A SYSTEMATIC LITERATURE REVIEW ON SECURITY INDICATORS FOR OPEN-SOURCE ENTERPRISE RESOURCE PLANNING SOFTWARE

Jane Wanjiru Njuki, Geoffrey Muchiri Muketha and John Gichuki Ndia

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

ABSTRACT

Open-source enterprise resource planning (ERP) software has become a preferred alternative for modern organizations due to its affordable cost, availability and ease of access. Open-source software allows access to customizable code which in most instances may have security loop holes due to the nature of its releases. The study is motivated by need for accountability and security assurance by stakeholders and the need for justification of investments towards information security. The objective was to analyse security indicators for open-source resource planning software. Papers and journals published between 2017 and 2021 from IEEE, ACM, Springer, arXiv, Wiley online library and EBSCO were reviewed. Out of the publications generated through the Google search, 62 publications were selected by reading the title, abstract, introduction and full text. Results indicate un-updated software, full access rights, inadequate training, failure to comply, single authentication and unauthorized software as some of the factors that indicate open-source enterprise resource planning software security. In conclusion effectiveness of mitigation measures to address these factors shows security or insecurity. Notably, there is need to institute security control measures and metrics for the identified factors to help assess security posture of enterprises during ERP software implementation. We recommend the design of security a measurement framework and definition of a metrics suite for assessing open-source ERP software security.

KEYWORDS

Open-source ERP software, vulnerabilities, software security, factors, indicators.

1. INTRODUCTION

ERP software systems can be referred to as corporate integrated information system incorporating all departments and structures of an enterprise into a single information and technological computer network to meet all the needs of individual units [3]. ERP systems aim at improving organizational competiveness, optimizing and boosting operational performance through digital transformation of customer experience [4].

Open-source enterprise resource planning (ERP) software has become a preferred alternative for modern organizations due to its affordability, availability and accessibility. Open-source software allows access to customizable code which in most instances may have security loopholes due to the nature of its releases [1]. As is the case in [1], our motivation is based on the need for accountability and security assurance by stakeholders and the need for justification of investments towards information security. Vulnerability life cycle affects the security of the open-source software (OSS) even though [1] posits several factors that contribute to OSS being supposedly more secure.

The results of the study are intended to enlighten researchers on existing gap in the open-source ERP software literature. The identified indicators form the basis for secure implementation of open-source ERP software.

The rest of the paper is organized as follows. In section two we present the background, in section 3 we present methods, in section 4 we present the results, in section 5 we present the discussion, and in section 6 we present the conclusion and future work.

2. BACKGROUND

The requirement to ensure data security and privacy by most governments across the globe has necessitated both public and private organizations to adopt strategies for assessing their security status. This is as a result of increased cyber-attacks targeting personal information and sensitive corporate data prompting global need for data protection. General data protection regulation (GDPR) [5] passed by the UK government heightened the need for legal considerations by the global community. Many other governments have come up with legislations to ensure implementation of information security mechanisms for data security and privacy [6][7]. Public organizations are required to comply with the requirements of ISO/IEC 27001 on information security management systems (ISMS) for assurance of information confidentiality, integrity and availability (CIA) [5]. Private organizations are also implementing ISMS to ensure compliance with data security and privacy requirements hence the need for secure software development [9] [10]. These requirements are well taken care of by the ISO/IEC 27001 standards [8][9]. Data security bleaches cost a lot resources to organizations in terms of legal litigations, damage of brand and loss of trust [10].

Open-source ERP software is being used by large, medium and small public and private organizations to leverage on information communication technologies (ICTs) due to its scalability [4]. Need for information security in the ERPs calls for institution of necessary security measures to comply with ISO/IEC 25010 and 27001 requirements on software quality and information security. ISO/IEC 25010:2011 categorizes safety and security as non-functional software quality factors [11] [12] [13] while ISO/IEC 27001 identifies confidentiality, integrity and availability (CIA) as principles of information security. Security of a software is indicated by measuring the effectiveness of controls instituted throughout software development cycle. However, at operational stages of ERP software implementation, some indicators of the security posture include use of updated versions of the software, ensuring access on a need to know basis, compliance with set standards among others

Estimates on cost of data breach reported in IBM annual report offers insights from 537 real breaches to help understand cyber risk in a changing world. This report estimated that data breach costs rose from USD 3.86 million to USD 4.24 million in 2021 which was the highest average total cost for the last 17 years of IBM report [14]. The McAfee estimates cybercrime costs at around $945 billion, or just over 1% of global Gross Domestic Product (GDP) [10] not to mention other hidden costs in terms of man hours, opportunity costs, system downtime among others.

