Investigating information security risk management in Yemeni banks: An CILOS-TOPSIS approach

Abdulmajed Ahmed Ghaleb Al-Khulaidi\textsuperscript{a} | Adel Abdulsalam Nasser\textsuperscript{b,c} | Mohammed Hussein Yahya Al-ashwal\textsuperscript{d} | Mujib Mohammed Yahya Al-Ashwal\textsuperscript{b,e} | Alrasheed Mohammed Al Tayeb\textsuperscript{f}

\textsuperscript{a}Department of Computer Science, Faculty of Computer and Information technology, Sana'a University, Sana'a, Yemen. \textsuperscript{b}Department of Information Systems and Computer Science, Sa'adah University, Sa'adah, Yemen. \textsuperscript{c}Department of Artificial Intelligence, Modern Specialized University, Sana'a, Yemen. \textsuperscript{d}Department of Cyber Security, Yemen University, Sana'a, Yemen. \textsuperscript{e}Department of Information Technology, University of Modern Sciences, Sana'a, Yemen.

Abstract In today's digital age, the banking sector faces increasing challenges in ensuring operational resilience, protecting customer assets, and maintaining a competitive edge. Prioritizing information security risk management (ISRM) practices is crucial to effectively address these challenges. This paper aims to demonstrate the effectiveness of the multi-criteria decision-making (MCDM) method in evaluating and improving ISRM practices in Yemeni banks. The study employs an integrated CILOS-TOPSIS model, considering two criteria and five sub-criteria, with criteria weights determined using the CILOS method. The results highlight the significance of specific criteria in ISRM, with the existence of a comprehensive business continuity and disaster recovery plan (C2.1) standing out as a top priority (weight: 0.266). Additionally, the frequency of data backups and the presence of an active backup policy (C2.2) and the adequacy of physical security measures (C1.1) are identified as crucial factors (weights: 0.228 and 0.203, respectively). Furthermore, the TOPSIS method is employed to rank 13 banks based on these criteria, revealing the top-performing banks as B10, B4, B13, B1, and B12. Conversely, the 7th, 5th, and 6th ranked banks require attention for improvement. The paper provides comprehensive details on criteria weighting, bank ranking, and recommendations for enhancements. The findings presented in this paper offer valuable insights to decision-makers in the banking sector, enabling them to effectively guide their efforts and allocate resources to areas, controls, and banks that require greater attention.

Keywords: banking, CILOS, information security, risk management, MCDM, TOPSIS, Yemen

1. Introduction

Information and communication technology (ICT) and information assets are essential for the success of the banking sector. According to Kauffman and Riggins (2012), ICT plays a crucial role in a maturing microfinance industry, benefiting customers, microfinance institutions, donors, and the industry as a whole. The researchers found a positive impact of ICT at various levels. However, it is important to acknowledge and address the challenges and risks associated with ICT usage. Similarly, Ngoc Thach et al. (2021) emphasize the significance of ICT in data processing, secure transactions, and advanced analytics for risk management in financial businesses. Nasser (2017) and Nasser et al. (2018) emphasize the significance of information assets, such as customer data and proprietary algorithms, in driving innovation and maintaining a competitive edge. Implementing robust security measures is crucial to safeguarding these assets and upholding customer trust (Nasser et al., 2020; Al-Khulaidi et al., 2023).

Additionally, Parate et al. (2023) and Hordofa (2023) specifically focus on the banking sector, highlighting its heavy reliance on ICT to streamline operations, enhance efficiency, and provide seamless services to customers. By effectively leveraging ICT, banks can remain competitive, meet customer expectations, and identify profitable opportunities. It is an integral component of any financial strategy aiming to facilitate access to a wide range of financial products and services (Hewa Wellalage et al., 2021).

However, the benefits of ICT and information assets are vulnerable to significant threats posed by cyberattacks. These attacks can have detrimental effects, including financial losses (Nasser et al., 2023), disruptions to banking operations (Al-Khulaidi et al., 2022), erosion of customer trust, damage to the reputation of banks, and theft of customer data (Balaram & Prabhu, 2023). To address these threats, numerous studies, as reviewed and reported by Urdenko (2019), have emphasized the importance of information security risk management measures. These studies shed light on the vulnerabilities faced by...
banks and the potential consequences they may encounter. The authors emphasize the implementation of robust information security risk practices (Al-Khulaidi et al., 2023; Urdenko, 2019; Nnatubemugo, 2013).

Financial institutions must prioritize the adoption of comprehensive information security risk management measures to safeguard themselves and maintain customer trust. Achieving a high level of information security risk management performance is crucial.

Many studies, including Nnatubemugo (2013), Barnes & Daim (2024), Barnes & Bridget (2021), and Al-Shameri (2017), have developed frameworks and methodologies to assist organizations in assessing their security posture and identifying areas for improvement. However, the goal is to provide flexible frameworks that organizations can tailor to focus on the specific security categories that are most relevant to their needs, as different organizations have varying security requirements (Al-Shameri, 2017). The proposed flexible maturity model by Nnatubemugo (2013) is an example of a framework that assesses risk management practices related to information security. This model incorporates five indicators, including the organization's ability to support the design of information systems for risk management requirements and actively implement and maintain effective mechanisms to respond to security attacks.

1.1. Research problem

Effective risk management is crucial for banks to mitigate the increasing complexity of cyber threats (Al-Khulaidi et al., 2023; Urdenko, 2019). Conducting a comparative analysis of risk management practices in the context of information security can provide valuable insights into identifying best practices and areas for improvement (Al-Khulaidi et al., 2023; Hewa Weallage et al., 2021). However, this analysis presents a multiple-criteria decision-making problem where various criteria and indicators need to be considered (Nasser et al., 2018). The importance of these criteria may vary across different banking environments. According to Miškić et al. (2023), it is essential to integrate comprehensive evaluation methods that capture all relevant performance inputs and weights to ensure an accurate comparison and ranking of the implementation of information security risk management across banks.

