International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6s, 2025
https://www.theaspd.com/ijes.php

Designing A Framework For Evaluating Information Security Policies For Banking Institutions

Mahmoud I. Alfeel[1], Abdalilah Alhalangy[2], Adil.O.Y. Mohamed[3], Omran Mahmoud Abdalaa[4]
[1] Department Deanship of Educational service, Qassim University, Saudi Arabia, alfeeeeel@gmail.com
[2] Department of Computer Engineering, College of Computer, Qassim University, Saudi Arabia a.alhalangy@qu.edu.sa , 0000-0003-2735-8208
[3]Department of Computer Science, College of Computer, Qassim University, Saudi Arabia, adi.mohamed@qu.edu.sa
[4]Department of Economics, College of Business & Economics, Qassim University, Saudi Arabia, O.mahmoud@qu.edu.sa

Abstract This paper aims to design and apply a framework for evaluating the confidentiality and privacy policy in information security policies. It is a descriptive analytical study applied to a sample of banking institutions (Bank of Sudan, Omdurman National Bank, Bank of Khartoum). The research problem is represented by the lack of continuous evaluation and development of confidentiality and privacy requirements in the country's financial institutions. The researchers also wanted to test and evaluate policies related to confidentiality and privacy in information security and analyze some of the policies used in some banking institutions in order to identify their strengths and weaknesses with the aim of arriving at results and recommendations by the researchers that contribute to protecting and securing the information network and data for those dealing with the institutions at various levels. This proposed framework was designed in accordance with ISO standards, as it has the ability to address the basic confidentiality and privacy requirements for ensuring information security. The proposed framework was tested by designing a program to evaluate the confidentiality and privacy policies followed in these banking institutions. By analyzing the results of testing the proposed framework, it was found that the highest percentage of confidentiality and privacy requirements was at the Bank of Sudan, which was 71.2%.
Keywords: Evaluation framework, Security policies, Confidentiality, Privacy.

INTRODUCTION

Security policies, especially confidentiality and privacy policies, must keep pace with the continuous change occurring in information systems by introducing new and advanced security systems that keep pace with the development of hacking methods and hackers (3).

The information security policy document should also be reviewed at specific intervals or when significant changes occur in the organization to ensure that the document is appropriate and effective. In general, there is no specific timeframe for reviewing and evaluating security policies; the period may vary, depending on the security policy, from every six months to every year (5).

There may be a working group to review security policies. It is necessary to have frameworks for evaluating security policies for confidentiality and privacy due to the rapid development of information technology and means of hacking and protection (6).

There is a need for an assessment framework for security requirements in both confidentiality and privacy and the assessment framework not only needs to perform this task with high

precision but also needs to do so on a continuous basis because this reduces the impact of the risk of attack (1).

Below, we propose an integrated framework for ensuring the assessment of confidentiality and privacy requirements in each security policy. This framework is based on the assessment of both confidentiality and privacy. Furthermore, the assessment of these policies is important for achieving the assessment of information system security requirements through a framework consisting of sequences (11).

RELATED WORKS

The foundations of the information security strategy and the variables influencing its integration are examined in this study. With the aim of creating a roadmap for the effective creation and execution of Greece's National Cybersecurity Strategy and identifying the national factors that may be in line with a nation's cybersecurity level, this paper makes a contribution by offering a model based on the ITU cybersecurity decisions (12).