Most public and private organizations use legacy IT systems whose integration become complex as the organization grows. To counter this complexity these organizations are moving towards ERP systems with commercial off the shelf packages dominating the scene [15]. Some of the ERP software adopted by large organizations include Sage Intacct, Oracle ERP cloud, Microsoft Dynamics 365 ERP and SAP. However, their implementation using the black box, very little customization options and poor integration with organizational processes are driving organizations towards open-source ERPs, hence their high rate of adoption.

Open-source software (OSS) has expanded from the operating systems like Linux to web servers, database, and Microsoft office-like applications among other systems including open-source ERP software [15]. OSS solutions are preferred because they offer a low total cost of ownership (TCO) and are also considered high quality systems because of their open and collaborative nature of development [4][5]. With OSS, bugs are fixed more quickly and user enhancements are made in time. Web-based projects such as Source forge have made collaborative development possible due to the ease of communication amongst distributed developers through the internet and support environments. Finally, the price of hardware has drastically dropped over the years contributing to the popularity of OSS including open-source ERPs.

There are several advantages accruing to open-source software including that source code is accessible and subject to inspection by a wide community of developers who are able to find and provide fixes for vulnerabilities [16]. However, at the operational stage, user action is paramount in security assurance due to the three tier architectural levels of security in the implementation of ERP system, namely, user application, network interface and the database. Alenezi and Zarour [18] identify information security awareness (ISA) as a starting point towards secure implementation of ERP systems. In agreement with the posts, it is important to identify factors that would lead to violation of information security in respect to open-source ERP software systems. These factors will serve as indicators of a secure implementation.

Challenges that decision makers perceive in their initial reasoning about Free/Libre and Open Source Software (FLOSS) integration have been investigated in [20]. This work identified technological, organizational, environmental and individual (TOEI) framework for categorizing barriers to adopting FLOSS. Open-source ERP software is also subject to these barriers though the work did not identify the factors that lead to the same. The current study investigated factors that affect open-source ERP software security after its adoption which serve as indicators for security. In [21], a systematic literature review on open-source software (OSS) evaluation, selection and adoption has analyzed selection models considering evaluation areas and factors addressed by OSS evaluation model. This work did not include security factors in its scope. Information security and data privacy are key in the current dispensation of organizational security posture requirements. This study brings out the indicators of security in open-source ERP software by identifying factors to be used in assessment of security posture.

3. METHOD

The systematic literature review method based on the guidelines for performing systematic literature review in software engineering [22][23] was used. The process started with planning, conducting and reporting the review. The review protocol included specification of the research questions and the methods to be used. The research question was, determination of factors that affect the open-source ERP software security. The formulation of search strategy involved consideration of the databases and the search criteria. Inclusion and exclusion criteria was specified based on the year and type of publication. A systematic literature review of academic and non-academic sources including peer reviewed journals and conference papers.

3.1. Research Questions

The research questions addressed in this study include the following:

RQ1. What factors indicate security of an open-source ERP software?
RQ2. What information security principles are affected by ineffective controls on the identified factors?

RQ3. How can the identified factors act as indicators for open-source ERP software security?

3.2. Search Criteria

The amount of existing data in the internet is enormous and using google search a lot of data was generated. The research work reviewed was retrieved from the IEEE explore, EBSCO, ACM digital library, arXiv, Springer, Wiley online library and Taylor & Francis databases. The retrieval involved use of the factors that affect open-source ERP software security as the search criteria in all the databases. The documents generated included white papers, conference papers, journal, books and book chapters. The work selected was considered on the basis of the title's, abstract's and the full article's relevance. The documents selected were those published between 2017 and 2021. Table 1 shows documents retrieved from each database, those discarded and those included.

Table 1. List of databases

Database	Number of documents retrieved	Discarded duplicates and/or older than 2017	Considered for inclusion
IEEE Explore	109	103	15
Springer	54	49	5
ACM digital library	64	57	7
Wiley online library	77	74	4
Taylor & Francis	62	58	4
EBSCO	21	19	2
arXiv	79	68	11
Snowballing			14
	466	428	62

3.3. Information Sources

Factors that affect open-source ERP software security were used as the search criteria in the Google search. The search term yielded tens of thousands of document since each document containing the term anywhere was retrieved. In all the databases the first few pages were searched and all the duplicate copies generated were discarded. If a document's digital object identifier (DOI) was equal to the DOI of another document, it was considered as a duplicate and discarded. The search covered all the documents published up to the year 2021. The search terms have been searched in the title, abstract and full article of the publication, whenever possible. Snowballing search was also carried out on some of the references in the selected papers and added to the list before refining the selection. Information retrieval process included confirming sufficiency of documents, searching each database using search terms, removing duplicates and snowballing as shown Figure 1.