Disregarding the dynamic nature of a criteria's importance or assuming equal significance among dimensions can lead to misleading comparisons (Miškić et al., 2023), impeding banks' ability to implement effective security measures and address potential threats. Therefore, it is imperative to determine the criteria with the highest importance and allocate appropriate attention and resources to achieve optimal results in information security risk management, thereby strengthening the overall security posture of banks.

1.2. Research motivation

Effective information security risk management is crucial for safeguarding organizational information assets (Urdenko, 2019). In this regard, the application of multi-criteria decision-making (MCDM) techniques plays a pivotal role in guiding decision-makers (Miškić et al., 2023). By employing MCDM, decision-makers can evaluate and prioritize risks based on multiple criteria, enabling them to make well-informed decisions regarding risk mitigation strategies. This approach takes into account factors such as the effectiveness, cost, and compliance of potential security controls. Decision-makers utilize MCDM to optimize resource allocation by considering criteria like cost-effectiveness and risk reduction potential. This ensures the efficient and effective allocation of limited resources to address information security risks (Zhang et al., 2020; Ya-qing et al., 2023; Alghawli, 2021). Furthermore, MCDM aids decision-makers in meeting compliance obligations, incorporating stakeholder considerations, and promoting transparency in the decision-making process (Vassoney et al., 2021). The effectiveness of MCDM techniques in information security risk management is supported by various studies and research reports (Gardas et al., 2022; Turskis et al., 2019; Ershadi & Forouzanadeh, 2019). These sources offer empirical evidence and case studies that demonstrate the benefits of employing MCDM in guiding decision-making processes related to information security risk management. The versatility of MCDM enables decision-makers to effectively tackle complex decision problems by considering multiple criteria and factors, resulting in well-informed and robust decisions. Commonly used MCDM methods include ELECTRE (Elimination and Choice Expressing Reality), PROMETHEE II (Preference-Ranking Organization Method for Enrichment Evaluations), COPRAS (Complex Proportional Assessment), TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution), and VIKOR (Višekriterijumska Optimizacija I Kompromisno Rešenje), MARCOS (Measurement of alternatives and ranking according to COMPromise solution), each with its own strengths and weaknesses.

According to Gardas et al. (2022), TOPSIS, the Technique for Order of Preference by Similarity to Ideal Solution, is a highly effective tool for addressing Multi-Criteria Decision-Making (MCDM) problems. It has gained widespread popularity and extensive utilization in decision-making scenarios. The strength of the TOPSIS approach lies in its ability to compare all possibilities for a given problem. This method offers several advantages, including simplicity, rationality, comprehensibility, high computational efficiency, and the ability to quantitatively assess the relative performance of each alternative using a straightforward mathematical representation. Hezer et al. (2021) also highlight the popularity of TOPSIS in the field of MCDM due to its easy-to-follow computational steps, robust mathematical principles, and user-friendly nature. Furthermore, as mentioned by Acuña-Soto et al. (2017), TOPSIS is widely recognized as a commonly used ranking method due to its simplicity,
rationality, comprehensibility, computational efficiency, and ability to assess the relative performance of alternatives through a straightforward mathematical representation. The TOPSIS approach aims to select alternatives that are closest to the positive ideal solution (PIS) and farthest from the negative ideal solution (NIS). In the classical approach, the positive ideal solution maximizes criteria of the "the more, the better" nature and minimizes criteria of the "the less, the better" nature, while the negative ideal solution maximizes "the more, the better" criteria and minimizes "the less, the better" criteria.

Moreover, the task of determining the criteria weights presents a notable difficulty in MCDM methods due to their vital role in the ranking of different alternatives. However, in real-world scenarios, partial knowledge of criteria weights is common, making it one of the most complex aspects of MCDM. MCDM approaches can be classified into three primary categories: subjective, objective, and integrated. Subjective methods, such as AHP, ANP, SWARA, Delphi, SMART, SIMOS, DEMATEL, and BWMM, rely on the expertise, constraints, and preferences of the decision-maker to establish the weights. In contrast, objective methods utilize the data within the decision matrix to calculate the criteria weights and are generally considered more impartial and objective. Examples of objective weighting methods include entropy-based approaches, the entropy weight method, the coefficient of variation weight method, data envelopment analysis, regression techniques, CRITIC, D-CRITIC (Krishnan et al., 2021), and Criterion Impact Loss CILOS (Zavadskas & Podvezko, 2016). Integrated methods combine elements from both subjective and objective methodologies. For instance, a decision-maker may initially use a subjective approach to determine the initial weights and then employ an objective method to refine these weights based on the data within the decision matrix.

However, Zavadskas & Podvezko (2016) developed the CILOS method as an improvement over Mirkin's original entropy method. CILOS is an objective approach that considers the diminishing importance of criteria as they approach their optimal values. It assigns higher weights to criteria with a smaller relative loss of impact, indicating a greater significance. Conversely, criteria with a substantial relative loss of impact are given lower weights. This differs from the entropy method, which assigns higher weights to criteria with higher uncertainty. This can pose problems when some criteria are already at or near their optimal values, as they will still be assigned high weights even though they have less impact on the overall decision. The advantage of the CILOS method is that it overcomes this drawback of the entropy method by considering the diminishing importance of criteria (Ayan et al., 2023). This makes it a more accurate and reliable method for determining the weight of criteria in decision-making problems (Ayan et al., 2023).

