where the issue of delayed software updates comes into play.

The organization should therefore ensure proper documentation of the software version and the kind of customization done. Applying ESMF the organization is able to track the upgrades to the said software in terms of versions and security patches. The framework prompts institution of security controls such as version and patch management leading to identification of any threats due to the use of older or un-updated versions. Requirement for information security applies to all types of organization. Therefore, small organizations' compliance with CIA is made possible through the uses of the ESMF.

6.2. Case 2: Medium Size Organizations

Medium size organizations are defined as entities with between 51 and 200 employees for the purpose of this study. Unlike most small organizations, these entities have more established structures and higher capital investment in ICTs. It is also most likely that the organization has a well-established IT function with requisite skills and/or has contracted a vender and even out-sources IT experts. Therefore, customization of open-source ERP software would be more comprehensive. Like the small organizations, medium organization may be confronted with several security issues emanating from the factors identified in the ESMF.

Medium size organizations use intranets and extranets in their operations presenting them with internal and external users. The open-source ERP software allows the interaction of these users during the enterprise operations. The users include employees, suppliers and customers who are given different levels of access to the system resources. The issue of insufficient control of access rights and single authentication are some of the causes of insecurity with these organizations.

Let us take a situation where and organization has assigned rights to and employees who later leaves the organization. If the organization fails to revoke the employees access rights upon exit, and the employee was in a position to transact business on behalf of the organization remotely,

then the employee may continue to use the access and may even harm the system. Secondly, if the IT personnel customizing the open-source ERP software are outsourced and their rights are not revoked after they finish their assignment, then they also pose a threat. Also, the different categories of users should have different levels of access right and where one is a customer and an employee, proper mechanism to control the rights should be institute. The administrators of systems usually have the capability of accessing all the functionalities of the system which brings the issue of single authentication. The organization should implement role based authentication to ensure people with different roles are not misusing privileges assigned to certain roles.

Attributes and factors in the ESMF are guiding principles in ensuring the security of the open-source ERP software. Trackability and auditability attributes help in identifying how the access rights are assigned and controlled hence alleviating the problem of insufficient control of access rights and single authentication. It is also possible to establish trust boundaries with the different users. This application provides a means to for medium size organizations to comply with CIA principles of information security.

6.3. Case 3: Large Organizations

Large organizations are defined as entities with over 200 employees for the purpose of this study. These organizations are characterized by interactions over a variety of ICTs including the internet for real time transactions. To a large extent these organizations have well established structures for business transactions as well as for the ICT. The level of automation in this type of organizations is high with most of them having implemented legacy IT systems and moving towards incorporation of open-source components. Some of the components that are being incorporated by these large organizations include open-source ERP modules such as customer relationship management and human resource.

Large organizations are leveraging on the customizable capabilities in the open-source ERP software and the capital IT infrastructure investment accumulated over the years. The expansive utilization of different facets of ICTs leads to an increased attack surface level for these organizations. The amount of data and transactions carried out serves an appetizer to the would be attackers. Security issues raised for the small and medium organizations apply to the large organization. Accountability and non-repudiation attributes are crucial in this kind of organizations due to the large numbers and varieties of their users.

To demonstrate how ESMF may be applied in these organizations, we look at the interactions and role played by the identified factors. The organization may have automated some of the controls to ensure their open-source ERP software is secure. For example, software updates may be automated in such a manner that it is possible to detect newer versions and patches from the open-source ERP software project database. This would ensure the issue of delayed software updates does not cause insecurity. Other automations may include access control and single authentication where it could be possible to detect and automatically review access rights based on the user role. However, it may not be possible to automate detection of inadequate user training, inadequate documentation and unlimited trust boundaries.