3.4. Inclusion and Exclusion Criteria

Publications from the year 2017 to 2021 were included in the review with the relevance being determined by the presence of the search term anywhere in the document. Further, the retrieved documents were categorized as relevant or not relevant after reading the titles, abstract, introduction and finally the full article. Documents were included on the basis of their relevance. Excluded from the review were any unpublished work on factors that affect the open-source ERP software security, documents from other fields and all other documents published in other databases. Snowballing was also done where documents cited in the relevant publications were

retrieved and included. Snowballing refers to the vertical search where citations are used as a guide to gain more insight on a concept.

3.5. Data Extraction and Synthesis

Data was extracted using spreadsheets where each row contained articles published in each of the selected databases for the years 2017–2021. Relevant bibliographic information was captured (e.g. title, author, database, page numbers) including a hyperlink to the article for viewing. The title, keywords and the abstract formed the basis for inclusion of an article for the final review. The two-phase process was applied where the abstract was read first and the article coded as relevant or not relevant based on the search context. The second phase involved reading the full article and contextualizing it as containing the relevant information regarding attribute or factors that affect open-source ERP software security.

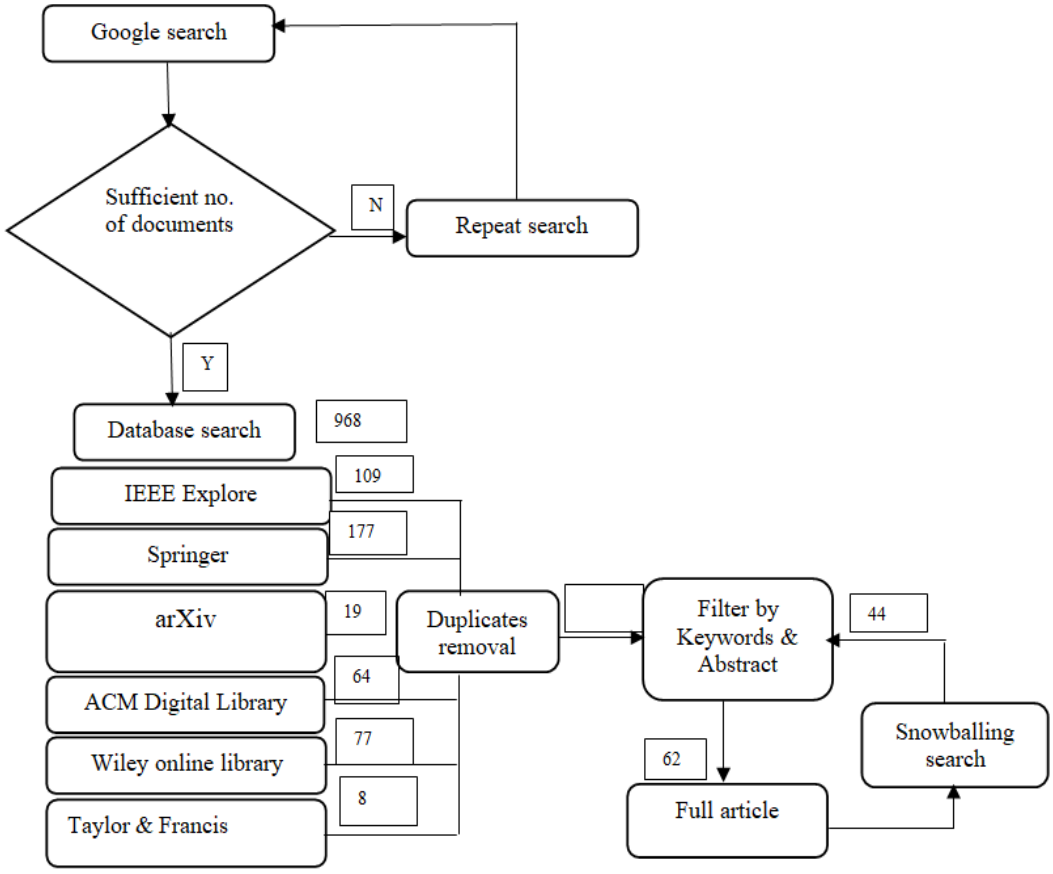

Figure 1. Documents retrieval process: Total documents retrieved is 968, No. for each database is as indicated, after filtering no. is indicated on the arrow, 62 is the no. reviewed.