1.3. Research gap

Effective information security risk management is crucial for banks to safeguard themselves against cyber threats. Yemeni banks face distinctive challenges, including the vulnerability of valuable assets to various attacks and threats, leading to potential financial losses and disruptions to business operations (Al-shaibany et al., 2023). Moreover, the underdeveloped banking system in Yemen, coupled with a lack of customer trust, further impedes the effective management of information security risks. Al-Fahim et al. (2021) have examined factors influencing the adoption of internet banking services in Yemen and found that trust significantly and positively impacts customers' intention to adopt such services. Additionally, certain banks in Yemen encounter specific risks inherent to their unique financing practices, such as credit risk, liquidity risk, operational risk, and legal risk (Siddiq et al., 2022). Collectively, these challenges underscore the need for enhanced information security management practices in Yemeni banks, particularly within the banking sector.

While multi-criteria decision-making (MCDM) methods have gained attention in information security risk management due to their ability to assess and prioritize risk management strategies, there exists a research gap concerning the application of MCDM methods specifically for evaluating information security practices in low-income countries like Yemen (Nasser et al., 2021). Local studies on the evaluation of information security practices across various domains (Nasser et al., 2020; Al-Khulaidi et al., 2022; Nasser, 2017), including information security risk management practices (Al-Khulaidi et al., 2023), primarily rely on statistical-based evaluation approaches that rank and analyze the maturity level of security. However, these approaches assume equal importance among all measurement indicators, potentially leading to misleading comparisons (Miškić et al., 2023). This research gap highlights the need for further investigation to address the unique context of Yemeni banks and explore the effectiveness of MCDM methods in enhancing information security risk management within these settings. By conducting comprehensive research in this area, we can bridge the existing gap, develop customized approaches, and contribute to the advancement of information security risk management practices in the banking sectors of low-income countries, ultimately bolstering their resilience against cyber threats.

The research objectives of this study are to utilize an MCDM model to evaluate information security risk management practices in Yemeni banks, with the aim of identifying areas that require improvement. The study aims to make several significant contributions. Firstly, it will conduct a comprehensive analysis of information security risk management practices in Yemeni banks, providing a thorough understanding of the current state of information security in this context. Secondly, the study intends to propose a framework to adapt the evaluation model specifically for the unique challenges faced by Yemeni banks, thereby addressing the contextual factors that influence information security risk management. This framework will contribute to the development of customized approaches tailored to the Yemeni banking sector.
Furthermore, the study emphasizes the importance of assessing criteria weights in evaluating the effectiveness of information security risk management practices. By considering the relative importance of various criteria, the study will provide insights into the factors that significantly impact the success of information security risk management strategies in Yemeni banks. This aspect of the research has the potential to enhance decision-making processes and resource allocation for information security risk management.

Lastly, the study aims to investigate and rank the information security risk management practices implemented by banks in Yemen using an MCDM model. This analysis will not only provide a comprehensive assessment of current practices but also contribute to the existing body of knowledge by demonstrating the applicability and effectiveness of MCDM methods in evaluating information security risk management in low-income countries like Yemen.

Through these research objectives, the study seeks to enhance the understanding of information security risk management practices in Yemeni banks and provide valuable insights for improving their effectiveness. The findings of this study will contribute to new knowledge by filling the research gap concerning the application of MCDM methods in evaluating information security practices in low-income countries. It will provide valuable insights into the state of information security risk management in Yemeni banks and offer practical recommendations for improving information security practices in this specific context.

2. Materials and Methods

The research methodology comprises the following key processes: data preparation, calculating the weights of criteria utilization using the CILOS weight method, ranking alternatives using the TOPSIS method, and subsequent comparison analysis. These processes are employed to thoroughly evaluate and analyze the extent of information security risk management within Yemeni banks.

2.1. Collecting and preparing the data for information security risk management decision matrix

This study utilizes an assessment framework developed by Al-Khulaidi et al. (2023) to evaluate the maturity level of information security risk management in Yemeni banks. The framework, which has undergone rigorous consensus and reliability testing, includes two primary criteria: (c) risk assessment and treatment, and (c) incident and business continuity management. Each criterion has a specific sub-criterion associated with it. The first criterion, risk assessment and treatment, consists of two sub-criteria: C1.1: Adequacy of physical security measures to protect information assets; and C1.2: Conducting a thorough risk assessment and implementing appropriate risk management measures for all information assets. The second criterion, Incident and Business Continuity Management, includes three indicators: C2.1: existence of a comprehensive business continuity and disaster recovery plan for the company's information systems and frequency of review and testing; C2.2: frequency of data backups and the presence of an active data backup policy and strategy; and C2.3: frequency of virus scans and implementation of necessary updates.

To analyze information security risk management in the examined banks, aggregated maturity index values ranging from 0 to 5 are used. The collected data is organized into a decision matrix, as shown in Table 1.

<table>
<thead>
<tr>
<th></th>
<th>C.1.1</th>
<th>C.1.2</th>
<th>C.2.1</th>
<th>C.2.2</th>
<th>C.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>B2</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>B3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>B4</td>
<td>4.7</td>
<td>4.3</td>
<td>4</td>
<td>4.7</td>
<td>4.7</td>
</tr>
<tr>
<td>B5</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>B6</td>
<td>3.3</td>
<td>2.7</td>
<td>3</td>
<td>4.3</td>
<td>5</td>
</tr>
<tr>
<td>B7</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>B8</td>
<td>4.3</td>
<td>3</td>
<td>4</td>
<td>3.7</td>
<td>5</td>
</tr>
<tr>
<td>B9</td>
<td>4.3</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>B10</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4.5</td>
<td>5</td>
</tr>
<tr>
<td>B11</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>B12</td>
<td>5</td>
<td>3.5</td>
<td>3.5</td>
<td>4.5</td>
<td>5</td>
</tr>
<tr>
<td>B13</td>
<td>4.7</td>
<td>4</td>
<td>4.3</td>
<td>4.3</td>
<td>4</td>
</tr>
</tbody>
</table>

Source: Al-Khulaidi et al. (2023)

2.2. CILOS method

The Criterion Impact Loss Method (CILOS) is a novel approach that focuses on evaluating the losses associated with each criterion by comparing them to the alternative that possesses the optimal (maximal or minimal) value. This method, which was introduced by Zavadskas & Podvezko (2016), provides a comprehensive framework that encompasses the logic,
ideas, and stages necessary for its application. In their publication, Zavadskas and Podvezko detailed the underlying principles and steps involved in implementing the CILOS method:

- Establish a decision matrix.