1. This study offers a thorough narrative overview of cybersecurity frameworks and standards, their applicability across a range of domains, and their current cybersecurity assets. This assists you in deciding which cybersecurity framework or standard best suits your needs. The latter aids in examining the experiences of businesses operating in this industry as well as those that depend on the most up-to-date cybersecurity guidelines and standards (13).
2. A cybersecurity culture framework for evaluating an organization's workforce's current security readiness is presented in this study. Following a thorough analysis of the most widely used security frameworks, this study created a domain-independent security model in order to identify and classify the key components associated with human security. After that, it described each model element in depth and made an effort to quantify it in order to develop a useful assessment process. The creation and development of a security culture assessment tool, which provides suggestions and alternate methods for workforce training programs and procedures, was then illustrated using this methodology (14).
3. This study investigated behavior associated with adherence to information security standards in Yemen's banking industry. A PLS-SEM model was used to analyses data gathered from 210 Yemeni banking personnel. This study showed that employees' deliberate behavior in adhering to information security standards is strongly influenced by perceived self-efficacy, reaction effectiveness, and response intensity. The theoretical and practical ramifications for improving information security compliance behavior are also included in the study (15).
4. The purpose of this study is to provide a definition of practical guidance. A precise definition can help with the creation of information security rules, enhance employee communication, and direct staff on the proper conduct to safeguard an organization's information assets. This effort is guided by the following research question: How can information security policies define actionable advice? The definition is based on an examination of 47 Swedish public-sector ISPs and a survey of the literature in order to accomplish this purpose (16).

6- This study looks at a substantial and expanding corpus of research on the coercive, persuasive, and deterrent factors that influence compliant and non-compliant behavior.

ISP compliance and non-compliance, according to this research viewpoint, cannot be uniformly and consistently characterized as "right" or "wrong," and only when assessed in relation to organizational results do they acquire significance. In order to establish our arguments and provide a rule-related information security behavior (RISB) framework for conceptualizing different forms of complying and non-compliant ISP behavior and its organizational consequences, we rely on organizational incident theorists (17).

Description of the proposed framework

A framework for evaluating security policies has been proposed. The evaluation framework is divided into a series of steps. The policies in this framework are based on ISO and NIST information security standards. These standards provide a structured approach to defining a wide range of information security activities (8).

Each series in this framework can result from evaluating a number of insurance policies with high accuracy because it includes all the features necessary for evaluating those policies, and at the same time requires a minimum of effort because the evaluation of policies is distributed among a number of series, as shown in Figure (1) below.

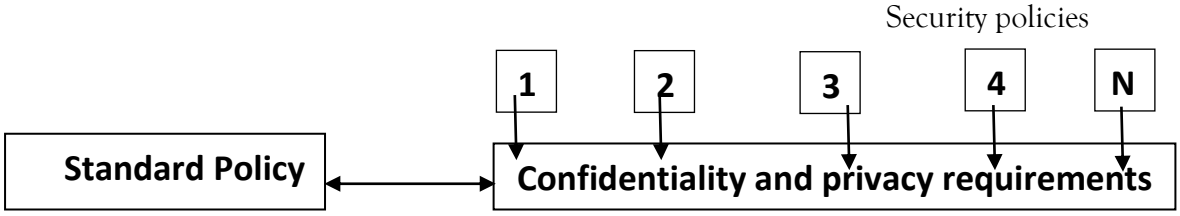

Figure (1) Policy Evaluation Framework

The security policy evaluation process is done by comparing the bank's policy to be evaluated with the standard policy. A point is given for each policy requirement that exists in the bank and is present in the standard policy. Each policy requirement is given one point because all requirements are equally important to achieve in the bank. Then, the points obtained in this policy are collected and divided by the total standard requirements and the result is multiplied by a percentage, which is as follows:

((Total points of the bank's existing security policy requirements) / (Total points of the standard policy requirements) %.

Frame Features

A number of different security policies and rules were evaluated for a group of Sudanese banks, such as the Bank of Khartoum, the National Bank of Omdurman, and the Central Bank of Sudan, which are considered among the largest and most important Sudanese banks in the field of banking technology in Sudan.

This proposed framework is considered suitable for evaluating insurance requirements in all financial institutions. The proposed framework is distinguished by the fact that its main reference is NIST and ISO standards (4).

