The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/1750-6166.htm

Transforming Government: People, Process and Policy

159

An intuitive approach to cybersecurity risk assessment for non-governmental organizations

Kawther Saeedi
Department of Information Systems, King Abdulaziz University, Jeddah, Saudi Arabia, and

Mariyam Abduljabbar Hassan, Suaad Alarifi and Haya Almagwashi
Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Received 19 August 2024
Revised 3 September 2024
19 September 2024
Accepted 22 September 2024

Abstract

Purpose – This study proposes a guided tool for cybersecurity risk assessment tailored for nongovernmental organizations (NGOs), enabling them to comply with cybersecurity policies despite limitations in security awareness, funding and expertise.

Design/methodology/approach – A digital transformation is indispensable for ensuring the sustainable operation of NGOs. Embracing a digital manifesto necessitates an awareness of cybersecurity risks, highlighting the critical need for a robust cybersecurity risk assessment methodology. Initial research phases revealed significant shortages in security awareness, funding and expertise. Consequently, this study introduces an intuitive approach tailored specifically for NGOs, supported by a customized tool designed to address their unique requirements. The NIST cybersecurity risk assessment framework and National Cybersecurity Authority (NCA) were adopted to define the risk assessment approach. The efficacy of this approach is evaluated qualitatively through a case study involving three NGOs in Saudi Arabia, aimed at assessing their capability to utilize the tool effectively. Following the implementation, a Likert-scale survey gauged satisfaction among NGOs regarding the tool's utility.

Findings – Results from the case study indicate high satisfaction, affirming its alignment with their operational needs and enhancement of compliance with NCA controls. Furthermore, the use of the tool enhances the awareness of NCA's cybercity requirements and controls.

Originality/value – Based on theoretical and empirical grounds, this research proposes a novel design of security assessment framework tailored for NGO requirements and supported by initiative tool enabling complying with cybersecurity policies and enhances the awareness of cybersecurity controls.

Keywords Cybersecurity, Nongovernmental organizations, Cybersecurity threats, Risk assessment tool, Security controls, Cybersecurity standard

Paper type Research paper

© Kawther Saeedi, Mariyam Abduljabbar Hassan, Suaad Alarifi and Haya Almagwashi. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at http://creativecommons.org/licences/by/4.0/legalcode

This research work was funded by King Abdulaziz University under Grant No. GPIP: 340-612-2024; therefore, the authors gratefully acknowledge the technical and financial support from the King Abdulaziz University, Jeddah, Saudi Arabia.

Transforming Government: People, Process and Policy
Vol. 19 No. 1, 2025
pp. 159-182
Emerald Publishing Limited
1750-6166
DOI 10.1108/TG-08-2024-0201

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

1. Introduction

Nongovernmental organizations (NGOs) rely on member support to address social issues in fields such as health, education and relief. NGOs, as not-for-profit entities, reinvest any surplus into their activities (Lyons *et al.*, 2006; Carey-Smith *et al.*, 2007). While they may receive funding from donors, participants and the government, they operate independently (Nações Unidas, 2003). Characterized by innovation, stakeholder commitment and limited resources, NGOs must still comply with regulations and governance, driving sector-wide change (Akingbola *et al.*, 2019; Visvizi and Lytras, 2020). In Saudi Arabia, NGOs are accredited and authorized by the Ministry of Human Resource and Social Development, and categorized based on activities like education, health and social services (MHRSD, 2024).

As technology advances, digital adoption becomes crucial for NGOs (Akingbola *et al.*, 2019). The shift toward digital transformation necessitates integration with government platforms for efficient data exchange and service delivery (Lin, 2019; Vermeulen and Von Solms, 2002). Governments mandate that NGOs comply with cybersecurity standards akin to the private and public sectors (Lin, 2019; Nações Unidas, 2003). Another compelling reason to adhere to these standards is the potential reputational damage affecting donors and volunteer support (Carey-Smith *et al.*, 2007).