Let’s consider a scenario where we have m alternatives, denoted as A = {Ai | i = 1, 2,..., m}, and n evaluation criteria, represented as C = {Cj | j = 1, 2,..., n}. To capture the ratings given to each alternative for each criterion, we utilize a decision matrix, denoted as X. Equation (1) serves as the definition for this decision matrix. The matrix comprises cells (x_{ij}) that represent the scores assigned to each alternative (i) where i = 1, 2, ..., m, and the corresponding criterion (j) where j = 1, 2, n.

\[ X = [X_{ij}]_{m \times n} \]  

- Convert the cost criteria (minimizing criteria) into maximizing criteria.

In order to ensure that the highest value corresponds to the best value of a criterion, it is important to transform cost criteria into maximized criteria according to Equation (2). The values of the criteria that are already maximizing in nature remain unaffected. Within this context, \( x_j^c = \min \{x_{1j}, x_{2j}, ..., x_{mj}\} \), where m denotes the number of alternatives.

\[ p_{ij} = \begin{cases} x_{ij}, & \text{if } C \text{ is benefit criteria} \\ \frac{x_j^c}{x_{ij}}, & \text{if } C \text{ is a cost criteria} \end{cases} \]  

- Establishing a reference point for the upper limit of each criterion.

To determine the vector of maximum values for the criteria, we identify the largest (maximum) value for each criterion, denoted as \( p_j^+ \), using the formula (3). In this equation, \( p_j^+ \) represents the maximum value for criterion j, and m signifies the total number of alternatives.

\[ p_j^+ = \max\{p_{1j}, p_{2j}, ..., p_{mj}\} \]  

- Form a square matrix A

To construct a square matrix A, we utilize a decision matrix with n evaluation criteria, represented as C = {Cj | j = 1, 2,..., n}. The resulting square matrix, denoted as \( X = [x_{ij}]_{n \times n} \), is formed. In this matrix, each row corresponds to a criterion where the maximum value is attained. Consequently, the main diagonal of the matrix will contain the maximum values of each respective criterion.

- Establish the relative loss matrix (L)

Equation (4) is employed to establish the L matrix, represented as \( L = [l_{ij}]_{n \times n} \). This matrix encompasses the relative losses of each criterion, comparing the values of alternatives with the values of the alternative possessing the best value for criterion j.

\[ l_{ij} = \begin{cases} \frac{p_j^+ - a_{ij}}{p_j^+}, & i \neq j \\ 0, & i = j \end{cases} \]  

- Determine F, and Identify the objective weight for each criterion \( W_j \)

The weights \( w = (w_1, w_2, ..., w_n) \) can be determined by solving the linear equation system defined by \( Fw = 0, \sum_{j=1}^{n} w_j = 1 \), where the matrix F is as presented in equation (5).

\[ F = \begin{pmatrix} -\sum_{i=1}^{n} p_{1i} & p_{12} & \cdots & p_{1n} \\ p_{21} & -\sum_{i=1}^{n} p_{2i} & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & -\sum_{i=1}^{n} p_{ni} \end{pmatrix} \]  

2.3. TOPSIS method

The TOPSIS compromise ranking algorithm can be divided into the following stages (Hezer et al., 2021):

To begin, construct the normalized matrix \( p_{ij} \). In this study, the original matrix was normalized using the formula (6) for normalization.

\[ p_{ij} = \frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}} \]  

Second, create a weighted matrix \( [S] \) by multiplying the normalized matrix with the assigned weights for each criterion. This step involves multiplying the normalized scores in the matrix by their respective weights, resulting in a weighted score for each alternative and criterion.
\[ S = [s_{ij}]_{mxn} = [w_j]_{1xn} \ast [p_{ij}]_{mxn} \quad (7) \]

The next step is to calculate the Euclidean distances. During this stage, the Euclidean distance is computed for each alternative with respect to both the positive ideal solution and the negative ideal solution. The Euclidean distances \( D_i^+ \) and \( D_i^- \) are calculated for each evaluation object, using equations (8) and (9) respectively. The positive ideal solution represents the best achievable outcome for each criterion, while the negative ideal solution represents the worst possible outcome for each criterion.

\[
D_i^+ = \sqrt{\sum_{j=1}^{n} \left( s_{ij} - S_i^+ \right)^2}, \quad S_i^+ = \max\{s_{1j}, s_{2j}, ..., s_{mj}\} \quad (8)
\]

\[
D_i^- = \sqrt{\sum_{j=1}^{n} \left( s_{ij} - S_i^- \right)^2}, \quad S_i^- = \min\{s_{1j}, s_{2j}, ..., s_{mj}\} \quad (9)
\]

In the fourth step, the relative proximity to the ideal solution for each alternative are calculated using equation (10).

\[
C_i = \frac{D_i^-}{D_i^+ + D_i^-} \quad (10)
\]

Finally, the priority ranking for all alternatives is created in descending order based on the composite score obtained.

3. Results and Discussion

3.1. The application of the proposed approach for assessing information security risk management in yemeni banks

In this sub section, we undertake a thorough investigation into the detailed implementation process of the state-of-the-art integrated CILOS-TOPSIS model. This model serves as a powerful and efficient tool for assessing the practices of Information Security Risk Management (ISRM) among the 13 esteemed banks operating in Yemen.