Evaluation and comparison:

The evaluation process must first ensure the following characteristics:

1. Classify each element of the policy to be evaluated.

2. Both the elements of the evaluation system and the policy to be evaluated must contain the same information for the elements to which they are assigned.
3. Compare all policies to be evaluated with the elements of the evaluation system and vice versa.
4. Ensure that the elements of both the existing policy and the elements of the evaluation system (9).
belong to the same classification and carry the same meaning.
Comparing the bank's policy to be evaluated with the elements of the reference evaluation system policies is important to determine the extent to which the bank's policy is suitable for insurance aspects. This comparison enables us to perform two tasks (10).
1. Assessing the compatibility of the bank's existing insurance policy with the elements of the rating system.
2. Improving consistency between existing policies, with the possibility of adding any additional policies.
The evaluation process is straightforward, by taking any insurance rule found in the bank's policy and comparing it with the reference policy. Through this comparison, we can decide to add a rule to the bank's policies.
When matching the two policies, all policies and all elements of the bank's security rules must be analyzed, and then a determination is made as to whether there is a match or not. At the end of the evaluation steps, the result we obtain is analyzed to determine which rules should be added to the bank's policy, as follows:
Step 1: We take the policy elements and compare them with the reference policy. We then mark each policy in the bank. The marked elements are part of the reference policy elements and are also part of the bank's existing policy.
Step 2: The policy table with the marked elements is analyzed with the existing policy elements. There are two possibilities:
1- When a policy is included in the reference policy elements and is present in the bank's policy, it remains as it is.
2- When it is included in the reference policy elements and is not present in the bank's policy, it is added to the bank's policy.

Components Of the Proposed Framework Program:
The program consists of several functions and procedures used throughout the program application. Microsoft SQL Server was used to create databases in the program. The program was tested in a Windows operating system environment.
The program consists of several screens. The main screen consists of five buttons:
First, the main menu button. By clicking on it, the first sub-screen appears, which is the screen for entering the name of the bank whose policies are to be evaluated. The program allows the names of the banks entered to be saved through the database used in the program. By clicking on the save button, the name is saved in the database.
The second button is the exit button.
The third button is the (Confidentiality Requirements) button. By clicking on it, a list appears containing a number of confidentiality requirements procedures and policies. When it is selected, a screen appears containing a list through which the name of the bank whose policy is to be evaluated can be selected, which has been entered and saved in the program's database.

Then, the bank's policy evaluation process can be carried out, comparing it with the elements of the reference evaluation system policies.
By clicking on the Display Report button, a screen is displayed showing the percentage of the bank's policy evaluation, with the appropriate rating given for this evaluation. If the evaluation percentage is greater than (85%), an excellent rating is given, but if the percentage is greater than (75%), the system gives a very good rating. The system displays a good rating if the percentage is greater than (65%), and the rating is acceptable if the percentage is greater than (50%), but if the percentage is less than (50%), the system gives a weak rating.
The program also shows, during evaluation, the procedures that are missing and that the bank must implement in all requirements. There is a restore button through which the evaluation of all the banks' policies that were evaluated can be retrieved, which is what the program can do by saving all the evaluation procedures for all the banks that were evaluated through the program's database.
This program was implemented by evaluating a number of bank policies (Central Bank of Sudan, Omdurman National Bank, Bank of Khartoum).
This program was distinguished:
1. In terms of flexibility, this system can evaluate a number of different types of policies, including confidentiality and privacy requirements.
2. Ensuring that the evaluation of any bank's policies that have been evaluated can be retrieved using the program's Microsoft SQL Server database.
3. The program's .NET design allows for interaction with other software via the Internet and email. It also greatly facilitates network users at various bank branches due to its ease of implementation, simple procedures, and low cost.
4. The program's simple design facilitates understanding and interaction.
5. The program can be implemented on any type of computer, both mobile and stationary.
6. The program's simplicity and clarity facilitate the training of employees on how to use it (5).