4. RESULTS

This section presents a summary of the results.

4.1. RQ1: What Factors Indicate Security of an Open-Source ERP Software?

The main attributes of information security also known as information security principles are confidentiality, integrity and availability (CIA)[24]. These attributes are core in ISO/IEC 27001 standard while they are classified as non-functional software product quality attributes in ISO/IEC 25010. Nevertheless, they form the basis of our discussion due to the importance of data security and protection by global authorities [7][25]. This study investigated factors that indicate open-source ERP software security and the type of control measures that are instituted to ensure security.

Insufficient control of access rights had the highest number of documents standing at 33.9% as shown in Table 2. This indicated that the access control mechanisms instituted highly reduced security incidences. Delayed software updates and single authentication both tied at 17.7 %. Inadequate training and use of unauthorized software also tied at 11.3% while failure to comply was at 8.1%.

Table 2. Representation of the number of papers covering the identified attributed

Factor	No. of papers	Percent (%)
Delayed software updates	11	17.7
Insufficient control of access rights	21	33.9
Single authentication	11	17.7
Inadequate training	7	11.3
Use of unauthorized/unlicensed software	7	11.3
Failure to comply	5	8.1
	62	100

The results in Table 2 were further illustrated using the bar graph in Figure 2. As indicated insufficient control of access rights was identified as the highest factor that affected open-source ERP software security. Delayed software updates and single authentication were rated as second in affecting open-source ERP software security. Use of unauthorized software and inadequate user training were rated third while failure to comply was the least factor that affected open-source ERP software security.

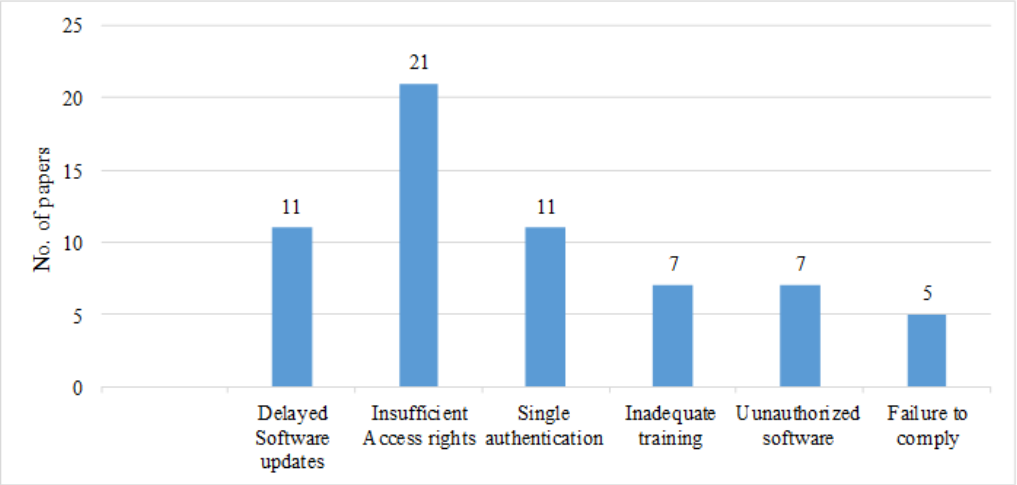

Figure 2. Number of papers discussing each of the identified attributes

4.2. RQ2: What Information Security Principles are Affected by Ineffective Controls on the Identified Factors?

Secure software is characterized by security of information in terms of confidentiality, integrity and availability. The identified factors were categorized based on the information security principle they affected as shown in Table 3. Further, the type of controls instituted to ensure security of the open-source ERP software were identified which included technical, logical and administrative. Confidentiality, integrity and availability were affected by delayed software updates and inadequate training. Insufficient control of access rights and single authentication affected confidentiality and integrity. Use of unauthorized software and failure to comply affected integrity and availability. Referred articles in relation to identified factors emphasized them as security indicators.

Table 3. Categorization of the effects identified factors based on CIA and controls that could be instituted (research data 2021)

	Type of control	Categorization			No. of papers	References
		C	I	A		
Delayed software updates	Technical/ Logical	√	√	√	11	[1][5][16][19][26][27] [61][62][63][64][65]
Insufficient control of access rights	Technical/ Logical	√	√		21	[4][10][12][20][21][28][29][30][31][32][33] [34][35][36][37][46] [50][52]55][60][66][67]
Single authentication	Technical/ Logical/ Administrative	√	√		11	[38][39][40][41][42][55] [68][69][70][71][43]
Inadequate training	Administrative	√	√	√	7	[3][44][45][46][47] [48][31][73]
Use of unauthorized /unlicensed software	Administrative		√	√	7	[49][50][51][52][53][54] [55]
Failure to comply	Administrative		√	√	5	[8][25][56][57][74]
					62	

4.3. RQ3: How Can the Identified Factors Act as Indicators of Open-Source ERP Software Security?

Effectiveness of instituted control measures on identified factors implied improved security of the open-source ERP software. Use of updated software, user training, sufficient control of access rights, proper authentication of users, use of authorized software and compliance with set standards were identified as indicators that reduced vulnerabilities as presented in Table 4.