3.1.1. Determining Weighted Criteria Values through the CILOS Method.

The weight values assigned to the criteria and sub-criteria presented in Table 1 were derived through a rigorous six-step approach known as the CILOS method, extensively elaborated in subsection 2.2. Let us now delve into each step to enhance our comprehension. The initial step involved creating three preliminary decision matrices (see Table 1). Step 2, which entails converting cost criteria (minimizing criteria) into maximizing criteria, was not applicable in our specific case as all the criteria in our problem are benefit criteria. Moving on to Step 3, we computed the maximum criterion vector, denoted as the vector of maximum values for each criterion, using equation (3). Proceeding to Step 4, we formed a square matrix A (Table 2). Equation (4) was then used to establish the L matrix, which represents the relative losses of each criterion (see Table 3). Additionally, equation (5) was employed to determine the F values (see Table 4).

The weights \( w = (w_1, w_2, ..., w_n) \) were subsequently determined by solving the linear equation system defined by \( Fw = 0 \). To derive the local weights of the C1 and C2 criteria based on the given global weights of the sub-criteria (C.1.1, C.1.2, C.2.1, C.2.2, C.2.3), the global weights of the sub-criteria within each criterion were summed up and then normalized. Furthermore, by normalizing the global weights of the sub-criteria within each criterion, the local weights of each sub-criteria were obtained. The results of these calculations are presented in Table 5.

3.1.2. Ranking the banks using the TOPSIS method

In this subsection, the procedure and results of applying the TOPSIS method to assess the maturity level of 13 Yemeni banks in ISRM are presented. The approach begins with constructing a weighted matrix, taking into account the normalized matrix and assigned weights for each criterion. Next, the Euclidean distance is computed for each alternative in relation to the positive and negative ideal solutions. Equations (8) and (9) are used to calculate the Euclidean distances from the positive ideal solution and the negative ideal solution, respectively. Equation (10) is utilized to determine the comprehensive score indexes for each bank. Finally, based on these values, the alternatives are ranked.

This process is repeated three times, considering the Risk assessment and treatment (C1) criteria, Incident and Business Continuity Management (C2), as well as the overall evaluation framework with all risk management sub criteria. The outcomes of this ranking process can be found in Table 6.
Table 2 A Square matrix (A).

<table>
<thead>
<tr>
<th></th>
<th>C.1.1</th>
<th>C.1.2</th>
<th>C.2.1</th>
<th>C.2.2</th>
<th>C.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.1.1</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>C.1.2</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>C.2.1</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>C.2.2</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>C.2.3</td>
<td>5</td>
<td>3.5</td>
<td>3.5</td>
<td>4.5</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 3 The relative losses matrix (L).

<table>
<thead>
<tr>
<th></th>
<th>C.1.1</th>
<th>C.1.2</th>
<th>C.2.1</th>
<th>C.2.2</th>
<th>C.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.1.1</td>
<td>0</td>
<td>0.4</td>
<td>0.4</td>
<td>0.2</td>
<td>0</td>
</tr>
<tr>
<td>C.1.2</td>
<td>0.2</td>
<td>0</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>C.2.1</td>
<td>0.4</td>
<td>0.2</td>
<td>0</td>
<td>0.2</td>
<td>0.8</td>
</tr>
<tr>
<td>C.2.2</td>
<td>0.4</td>
<td>0.2</td>
<td>0</td>
<td>0.2</td>
<td>0</td>
</tr>
<tr>
<td>C.2.3</td>
<td>0</td>
<td>0.3</td>
<td>0.3</td>
<td>0.1</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 4 The F matrix.

<table>
<thead>
<tr>
<th></th>
<th>C.1.1</th>
<th>C.1.2</th>
<th>C.2.1</th>
<th>C.2.2</th>
<th>C.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.1.1</td>
<td>-1</td>
<td>0.4</td>
<td>0.4</td>
<td>0.2</td>
<td>0</td>
</tr>
<tr>
<td>C.1.2</td>
<td>0.2</td>
<td>-1.1</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>C.2.1</td>
<td>0.4</td>
<td>0.2</td>
<td>-1.1</td>
<td>0.2</td>
<td>0.8</td>
</tr>
<tr>
<td>C.2.2</td>
<td>0.4</td>
<td>0.2</td>
<td>0.2</td>
<td>-0.7</td>
<td>0</td>
</tr>
<tr>
<td>C.2.3</td>
<td>0</td>
<td>0.3</td>
<td>0.3</td>
<td>0.1</td>
<td>-0.8</td>
</tr>
</tbody>
</table>

Table 5 The local and global CILOS weights and ranks of all evaluation criteria and sub-criteria.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Local Weight</th>
<th>Rank</th>
<th>Sub criteria</th>
<th>Local Weight</th>
<th>Rank</th>
<th>Global Weight</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>0.330</td>
<td>2</td>
<td>C.1.1</td>
<td>0.615</td>
<td>1</td>
<td>0.203</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C.1.2</td>
<td>0.385</td>
<td>2</td>
<td>0.127</td>
<td>5</td>
</tr>
<tr>
<td>C2</td>
<td>0.670</td>
<td>1</td>
<td>C.2.1</td>
<td>0.397</td>
<td>1</td>
<td>0.266</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C.2.2</td>
<td>0.340</td>
<td>2</td>
<td>0.228</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C.2.3</td>
<td>0.262</td>
<td>3</td>
<td>0.176</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 6 The final ranking results.