General Picture Diagram of The Evaluation Process System
Where all parties involved in the evaluation process are shown, the system requests the security policy to be evaluated and then checks the existence of the policy in the database within the system. The evaluation system compares the bank's policy with the existing reference policy and completes the evaluation process. Finally, the system returns the bank's policy evaluated. This is as shown in Figure (2):

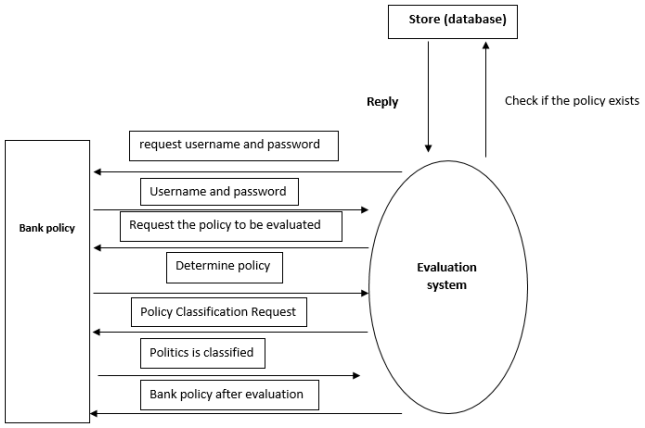

Figure 2: General diagram of the evaluation process system

A chart outlining the missing procedures to be added to the bank's policies.

This sub-scheme describes the stages in which the process of evaluating bank policies takes place, and identifying the procedures that do not exist to be added to the bank policies, with the possibility of retrieving all the policies that have been evaluated in all banking institutions through the database within the system. It is as shown in (3).