Organizations typically choose cybersecurity risk assessment methodologies to identify requirements and protect assets from potential threats. Multiple standards exist, including those from the National Institute of Standards and Technology (NIST) (Shrivastava *et al.*, 2024), the International Organization for Standardization (ISO 27001) and the Organization for Economic Co-operation and Development (OECD), all aimed at safeguarding enterprise assets from vulnerabilities (Bowen *et al.*, 2006; Mierzwa and Scott, 2017). NIST guidelines are particularly detailed in their risk management approach compared to other standards (Ngamboé *et al.*, 2021). In Saudi Arabia, the National Cybersecurity Authority (NCA) has established specific controls and guidelines for all organizations (National Cybersecurity Authority, 2024).

NGOs encounter several challenges in adopting existing cybersecurity management standards and conducting risk assessments, including complexity, limited resources, lack of experienced staff, and constrained budgets (Hassan *et al.*, 2023; Carey-Smith *et al.*, 2007). Additionally, some NGOs do not prioritize cybersecurity (Enisa, 2024; Carey-Smith *et al.*, 2007). Hence, there is an urgent need for simplified approaches tailored to NGOs' capabilities and resource limitations. Current research suggests leveraging established standards such as NIST guidelines and ISO 27001 for assessing cybersecurity risks in NGOs, although their applicability to NGOs lacking cybersecurity expertise and resources remains largely unexplored.

This paper introduces a comprehensive approach to assess cybersecurity risks tailored specifically for NGOs facing resource constraints and limited cybersecurity management experience. The initial research phase identified security requirements, risks, and threats (Hassan *et al.*, 2023). Subsequently, this paper details the design and implementation of risk assessment tools customized to meet NGO requirements. A qualitative evaluation of this approach is then conducted through a case study involving three NGOs in Saudi Arabia. Organizations A, B, and C, though varying in size and sector, all face significant challenges in cybersecurity management. Organization A, a small health-focused NGO, lacks both a dedicated cybersecurity department and a standardized risk assessment methodology, delegating cybersecurity duties to a member of its IT team who also participated in tool testing. Organization B, a micro-sized NGO providing social services, is even more constrained, with no IT department and limited awareness of the necessity for cybersecurity controls, leaving the CEO to engage in tool evaluation. Meanwhile, Organization C, a

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

medium-sized health NGO, has implemented basic cybersecurity procedures and plans to comply with NCA controls, but despite possessing IT expertise, it lacks the resources to develop a standardized risk assessment methodology. The aim of the experiment is to evaluate their ability to effectively use the tool given their current capabilities. This assessment aimed to gauge their proficiency in tool utilization. Following the completion of cybersecurity risk assessments and subsequent analysis, a Likert-scale survey was administered to measure NGO satisfaction with the tool. The results highlight that NGOs found the tool satisfactory, meeting their needs while enhancing their understanding of NCA controls.

2. Theoretical framework

This section reviews the main concepts of the work related to this research. Section 2.1 provides an overview of cybersecurity risk assessment approaches. Section 2.2 presents related work focusing on cybersecurity management approaches managing for NGOs.

2.1 Cybersecurity risk assessment approaches

Risk assessment constitutes a fundamental component within the broader risk management process. According to the NIST standard (Stoneburner *et al.*, 2002), risk management encompasses the systematic identification, control and mitigation of risks pertaining to an information system. Specifically, risk assessment represents the initial phase in this process, enabling organizations to identify potential threats and risks associated with their information systems, assess the impact of these risks and identify appropriate measures to mitigate them. A critical determinant of the efficacy of the risk management process within an organization is the commitment of its members to implementing security controls and their awareness of the necessity of compliance with these controls. Therefore, conducting control analysis plays a pivotal role in the risk assessment process, as it aids in assessing the likelihood of threats occurring (Stoneburner *et al.*, 2002; Visvizi and Lytras, 2020).

The NIST SP 800-30 framework exemplifies a suitable cybersecurity risk assessment methodology for NGOs, as recommended by prior research (Shamala *et al.*, 2013). This framework encompasses essential elements, including the risk assessment process, risk model, assessment approach and analysis approach (NIST, 2012). The risk assessment process entails four distinct steps:

(1) Preparation for Assessment, involving the identification of information sources, risk models, assessment methods and analytical approaches;

(2) Assessment Execution, which encompasses threat identification, vulnerability identification, likelihood determination, impact assessment and overall risk determination;

(3) Results Communication, where assessment outcomes are conveyed to organizational managers and decision-makers; and

(4) Assessment Maintenance, supporting ongoing review of risk management decisions (NIST, 2012).