<table>
<thead>
<tr>
<th>Ranking considering risk assessment and treatment factors</th>
<th>Ranking considering Incident and Business Continuity Management factors</th>
<th>Ranking considering all weighted sub-criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>D_{i}^{+}</td>
<td>D_{i}^{-}</td>
<td>C_{i}</td>
</tr>
<tr>
<td>B1</td>
<td>0.012</td>
<td>0.041</td>
</tr>
<tr>
<td>B2</td>
<td>0.025</td>
<td>0.028</td>
</tr>
<tr>
<td>B3</td>
<td>0.025</td>
<td>0.028</td>
</tr>
<tr>
<td>B4</td>
<td>0.007</td>
<td>0.042</td>
</tr>
<tr>
<td>B5</td>
<td>0.049</td>
<td>0.000</td>
</tr>
<tr>
<td>B6</td>
<td>0.028</td>
<td>0.021</td>
</tr>
<tr>
<td>B7</td>
<td>0.029</td>
<td>0.020</td>
</tr>
<tr>
<td>B8</td>
<td>0.019</td>
<td>0.032</td>
</tr>
<tr>
<td>B9</td>
<td>0.012</td>
<td>0.037</td>
</tr>
<tr>
<td>B10</td>
<td>0.000</td>
<td>0.049</td>
</tr>
<tr>
<td>B11</td>
<td>0.017</td>
<td>0.040</td>
</tr>
<tr>
<td>B12</td>
<td>0.012</td>
<td>0.042</td>
</tr>
<tr>
<td>B13</td>
<td>0.009</td>
<td>0.041</td>
</tr>
</tbody>
</table>

3.2. Findings and their discussion

This study proposes an effective multi-criteria decision-making approach that combines the CILOS and TOPSIS methods to evaluate the effectiveness of Information Security Risk Management (ISRM) in Yemeni banks. The primary objective is to provide a comprehensive evaluation of the necessary level of ISRM within these financial institutions. The proposed approach offers a reliable and well-established conceptual framework that contributes to the advancement of ISRM, addressing the critical need for robust security measures in financial institutions. To demonstrate the practical implementation of the approach, it has been successfully applied in Yemeni banks, showcasing its feasibility and relevance in real-world scenarios. In the subsequent sections, a detailed analysis of the decision-making process is conducted, providing comprehensive insights into the methodology and outcomes of the study.

https://www.malque.pub/ojs/index.php/msj
3.2.1. Results analysis of the evaluation criteria

The CILOS evaluation was conducted to determine the weights of ISRM criteria in Yemeni banks. The results of the evaluation, as shown in Table 5 and Figure 1, indicate that Incident and Business Continuity Management (C2) carries a higher weight (0.670) compared to Risk assessment and treatment (C1) (0.330). This means that the criteria and indicators related to Incident and Business Continuity Management are considered more important in assessing the effectiveness of Information Security Risk Management (ISRM) in Yemeni banks. The higher weight assigned to C2 implies that aspects such as the presence of a comprehensive business continuity and disaster recovery plan, frequency of review and testing, frequency of data backups, and implementation of necessary updates are considered critical factors in evaluating the maturity level of ISRM. These findings highlight the significance placed on ensuring the ability to handle incidents, maintain business continuity, and safeguard data in the context of information security management.

In Table 5 and Figure 2, the CILOS weights of the sub-criteria for Risk assessment and treatment are presented within the domain of "Risk assessment and treatment." The weights for the sub-criteria are as follows: C1.1 - Adequacy of physical security measures to protect information assets ranked highest with a weight of 0.615, indicating its greater importance in the evaluation. C1.2 - Conducting a thorough risk assessment and implementing appropriate risk management measures for all information assets had a relatively lower weight of 0.385.

These findings suggest that within the domain of risk assessment and treatment, the significance attributed to physical security measures is higher compared to conducting a thorough risk assessment and implementing risk management measures for all information assets.

Within the domain of "Incident and Business Continuity Management," as presented in Table 5 and Figure 3, the CILOS weights for the sub-criteria are as follows: "(C2.1) Existence of a comprehensive business continuity and disaster recovery plan for the company's information systems, and frequency of review and testing" stands out with a weight of 0.397, indicating its higher level of importance. "(C2.2) Frequency of data backups and the presence of an active data backup policy and strategy" also holds significant weight with a value of 0.340.

On the other hand, the sub-criterion "(C2.3) Frequency of virus scans and implementation of necessary updates" carries a lower weight of 0.262. These findings suggest that the presence of a comprehensive business continuity and disaster
recovery plan, along with the frequency of review and testing, as well as the frequency of data backups, are considered more important when evaluating the maturity level of Incident and Business Continuity Management in Yemeni banks.

When considering the overall weights of each criterion in the ISRM framework for Yemeni banks (see Table 5, and Figure 4), three sub-criteria emerge as particularly important. These sub-criteria include "(C2.1)" with a weight of 0.266, "(C2.2)" with a weight of 0.228, "(C1.1)" with a weight of 0.203. These higher weights indicate that decision-makers place significant emphasis on these sub-criteria when evaluating the effectiveness of ISRM in Yemeni banks. Existence of a comprehensive business continuity and disaster recovery plan for the company's information systems, and frequency of review and testing, Frequency of data backups and the presence of an active data backup policy and strategy, and Adequacy of physical security measures to protect information assets are all regarded as crucial elements in ensuring robust information security.

![Figure 3 The local weights of the incident and business continuity management sub-criteria.](image)

On the other hand, certain criteria, specifically "(C2.3)" with a weight of 0.176 and "(C1.2)" with a weight of 0.127, receive lower overall weights. These lower weights indicate that decision-makers assign relatively less importance to these factors when making decisions about Information Security Risk Management (ISRM). It is likely that other criteria are considered higher priorities within the context of Yemeni banks. These interpretations provide valuable insights into the relative significance and priorities of different criteria and sub-criteria within the broader ISRM framework for Yemeni banks. Decision-makers can utilize this information to guide their efforts and allocate resources towards areas that require greater attention, ultimately enhancing the security posture and effectiveness of ISRM in Yemeni banks.