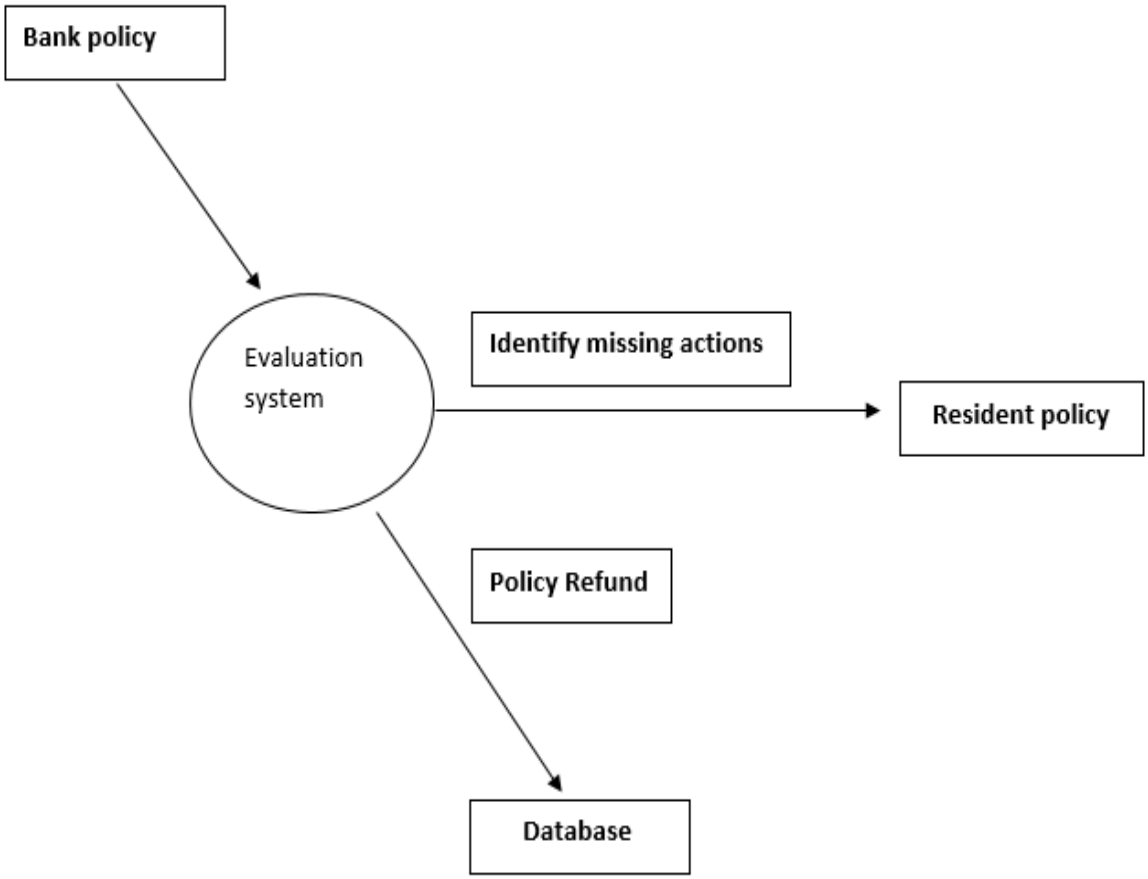

Figure 3: Identifying the missing procedures to add them to the bank's policies

Proposed framework action plan:

This diagram illustrates the stages of the evaluation process, including the classification and identification of the policy to be evaluated. The system conducts the evaluation process by comparing the bank's policy with the reference evaluation system's policy and ensuring that the policy is included within the bank's policies (7). There are two options: the first: If the policy is included within the bank's policies, it remains as it is. The second option: If the policy is not included within the bank's policies, it must be added to the bank's policies. This is illustrated in Figure (4).

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6s, 2025
https://www.theaspd.com/ijes.php

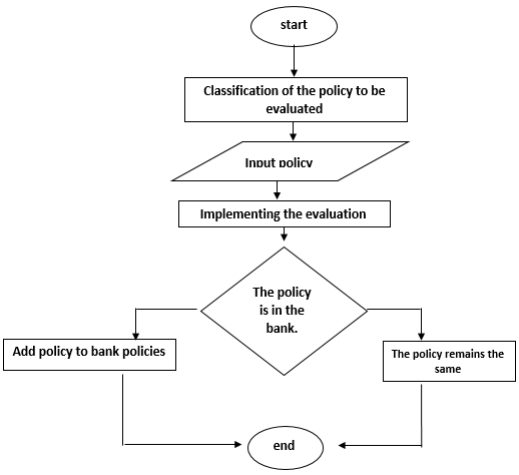

Figure 4: Evaluation process diagram with the proposed framework

Analysis Results

To test the proposed framework, a sample of banks was selected, namely Omdurman National Bank, Bank of Sudan, and Bank of Khartoum. By analyzing the results of the assessment of the insurance requirements of these banks, the results were reached, which will be discussed in the following sections.

Analysis of the results of the confidentiality and privacy policies of the National Bank of Omdurman:

It included an evaluation of a number of confidentiality procedures, and the confidentiality requirements of the National Bank of Omdurman were good at 65%.

Table 1: Confidentiality and privacy policies requirements percentage at the National Bank of Omdurman

% the percentage	Requirement name
65	Confidentiality and Privacy

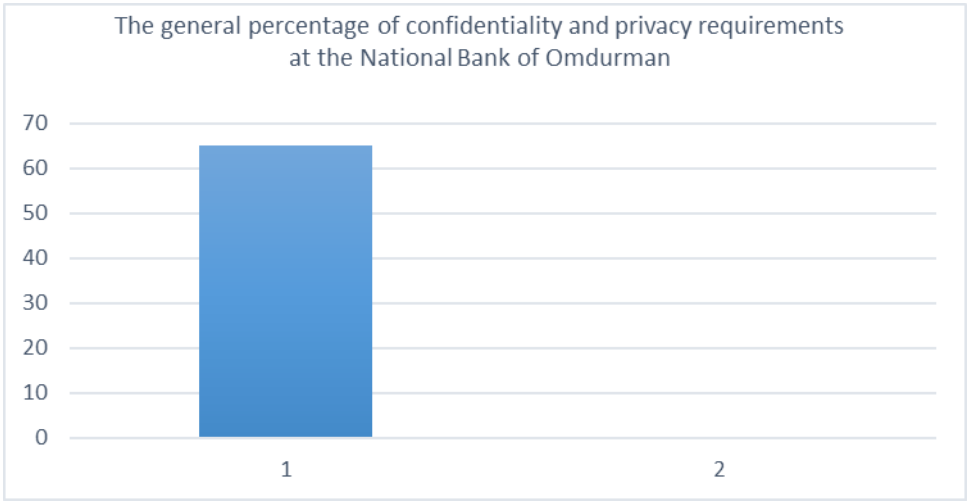

Figure 5: Confidentiality and privacy policies requirements percentage at the National Bank of Omdurman