Trackability and auditability of real time transactions in these organizations would promote security through review of trust boundaries and prompting user trainers where there is evidence of erroneous transactions. ESMF has identified eight attributes and eight factors that would aid the large organizations in ensuring high levels of security. With proper security controls, acceptable security posture would be realized hence promoting customers' confidence. With high levels of investment in the IT infrastructure and the requirement for compliance with information

security principles (CIA), ESMF would be of great benefit. Continued investment in information security would be informed by the application of ESMF for open-source ERP software.

7. CONCLUSIONS

In conclusion we have developed an extended security measurement framework for open-source ERP software, incorporating attributes defined in ISO 25010 and ISO/IEC2700. Eight factors that cause vulnerability in open-source ERP software were defined as delayed software updates, inadequate training, insufficient control of access rights, single authentication, use of unauthorized software, failure to comply, inadequate documentation and unlimited trust boundaries. Security measurement framework architecture formation involved mapping the factors and attributes to technical, logical and administrative controls.

The extended structure consists of eight sub-attributes namely confidentiality, integrity, non-repudiation, accountability, authenticity and availability according to quality attribute of the product quality and two additional attributes, auditability and trackability and the eight factors mentioned earlier to complete the extended security dimension framework.

The developed architecture of the effectiveness of the introduced controls shows the level of security or lack of security. To ascertain the security level, effectiveness of instituted controls should be measured by use of metrics. Measurements and metrics provides a means to present information security reports which are easier to understand and useful for decision making. Established security posture promotes accountability, customer confidence and justified investment in security. Therefore, we recommend validation of the extended measurement framework through an expert opinion survey and an experiment. This will be presented in our next publication.

REFERENCES

[1] A. Jaquith, *Security Metrics Replacing Fear, Uncertainity, and Dout*, vol. 53, no. 9. 2017.

[2] N. Brehm and J. M. Gomez, "Distribution of ERP System Components and Security Considerations," *Emerg. Trends Challenges Inf. Technol. Manag.*, vol. 1–2, pp. 494–501, 2006.

[3] F. Mahmood, A. Z. Khan, and R. H. Bokhari, "ERP issues and challenges: a research synthesis," *Kybernetes*, vol. 49, no. 3, pp. 629–659, 2020, doi: 10.1108/K-12-2018-0699.

[4] A. D. Kozhukhivskyi and O. A. Kozhukhivska, "Erp-System Risk Assessment Methods and Models," *Radio Electron. Comput. Sci. Control*, vol. 0, no. 4, pp. 151–162, 2020, doi: 10.15588/1607-3274-2020-4-15.

[5] T. Mladenova, "Open-source ERP systems: An overview," *2020 Int. Conf. Autom. Informatics, ICAI 2020 - Proc.*, 2020, doi: 10.1109/ICAI50593.2020.9311331.

[6] M. El Mohadab, B. B. Khalene, and S. Safi, "Enterprise resource planning: Introductory overview," *Proc. 2017 Int. Conf. Electr. Inf. Technol. ICEIT 2017*, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/EITech.2017.8255306.

[7] D. Petrov and N. Obwegeser, "Adoption Barriers of Open-Source Software: A Systematic Review," *Proc. 27th Int. Conf. Inf. Syst. Dev. Des. Digit. ISD 2018*, no. March, 2018.

[8] G. R. Gosavi and V. M. Thakare, "Mathematically Modeled Algorithm for Intelligently Customized Optimization of an Erp," *Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018*, 2018, doi: 10.1109/ICCUBEA.2018.8697418.

[9] C. Wang and W. a. Wulf, "Towards a framework for security measurement," *20th Natl. Inf. Syst. Secur. Conf. Balt.*, pp. 1–15, 1997.

[10] N. Fenton, "Software Measurement: A Necessary Scientific Basis," *IEEE Trans. Softw. Eng.*, vol. 20, no. 3, pp. 199–206, 1994, doi: 10.1109/32.268921.

[11] C. Kaner and W. P. Bond, "Software Engineering Metrics : What Do They Measure and How Do We Know ?," *10Th Int. Softw. Metrics Symp. Metrics 2004*, vol. 8, pp. 1–12, 2004.