### 3.2.2. Discussion of Ranking Results

The banks listed in Table 1 underwent a ranking and prioritization process using the TOPSIS method. The ranking was determined based on the relative closeness values of each bank, with the best-performing bank being the one that had the smallest deviation from the positive ideal solution and the greatest separation from the negative ideal solution. The results of the TOPSIS analysis, which took into account risk assessment and treatment factors, as well as Incident and Business Continuity Management factors, can be found in Table 6. Visual representations of the rankings based on these specific sub-factors are provided in Figures 5 and 6. The comprehensive TOPSIS results, considering all weighted criteria and sub-criteria, can be found in Table 7 and Figure 7.

According to the data presented Figure 5, Banks 10, 4, and 13 demonstrated superior performance in risk assessment and treatment compared to the other banks, securing the first, second, and third ranks, respectively. Similarly, Banks 10, 2,
and 4 exhibited exceptional performance in Incident and Business Continuity Management, attaining the highest ranks in this category, as shown in Figure 6.

Furthermore, considering all weighted criteria and sub-criteria, as shown in Table 6 and Figure 7, Bank 10 emerges as the top performer in Information Security Risk Management (ISRM), achieving the highest level of closeness to the optimal value (CSI) of 93%, as depicted in Figure 7. This remarkable accomplishment highlights the bank's strong commitment to implementing rigorous ISRM measures and demonstrates its exceptional performance compared to the other evaluated banks. Bank 10's dedication to prioritizing and effectively executing ISRM practices is evident, as it has made significant progress in strengthening its information security framework. On the other hand, banks B4, B13, B1, and B12 fall within the intermediate range in terms of their ISRM practices, with their relative closeness to the CSI value (Ci) ranging from approximately 70% to slightly below 79%, as shown in Figure 7. While these banks have made notable advancements in specific aspects of ISRM, there is still significant room for improvement to reach optimal levels. These institutions need to focus on enhancing their security measures and elevating their performance to align more closely with industry best practices and standards. By prioritizing these improvements, these banks can enhance their overall security posture and ensure a higher level of protection for their valuable information assets (Al-Khulaidi et al., 2023; Urdenko, 2019).
In contrast, banks B3, B6, B5, and B7 rank lower in terms of ISRM. Their relative closeness to the optimal value (CI) falls below the threshold of 54%. This significant disparity highlights the challenges these banks face in terms of ISRM. It is evident that these institutions require substantial improvements in their security systems and capabilities. Addressing these shortcomings is crucial for strengthening their overall security posture and safeguarding sensitive information integrity.

However, Banks 2, 3, 5, 6, and 7 should prioritize strengthening physical protection practices to safeguard information assets from all potential threats. Recommendations aligned with ISO 27001 and 27002 include conducting comprehensive risk assessments, implementing appropriate physical protection measures, keeping up with technological advancements, developing and implementing security policies, providing staff training, regularly testing and auditing security controls, and establishing effective incident monitoring and response protocols (Al-Khulaidei et al., 2023; Urdenko, 2019; Nnatubemugo, 2013). Additionally, banks 5, 6, 7, 8, 11, and 12 should improve risk assessment and management practices by conducting comprehensive assessments, establishing risk appetite, developing treatment plans, implementing continuous review processes, enhancing proactive risk management, fostering a risk-aware culture, and regularly auditing practices (Urdenko, 2019; Al-Khulaidei et al., 2022). To enhance business continuity and disaster recovery plans, banks 3, 5, 6, 7, 11, and 12 should develop comprehensive plans, conduct regular reviews and tests, integrate incident response procedures, provide training, establish robust backup and recovery mechanisms, foster continuous improvement, and ensure regulatory compliance (Nasser, 2017, Nasser et al., 2018; Hewa Wellalage et al., 2021). By implementing these measures, the banks can enhance information security, compliance, and risk management practices effectively.

3.2.3. Implication of study

In contrast to a previous study (Al-Khulaidei et al., 2023) that focused on evaluating ISRM practices in banks, this study goes a step further by analyzing the weights assigned to the criteria and sub-criteria of ISRM. It also ranks alternatives using the TOPSIS method while considering the CILOS weights assigned to those criteria and sub-criteria. Additionally, this study compares the rankings obtained with the results of the study by Al-Khulaidei et al. (2023), which ranked the banks using the statistical traditional mean (average) method.

The present study utilized the CILOS method to determine the weights assigned to ISRM factors. A greater CILOS weight signifies a greater level of importance for a particular factor. These findings establish a basis for information security managers in banks, as well as professionals and researchers in the field, to concentrate on the factors highlighted as significant by the CILOS method.

Assigning higher weights to Incident and Business Continuity Management compared to Risk assessment and treatment in Yemeni banks has several implications. Decision-makers prioritize managing business disruptions caused by incidents over the management of risks, indicating a reactive approach rather than a proactive one (Sawalha, 2021). They consider the impact of risk events more important than their likelihood, focusing on responding to incidents rather than preventing them. The presence of a comprehensive business continuity and disaster recovery plan, frequency of review and testing, and frequency of data backups are critical factors in evaluating the maturity level of Information Security Risk Management (ISRM) in Yemeni banks. This emphasizes the importance of handling incidents, maintaining business continuity, and safeguarding data. Decision-makers may allocate more resources towards activities such as business impact analysis and establishing contingency actions (Corallo et al., 2020). Decision-makers focus more on actual events and response actions rather than the possibility and proactive management of risk events. The adequacy of physical security measures, the presence of a comprehensive business continuity and disaster recovery plan, and the frequency of data backups are considered more important than conducting a thorough risk assessment and implementing risk management measures for all information assets. Decision-makers prioritize the effectiveness of Incident and Business Continuity Management based on the presence of a comprehensive plan, frequency of review and testing, and frequency of data backups. They may allocate more resources towards cost-effective measures to respond to significant business disruptions rather than assessing the likelihood and consequences of such events. These findings offer valuable insights into the importance and priorities of different criteria and sub-criteria within the comprehensive framework of ISRM for banks in Yemen. Decision-makers can leverage this information to inform their actions and allocate resources to areas that demand greater attention. Ultimately, this will contribute to improving the security posture and effectiveness of ISRM in Yemeni banks.