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6s, 2025
https://www.theaspd.com/ijes.php

Analysis of the results of the confidentiality and privacy policies of the Central Bank of Sudan:
Regarding the bank's confidentiality requirements, a number of insurance rules were evaluated and, in general, the confidentiality requirements of the Central Bank of Sudan are considered good at 68.7%.

Table 2: Confidentiality and privacy policies requirements percentage at the Bank of Sudan

The Percentage%	Requirement Name
68.7	Confidentiality and Privacy

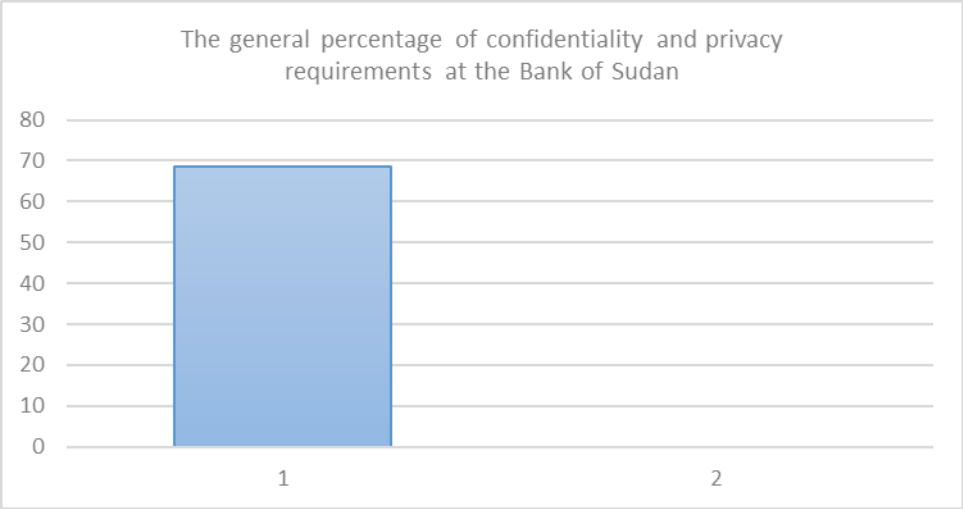

Figure 6: Confidentiality and privacy policies requirements ratios at the Bank of Sudan

Analysis of the results of the confidentiality and privacy policies of the Bank of Khartoum:
Regarding confidentiality requirements, a number of insurance rules that meet confidentiality requirements were evaluated, and confidentiality requirements at the Bank of Khartoum were considered good at a rate of 71.2%. Table (4-3) and Figure (4-3) show details of the confidentiality requirements.

Table 3: Confidentiality and privacy policies requirements ratios at the Bank of Khartoum:

the percentage%	Requirement name
71.2	Confidentiality and Privacy

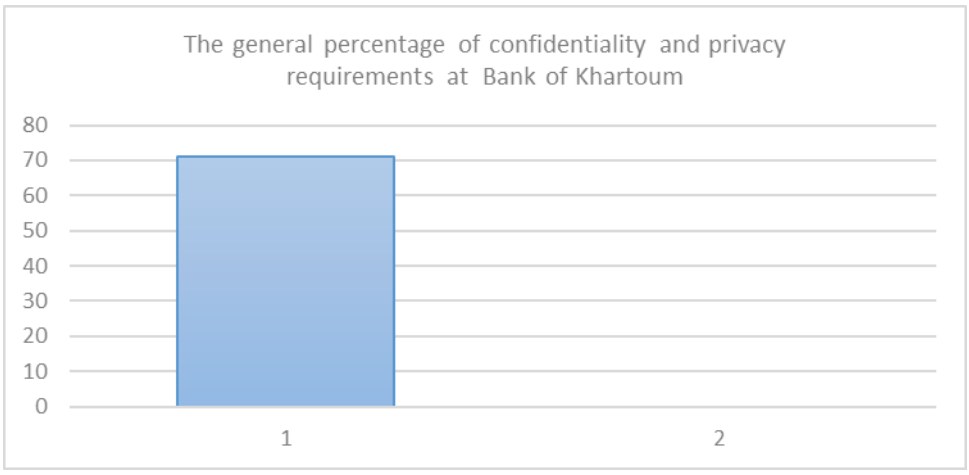

Figure 7: Confidentiality and privacy policies requirements ratios at the Bank of Khartoum:

General ratios for all banks

In general, by comparing and analyzing the evaluation of all insurance requirements (confidentiality and privacy) for all banks (Bank of Sudan, Omdurman National Bank, and Bank of Khartoum), it was concluded that the general percentage of confidentiality requirements for Omdurman National Bank was 65%. As for Bank of Sudan, its percentage was 68.7%. The highest percentage of confidentiality requirements was at Bank of Khartoum, which reached 71.1%. Table (5-1) and Figure (5-1) show the general details of the insurance requirements.

Table 4: General percentages of confidentiality and privacy requirements

Bank Name	Bank of Sudan	Omdurman National Bank	Bank of Khartoum
General percentage	68.7	65	71.2

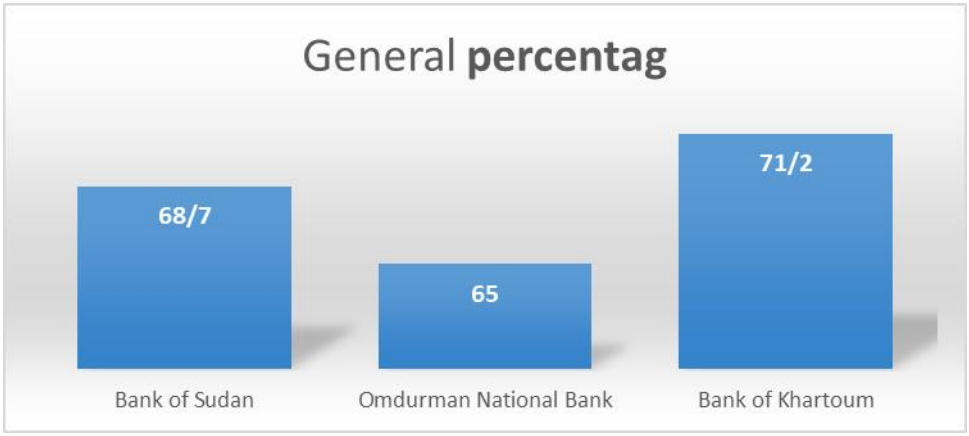

Figure 8: General proportions of confidentiality and privacy requirements

CONCLUSION

The primary purpose of information security research, strategies and methods, both technically and performance-wise, is to ensure the availability of the basic requirements for adequate protection, namely (confidentiality and privacy).

This framework addresses the basic requirements of security (confidentiality and privacy) by evaluating these requirements using sequences, each of which evaluates a number of security policies. The evaluation framework is divided into several sequences. Each sequence can be used to evaluate multiple security policies with high accuracy, as it includes all the features necessary for evaluating those policies.

This framework can evaluate a number of security rules such as physical security, acceptance of use, procedures for the compatibility of this policy with the facility's policies, the policy for checking and following up on the implementation of the security policy and monitoring of employees, the policy for verifying the user's identity, security procedures, and software development. , and a security policy for all types of networks, such as the Internet, internal and external networks, open and closed networks, and policies for securing connections to the Internet, email, and data encryption. This framework also included an assessment of how to deal with customer privacy through a number of different procedures, such as full commitment to maintaining the security and integrity of customer information.