Table 4. Categorization of factors, control measure and effect on confidentiality, integrity and availability

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/ unlicensed software	Administrative		√	√
Failure to comply	Administrative		√	√

5. DISCUSSION

5.1. Security Indicators

The results implied that delayed software updates, insufficient control of access rights and single authentication posed as the highest indicators of open-source ERP software insecurity while inadequate training, unauthorized software and failure to comply indicated minimal insecurity. Effectiveness of instituted controls indicates security posture of an organization which is of interest to decision makers and other stakeholders.

5.2. Effects on Security Principles

Confidentiality, integrity and availability would be affected by the determined factors of open-source ERP software security. Exploitation of any vulnerability presented by these factors leads to modification and fabrication of information which are confidentiality and integrity issues. Availability means access to information by the authorized users when needed and when attackers exploit these vulnerabilities confidentiality and integrity are also affected.

5.3. Sealing Security Loopholes

Effectiveness of administrative controls to address inadequate training, single authentication, unauthorized software and failure to comply would lead to secure open-source ERP software. Further, institution of logical and technical controls for mitigation of delayed software updates, insufficient access rights and single authentication would enhance open-source ERP software security.

6. CONCLUSIONS

During the review factors affecting open-source ERP software security were identified as delayed software updates, access rights, single authentication, inadequate training and failure to comply. These factors affected the principles of information security which are confidentiality, integrity and availability. Effectiveness of instituted administrative, logical and technical control measure indicate the security posture of an organization.

The security posture of an organization implementing open-source ERP software informs the amount of resources invested on security as well as building stakeholders' confidence. To establish the Security posture measurements and metrics are useful. The use of metrics would ensure business continuity. The future work includes design of security measurement framework and definition of a metrics suite for assessing open-source ERP software security.

REFERENCES

[1] S. M. Muegge and S. M. M. Murshed, "Time to discover and fix software vulnerabilities in open source software projects: Notes on measurement and data availability," PICMET 2018 - Portl. Int. Conf. Manag. Eng. Technol. Manag. Technol. Entrep. Engine Econ. Growth, Proc., 2018, doi: 10.23919/PICMET.2018.8481833.

[2] P. Mukherjee and C. Mazumdar, "'Security Concern' as a metric for enterprise business processes," IEEE Syst. J., vol. 13, no. 4, pp. 4015–4026, 2019, doi: 10.1109/JSYST.2019.2918116.