Regarding the TOPSIS results and the ranking of alternatives based on ISRM criteria and sub-criteria, Bank 10 stands out as the top performer, achieving the highest level of ISRM with a closeness to the optimal value of 93%. This highlights the bank’s strong commitment to stringent security measures. However, banks B4, B13, B1, and B12 have intermediate levels of ISRM, indicating room for improvement. These banks should focus on fortifying ISRM security measures, ensuring better protection for their valuable information assets. In contrast, banks B3, B6, B5, and B7 rank lower in terms of ISRM. Their relative closeness to the optimal value (CI) falls below the threshold of 53%. This significant disparity highlights the challenges these banks face in terms of ISRM. It is evident that these institutions require substantial improvements in their risk management capabilities.
In contrast to a previous study, (Al-Khulaidi et al., 2023) that focused on evaluating ISRM practices in banks using the statistical traditional mean (average) method, as shown in Figure 8, the current study found similar ranking findings for 31% of the alternatives. Namely, banks B2, B4, B9, and B10 consistently achieve similar rankings in both studies. However, the remaining banks (69%) have different rankings between the two studies. This indicates that the methods prioritize certain criteria differently, leading to variations in the rankings.

Furthermore, the ranking results demonstrate the variations in ISRM levels among the analyzed banks. These findings provide a starting point for identifying specific areas that require attention and improvement. By recognizing the gaps and vulnerabilities in their security practices, banks can allocate resources effectively and implement targeted strategies to enhance their ISRM efforts. Ultimately, this will contribute to a more secure and resilient banking environment.

![Figure 8](image.png)

**Figure 8** Comparison of ranking results between study methods for Yemeni banks’ ISRM practices.

### 3.2.4. Limitations and future work

This study conducted in this context has identified several limitations that need to be addressed for future research improvement. Firstly, the study focuses solely on ISRM practices within Yemeni banks using the CILOS-TOPSIS methods. To enhance the comprehensiveness of future studies, it would be beneficial to consider a broader scope that includes other industries or regions, as well as additional security dimensions. Furthermore, the study does not explore the reasons behind the observed disparities in the levels of banking ISRM. To gain a deeper understanding of these disparities and develop more targeted solutions, future research should aim to investigate the underlying factors contributing to the variations in security levels among banks. Additionally, future studies could benefit from evaluating other aspects of information security by employing alternative combinations of Multiple Criteria Decision Making (MCDM) approaches. This approach would provide a more comprehensive analysis and enable comparisons between findings derived from different methodologies.

### 4. Conclusions

Effective risk management is crucial for banks to mitigate the increasing complexity of cyber threats. Conducting a comparative analysis of risk management practices in the context of information security can provide valuable insights into identifying best practices and areas for improvement, facilitate the high-quality development and competitiveness of the information security management systems within these banks. In this paper, an integrated CILOS-TOPSIS model was applied to evaluate the ISRM practices of the Yemeni banks based on 16 factors. The weights of the criteria were determined using the CILOS method. Based on the results, it can be concluded that the most crucial criterion is "(C2.1) Existence of a comprehensive business continuity and disaster recovery plan for the company's information systems, and frequency of review and testing" stands out with a weight of 0.266. Following this, the criteria are ranked in the following order: "(C2.2) Frequency of data backups and the presence of an active data backup policy and strategy," with a weight of 0.228, and " Adequacy of physical security measures to protect information assets (C1.1) with a weight of 0.203. Next, the TOPSIS method was applied to rank 13 banks based on the aforementioned criteria. The results indicate that the highest-ranked bank is B10, followed by B4, B13, B1, and B12. Conversely, the 7th, 5th, and 6th banks in the ranking are the lowest-ranked institution.

This research highlights the importance of prioritizing the strengthening of physical protection practices for Banks 2, 3, 5, 6, and 7 to protect their information assets from potential threats. To achieve this, it is suggested that these banks align...
their practices with ISO 27001 and 27002 standards. The suggestions include conducting comprehensive risk evaluations, implementing appropriate measures to safeguard physical assets, staying updated with technological advancements, developing and implementing security guidelines, providing staff training, regularly examining and assessing security measures, and establishing efficient procedures for monitoring and responding to incidents.

Furthermore, there is a need for Banks 5, 6, 7, 8, 11, and 12 to improve their risk assessment and management practices. This can be accomplished through comprehensive evaluations, establishing precise risk tolerance criteria, devising risk mitigation strategies, implementing continuous monitoring protocols, enhancing proactive risk management approaches, cultivating a risk-conscious environment, and conducting periodic audits. To strengthen the plans for business continuity and disaster recovery, Banks 3, 5, 6, 7, 11, and 12 should develop comprehensive strategies, regularly evaluate and assess them, incorporate procedures for responding to incidents, offer training, establish resilient backup and recovery systems, foster ongoing enhancements, and ensure adherence to regulatory requirements.

Implementing these recommended measures will effectively enhance information security, compliance, and risk management practices for the banks. By taking proactive measures, they can mitigate potential threats, safeguard valuable assets, and ensure the resilience and uninterrupted operation of their services.

**Ethical considerations**

Not applicable

**Conflict of Interest**

The authors declare no conflicts of interest.

**Funding**

This research did not receive any financial support.

**References**