This framework was tested to evaluate a number of different security policies for several banks, including the Central Bank of Sudan, Bank of Khartoum, and Omdurman National Bank, using a program that reflects the image of the proposed framework. New conclusions, recommendations, and results were derived that enrich the subject of this paper. In general, through analyzing the results of the evaluation of the security policies of these banks, the highest percentage of confidentiality and privacy requirements, 71.2%, was found at Bank of Khartoum.

RECOMMENDATIONS

Through the discussion and analysis that the researcher has presented, he recommends the following:

1- Conducting continuous evaluations of all security policies related to confidentiality and privacy in financial banks by applying this proposed framework to evaluate the various security policies in all local banks, as this framework can address the basic requirements of insurance.

2- Developing and unifying security standards and their regulatory and auditing requirements with the aim of achieving the national transformer for linking the various Sudanese banks.

3- Implementing and implementing a security policy saves significant effort and money in securing the bank's systems, networks, and electronic channels. It helps banks provide secure and distinctive banking services that help attract more customers, attract more investments, and provide more banking services.

4- Developing a comprehensive security policy based on international standards for banks and financial institutions, particularly those related to electronic money and banking and financial services technologies, most notably financial cards, electronic transfer systems, and banking and financial operations.

5- Providing a culture of dealing with the digital environment and awareness of information security issues among users and customers of banks and financial institutions in relation to managing their personal data.

REFERENCES

1. Olutimehin, A.T., 2025. Assessing the effectiveness of cybersecurity frameworks in mitigating cyberattacks in the banking sector and its applicability to decentralized finance (DeFi). *Available at SSRN 5133050*
2. Akash, T.R., Reza, J. and Alam, M.A., 2024. Evaluating financial risk management in corporation financial security systems. *World Journal of Advanced Research and Reviews*, *23*(1), pp.2203-2213.
3. Edunjobi, T.E. and Odejide, O.A., 2024. Theoretical frameworks in AI for credit risk assessment: Towards banking efficiency and accuracy. *International Journal of Scientific Research Updates*, *7*(01), pp.092-102.
4. Adejumo, A. and Ogburie, C., 2025. The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*.
5. Ejiofor, O.E., 2023. A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. *European Journal of Computer Science and Information Technology*, *11*(6), pp.62-83.
6. Kayode-Ajala, O., 2023. Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), pp.1-21.
7. Oyewole, A.T., Okoye, C.C., Ofodile, O.C. and Ugochukwu, C.E., 2024. Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), pp.625-643.
8. Ilori, O., Nwosu, N.T. and Naiho, H.N.N., 2024. Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, *22*(3), pp.213-224.
9. Melaku, H.M., 2023. A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), pp.327-350.
10. Li, H.J., Si, D.K. and Chen, M.L., 2024. How does macroprudential policy affect the relationship between financial openness and bank risk-taking. *Economic Analysis and Policy*, *84*, pp.1820-1839.
11. Huang, S.Y., Wang, T., Huang, Y.T. and Yeh, T.N., 2024. Information security risk items and management practices for mobile payment using non-financial-institution service providers: An exploratory study. *International Journal of Accounting Information Systems*, *53*, p.100684.
12. Kamariotou, M. and Kitsios, F., 2023. Information systems strategy and security policy: A conceptual framework. *Electronics*, *12*(2), p.382.
13. Taherdoost, H., 2022. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. Electronics, 11(14), p.2181.
14. Georgiadou, A., Mouzakitis, S., Bounas, K. and Askounis, D., 2022. A cyber-security culture framework for assessing organization readiness. Journal of Computer Information Systems, *62*(3), pp.452-462.
15. Alrawhani, E.M., Romli, A. and Al-Sharafi, M.A., 2025. Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, *11*(1), p.100463.

16. Rostami, E., Hanif, M., Karlsson, F. and Gao, S., 2025. Defining Actionable Advice in Information Security Policies-Guiding Employees to Strengthen Digital Sovereignty of Organizations. *Procedia Computer Science*, *254*, pp.30-38.
17. Niemimaa, M., 2024. Incorrect compliance and correct noncompliance with information security policies: A framework of rule-related information security behaviour. *Computers & Security*, *145*, p.103986.