[3] T. Mladenova, "Open-source ERP systems: An overview," 2020 Int. Conf. Autom. Informatics, ICAI 2020 - Proc., 2020, doi: 10.1109/ICAI50593.2020.9311331.
[4] S. Tasnawijitwong and T. Samanchuen, "Open source ERP selection for small and medium enterprises by using analytic hierarchy process," Proc. 2018 5th Int. Conf. Bus. Ind. Res. Smart Technol. Next Gener. Information, Eng. Bus. Soc. Sci. ICBIR 2018, pp. 382–386, 2018, doi: 10.1109/ICBIR.2018.8391226.
[5] 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.
[6] R. G. Priest, Data Protection Act, vol. 12, no. 5. 2018, pp. 204–204.
[7] N. C. GoK, For, L. A. W. Reporting, and S. Issue, Data Protection Act, 2019, vol. 181, no. 181. Kenya, 2019, pp. 1–25.
[8] M. Alenezi and S. Almuairfi, "Essential Activities for Secure Software Development," Int. J. Softw. Eng. Appl., vol. 11, no. 2, pp. 1–14, 2020, doi: 10.5121/ijsea.2020.11201.
[9] A. A. Magableh and A. M. R. AlSobeh, "Securing Software Development Stages Using Aspect-Orientation Concepts," Int. J. Softw. Eng. Appl., vol. 9, no. 6, pp. 57–71, 2018, doi: 10.5121/ijsea.2018.9605.
[10] S.-T. Lai, "A Security Requirement Quality Measurement Model for Reducing E-Commerce Security Risk," Int. J. Softw. Eng. Appl., vol. 5, no. 1, pp. 31–42, 2014, doi: 10.5121/ijsea.2014.5103.
[11] A. T. Approach, "feature feature Enterprise Security Architecture —," vol. 4, pp. 1–8, 2017.
[12] M. P. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "A propose technical security metrics model for SCADA systems," Proc. 2012 Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensic, CyberSec 2012, pp. 70–75, 2012, doi: 10.1109/CyberSec.2012.6246089.
[13] L. Zhanna Malekos, Smith; Eugenia and J. A. Lewis, "The Hidden Costs of Cybercrime," McAfee. pp. 1–38, 2020.
[14] A. Adewumi, S. Misra, and N. Omoregbe, "Evaluating open source software quality models against ISO 25010," Proc. - 15th IEEE Int. Conf. Comput. Inf. Technol. CIT 2015, 14th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC 2015, 13th IEEE Int. Conf. Dependable, Auton. Se, pp. 872–877, 2015, doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.130.
[15] H. Panduwiyasa, M. Saputra, Z. F. Azzahra, and A. R. Aniko, "Accounting and Smart System: Functional Evaluation of ISO/IEC 25010:2011 Quality Model (a Case Study)," IOP Conf. Ser. Mater. Sci. Eng., vol. 1092, no. 1, p. 012065, 2021, doi: 10.1088/1757-899x/1092/1/012065.
[16] S. Birla and M. Johansson, "Quality Requirements for Software-dependent Safety-critical Systems History, current status, and future needs," Proc. 38th Meet. Ser. Enlarg. Halden Program. Gr. Meet., no. 1, 2014.
[17] "Cost of Data breach 2021 report," IBM.
[18] M. Alenezi and M. Zarour, "On the Relationship between Software Complexity and Security," Int. J. Softw. Eng. Appl., vol. 11, no. 1, pp. 51–60, 2020, doi: 10.5121/ijsea.2020.11104.
[19] S. Parthasarathy and S. Sharma, "Impact of customization over software quality in ERP projects: an empirical study," Softw. Qual. J., vol. 25, no. 2, pp. 581–598, 2017, doi: 10.1007/s11219-016-9314-x.
[20] M. Korolov, "Open source software security challenges persist," Cso, no. December, 2018.
[21] P. Zhezhnych and D. Tarasov, "Methods of data processing restriction in ERP systems," 2018 IEEE 13th Int. Sci. Tech. Conf. Comput. Sci. Inf. Technol. CSIT 2018 - Proc., vol. 1, pp. 274–277, 2018, doi: 10.1109/STC-CSIT.2018.8526734.
[22] M. Lubis, D. Novalia, and Puspita, "Development of security awareness domain and resources (SADAR) Framework: Capacity metrics to evaluate enterprise resource planning (ERP) Implementation," 2020 4th Int. Conf. Electr. Telecommun. Comput. Eng. ELTICOM 2020 - Proc., pp. 170–175, 2020, doi: 10.1109/ELTICOM50775.2020.9230523.
[23] T. C. Pfutzenreuter and E. P. De Lima, "ERP Integration with Performance Analytics: A Systematic Literature Review," 2020.
[24] 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.
[25] V. Lenarduzzi, D. Taibi, D. Tosi, L. Lavazza, and S. Morasca, "Open Source Software Evaluation, Selection, and Adoption: A Systematic Literature Review," Proc. - 46th Euromicro Conf. Softw. Eng. Adv. Appl. SEAA 2020, pp. 437–444, 2020, doi: 10.1109/SEAA51224.2020.00076.
[26] S. E. Group, "Guidelines for performing Systematic Literature Reviews in Software Engineering," 2007.