[12] U. P. D. Ani, H. M. He, and A. Tiwari, "A framework for Operational Security Metrics Development

for industrial control environment A Framework for Operational Security Metrics Development for Industrial Control Environment .," no. January 2019, 2018, doi: 10.1080/23742917.2018.1554986.

[13] J. Hallberg, A. Hunstad, and M. Peterson, "A framework for system security assessment," *Proc. from 6th Annu. IEEE Syst. Man Cybern. Inf. Assur. Work. SMC 2005*, vol. 2005, pp. 224–231, 2005, doi: 10.1109/IAW.2005.1495956.

[14] W. Krag, *PRAGMATIC Security Metrics: Applying Metametrics to Information Security*. Taylor & Francis, 2013.

[15] R. W. Saaty, "The analytic hierarchy process-what it is and how it is used," *Math. Model.*, vol. 9, no. 3–5, pp. 161–176, 1987, doi: 10.1016/0270-0255(87)90473-8.

[16] V. Verendel, "Quantified Security is a Weak Hypothesis."

[17] B. Reeve, "An introduction to modern measurement theory," *Natl. Cancer Institute, USA*, no. 301, 2002.

[18] R. R. Aparasu, "Measurement theory and practice," *Res. Methods Pharm. Pract. Policy*, no. Donabedian 2003, 2005.

[19] D. J. Hand, "Statistics and the Theory of Measurement," *J. R. Stat. Soc. Ser. A (Statistics Soc.*, vol. 159, no. 3, p. 445, 1996, doi: 10.2307/2983326.

[20] K. Julisch, "A Unifying Theory of Security Metrics with Applications with Applications," *Security*, p. 19, 2009.

[21] B. Karabey and N. Baykal, "Information Security Metric Integrating Enterprise Objectives," *43rd Annu. 2009 Int. Carnahan Conf. Secur. Technol.*, pp. 144–148, 2009, doi: 10.1109/CCST.2009.5335549.

[22] A. Arabsorkhi, "Security Metrics : Principles and Security Assessment Methods," *2018 9th Int. Symp. Telecommun.*, pp. 305–310, 2018.

[23] B. Curtis, "Update on CISQ and ISO 25010," 2019.

[24] I. Saptarini, S. Rochimah, and U. L. Yuhana, "Security Quality Measurement Framework for Academic Information System (AIS) Based on ISO/IEC 25010 Quality Model," *IPTEK J. Proc. Ser.*, vol. 0, no. 2, p. 128, 2017, doi: 10.12962/j23546026.y2017i2.2310.

[25] E. Peters and G. K. Aggrey, "An ISO 25010 Based Quality Model for ERP Systems," vol. 5, no. 2, pp. 578–583, 2020.

[26] K. T. Al-Sarayreh, M. Alenezi, M. Zarour, and K. Meridji, " A reference measurement framework of software security product quality (SPQ NFSR) ," *IET Inf. Secur.*, vol. 15, no. 1, pp. 23–37, 2021, doi: 10.1049/ise2.12002.

[27] G. Hatzivasilis, I. Papaefstathiou, and C. Manifavas, "Software Security , Privacy , and Dependability Metrics and Measurement," *IEEE Softw.*, vol. 33, pp. 46–54, 2016, doi: 10.1109/MS.2016.61.

[28] M. Falco and G. Robiolo, "Building a catalogue of ISO/IEC 25010 quality measures applied in an industrial context," *J. Phys. Conf. Ser.*, vol. 1828, no. 1, 2021, doi: 10.1088/1742-6596/1828/1/012077.

[29] M. Siavvas, D. Kehagias, D. Tzovaras, and E. Gelenbe, *A hierarchical model for quantifying software security based on static analysis alerts and software metrics*, vol. 29, no. 2. Springer US, 2021.

[30] M. Nicho, "A process model for implementing information systems security governance," 2017, doi: 10.1108/ICS-07-2016-0061.