[27] B. Kitchenham and C. Ebse, "Guidelines for performing Systematic Literature Reviews in Software Engineering Executive summary," 2007.
[28] M. McClintock, K. Falkner, C. Szabo, and Y. Yarom, "Enterprise security architecture: Mythology or methodology?" ICEIS 2020 - Proc. 22nd Int. Conf. Enterp. Inf. Syst., vol. 2, no. Iceis, pp. 679–689, 2020, doi: 10.5220/0009404406790689.
[29] I. (Information C. Office), "Guide to the General Data Protection Regulation (GDPR)," Guid. to Gen. Data Prot. Regul., no. May, p. n/a, 2019.
[30] R. Arora, S. Gera, and M. Saxena, "Mitigating security risks on privacy of sensitive data used in cloud-based ERP applications," Proc. 2021 8th Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2021, pp. 458–463, 2021, doi: 10.1109/INDIACom51348.2021.00081.
[31] P. Mell and M. C. Tracy, "Procedures for Handling Security Patches Recommendations of the National Institute of Standards and Technology."
[32] M. Khadir and M. Belaissaoui, "The End-User Continuance Intention with an Open Source ERP: A Proposal for an Integrated Model," Int. J. Comput. Sci. Mob. Comput., vol. 6, no. 6, pp. 448–456, 2017.
[33] D. Stefanović, D. Nikolić, D. Dakić, I. Spasojević, and S. Ristić, "Static code analysis tools: A systematic literature review," Ann. DAAAM Proc. Int. DAAAM Symp., vol. 31, no. 1, pp. 565–573, 2020, doi: 10.2507/31st.daaam.proceedings.078.
[34] S. F. Wen, M. Kianpour, and S. Kowalski, "An empirical study of security culture in open source software communities," Proc. 2019 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Mining, ASONAM 2019, pp. 863–870, 2019, doi: 10.1145/3341161.3343520.
[35] S. AlMuhayfith and H. Shaiti, "The impact of enterprise resource planning on business performance: With the discussion on its relationship with open innovation," J. Open Innov. Technol. Mark. Complex., vol. 6, no. 3, 2020, doi: 10.3390/JOITMC6030087.
[36] J. D. Lenaeus et al., "How to Implement Security Controls for an Information Security Program at CBRN Facilities," Centers Excell., 2015.
[37] P. Samarati and S. De Capitani, "Access Control: Policies, Models, and," pp. 137–196, 2001.
[38] H. F. Atlam, M. A. Azad, M. O. Alassafi, A. A. Alshdadi, and A. Alenezi, "Risk-based access control model: A systematic literature review," Futur. Internet, vol. 12, no. 6, pp. 1–23, 2020, doi: 10.3390/fi12060103.
[39] C. E. Da Silva, J. D. S. Da Silva, C. Paterson, and R. Calinescu, "Self-Adaptive Role-Based Access Control for Business Processes," Proc. - 2017 IEEE/ACM 12th Int. Symp. Softw. Eng. Adapt. Self-Managing Syst. SEAMS 2017, pp. 193–203, 2017, doi: 10.1109/SEAMS.2017.13.
[40] M. Satterlee and J. Gibbons, "Enterprise Networks," Build. Netw. Futur., pp. 201–222, 2021, doi: 10.1201/9781315208787-10.
[41] G. Keifer and F. Effenberger, Access Control Systems: Security, Identity Management and Trust Models, vol. 6, no. 11. 1967.
[42] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security fctors for decision-makers," vol. 92, 2020, doi: 10.1016/j.cose.2020.101747.
[43] R. Matulevi, Fundamentals of Secure System Modelling. Springer International Publishing, 2017.
[44] NIST, "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP-800-53 Ar4, p. 400+, 2013, doi: 10.6028/NIST.SP.800-53Ar4.
[45] NIST SP800-53, "Security and privacy controls for federal information systems and organizations," NIST Spec. Publ., vol. 800, no. September, 2020, p. 53, 2013.
[46] C. T. Jérémy Briffaut, Jean-François Lalande, "Formalization of Security Properties: Enforcement for MAC Operating Systems and Verification of Dynamic MAC Policies," Int. J. Adv. Secur., vol. 2, no. 4, p. 325, 2009.
[47] N. Eya and G. R. S. Weir, "End-User Authentication Control in Cloud-based ERP Systems," Proc. - 2021 IEEE 4th Natl. Comput. Coll. Conf. NCCC 2021, 2021, doi: 10.1109/NCCC49330.2021.9428846.
[48] E. Jonsson, "An Integrated Framework for Security and Dependability," ACM Digit. Libr., 2015.
[49] 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.
[50] V. C. V. Hu, D. F. Ferraiolo, and D. R. Kuhn, "Assessment of access control systems," Nistir 7316, p. 60, 2006.

[51] A. Almehmadi and K. El-Khatib, "On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC)," IEEE Syst. J., vol. 11, no. 2, pp. 373–384, 2017, doi: 10.1109/JSYST.2015.2424677.
[52] V. C. Hu and K. Scarfone, "Guidelines for Access Control System Evaluation Metrics," Natl. Inst. Stand. Technol., pp. 1–32, 2012.
[53] D. T. Bourgeois and J. L. Smith, "Information Systems for Business and Beyond Information Systems for Business and Beyond (2019)," 2019.
[54] S. Program and B. Executives, "Using Security Metrics to Drive Action."
[55] 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.
[56] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?" 2016 IEEE 35th Int. Perform. Comput. Commun. Conf. IPCCC 2016, 2017, doi: 10.1109/PCCC.2016.7820663.
[57] P. Morrison, D. Moye, R. Pandita, and L. Williams, "Mapping the field of software life cycle security metrics," Inf. Softw. Technol., vol. 102, no. May, pp. 146–159, 2018, doi: 10.1016/j.infsof.2018.05.011.
[58] W. C. Barker, W. C. Barker, and W. Fisher, "Cybersecurity Framework Profile for Ransomware Risk Management Preliminary Draft NISTIR 8374 Cybersecurity Framework Profile for Ransomware Risk Management."
[59] N. Dissanayake, A. Jayatilaka, M. Zahedi, and M. Ali Babar, "Software security patch management - A systematic literature review of challenges, approaches, tools and practices," arXiv, 2020.
[60] V. Dehalwar, A. Kalam, M. L. Kolhe, and A. Zayegh, "Review of web-based information security threats in smart grid," 2017 7th Int. Conf. Power Syst. ICPS 2017, pp. 849–853, 2018, doi: 10.1109/ICPES.2017.8387407.
[61] E. Takamura, K. Mangum, F. Wasiak, and C. Gomez-rosa, "Information Security Considerations for Protecting NASA Mission Operations Centers (MOCs)," 2015 IEEE Aerosp. Conf., pp. 1–14, doi: 10.1109/AERO.2015.7119207.
[62] L. Revised, "CIS Controls Assessment Specification Table of Contents," 2021.
[63] K. M. Goertzel, T. Winograd, H. L. McKinley, and P. (Booz A. H. Holley, "Security in the Software Lifecycle: Making Software Development Processes —and the Software Produced by Them—More Secure, Draft Version 1.2 (August 2006), U.S. Department of Homeland Security," no. August, 2006.
[64] S. Bellovin, "Introduction to Software Security ". . .," pp. 1–28.
[65] "Open Source for Global Public Goods," Open Source Glob. Public Goods, 2019, doi: 10.1596/33401.
[66] A. Mathur, J. Engel, S. Sobti, V. Chang, and M. Chetty, "'They keep coming back like zombies': Improving software updating interfaces," SOUPS 2016 - 12th Symp. Usable Priv. Secur., no. Soups, pp. 43–58, 2019.
[67] K. Vaniea and Y. Rashidi, "Edinburgh Research Explorer Tales of Software Updates: The process of updating software Tales of Software Updates: The process of updating software," Proc. Comput. Hum. Interact. 2016, p. 13, 2016.
[68] E. M. Redmiles et al., "A comprehensive quality evaluation of security and privacy advice on the web," Proc. 29th USENIX Secur. Symp., pp. 89–108, 2020.
[69] T. Takahashi, "Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information," no. October 2017, pp. 1–21, 2018, doi: 10.1002/dac.3470.
[70] W. Paper, "The Importance of Vulnerability Assessment and Patch Management with 𝔞 Cyber Protect Identify and close," pp. 1–6.
[71] M. Sirshar, A. Ali, and S. Ibrahim, "A Comparitive Analysis Between Open Source and Closed Source Software in Terms of Complexity and Quality Factors," no. December, 2019, doi: 10.20944/preprints201912. 0063.v1.
[72] J. M. Borky and T. H. Bradley, Effective Model-Based Systems Engineering. 2019.
[73] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, "Trust-based recommendation systems in Internet of Things: a systematic literature review," Human-centric Comput. Inf. Sci., vol. 9, no. 1, 2019, doi: 10.1186/s13673-019-0183-8.
[74] T. Khodadadi, A. K. M. M. Islam, S. Baharun, and S. Komaki, "Evaluation of recognition-based graphical password schemes in terms of usability and security attributes," Int. J. Electr. Comput. Eng., vol. 6, no. 6, pp. 2939–2948, 2016, doi: 10.11591/ijece. v6i6.11227.
[75] K. Ramezani, E. Sithirasenan, and K. Su, "Formal Security Analysis of EAP-ERP Using Casper," IEEE Access, vol. 4, pp. 383–396, 2016, doi: 10.1109/ACCESS.2016.2517179.

[76] NIST Cybersecurity Framework Team, "Framework for improving critical infrastructure cybersecurity," Proc. Annu. ISA Anal. Div. Symp., vol. 535, pp. 9–25, 2018.
[77] ISO/IEC, International Stanard ISO/IEC 27002: 2013.pdf, vol. 2013. 2013, p. 90.
[78] I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," J. Comput. Inf. Syst., vol. 0, no. 00, pp. 1–12, 2019, doi: 10.1080/08874417.2019.1650676.