The risk model within this framework defines key risk factors and elucidates their interrelationships, focusing on threats, vulnerabilities, likelihood and impact (NIST, 2012). Assessment approaches dictate how values of these risk factors are quantitatively or qualitatively represented and integrated to ascertain the risk level (Sajko *et al.*, 2006; Shameli-Sendi *et al.*, 2016). Meanwhile, the analysis approach determines the initiation point and depth of the risk assessment, offering three distinct methodologies: threat-oriented, asset/impact-oriented and vulnerability-oriented (NIST, 2012).

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

2.2 Existing approaches to manage cybersecurity in NGOs

The majority of the recommended practices and approaches discussed in this section are applicable across various domains and are not specifically tailored to NGOs. However, we have chosen to present them here because researchers suggest and recommend them for implementation within the NGO sector. Many studies emphasize the importance of awareness programs aimed at employees to educate them on the significance of cybersecurity risk assessment and to promote adherence to best practices that enhance security management within NGOs. Kolb and Abdullah (2009) note that most NGOs prioritize fundraising and operational management over cybersecurity management and risk assessment. They advocate using NIST guidelines to develop a cybersecurity awareness program targeting employees. Recommendations include securing approval and support from top management to ensure adequate resources. In addition, assembling a team with diverse expertise – spanning legal, human resources and information technology – and conducting environmental assessments to review and amend policies as necessary. Surveying employees to assess their understanding of policies and initiating training sessions to bolster security awareness are further proposed actions.

Carey-Smith *et al.* (2007) proposed an approach for enhancing cybersecurity management in NGOs. They use action research as a methodology and use the technology acceptance model within a theoretical framework. Their approach aims to empower NGO employees to enhance their skills and capabilities autonomously, aligning with the characteristic consensus-based decision-making and informal relationships among members that distinguish NGOs from small enterprises.

Ghani *et al.* (2019) examined the impact of employees' comprehension of the risk assessment process on risk management within NGOs. They use surveys to test their hypothesis that employee knowledge and understanding of risk identification, assessment and management contribute significantly to effective risk control. The researchers acknowledge potential limitations in their findings due to the small sample size, focusing on only one NGO. Consequently, they advocate urgently implementing awareness programs aimed at enhancing employee proficiency in risk management.

Carey-Smith *et al.* (2007) discussed the applicability of ISO 27001 within NGOs, highlighting its challenges due to its expense and complexity for those lacking cybersecurity management expertise. He recommends strategies such as effective financial and human resource management, hiring personnel with requisite cybersecurity skills and instituting awareness programs that underscore the importance of cybersecurity risk assessment. Moreover, he suggests engaging students and graduates in NGO work to prepare them for addressing real-world cybersecurity challenges.

In addition to employee awareness programs on cybersecurity risk assessment, other studies emphasize the necessity of developing comprehensive cybersecurity risk management plans. Lee E. Rice *et al.* stress the importance of crafting such plans for NGOs to safeguard critical assets and data, despite the inherent challenges. They advocate for universal prioritization of cybersecurity risk assessment across all departments and staff (Rice, 2012).

Mierzwa and Scott (2017) argued that despite resource constraints, NGOs can leverage existing cybersecurity standards like ISO 27001 and NIST guidelines to develop cybersecurity plans outlining steps to address cybersecurity concerns. They also advocate for enhancing IT staff awareness to facilitate effective cybersecurity risk assessment activities within NGOs.

Imboden *et al.* (2013) identified budget as the primary determinant for NGOs considering cybersecurity management practices. They note that even organizations with sensitive data

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

may prioritize security based on financial considerations. They recommend using established and dependable cybersecurity templates and standards, alongside regular training and discussion of cybersecurity policies and practices among staff.

Conversely, Lin (2019) suggested practices for governments adopting e-government initiatives to collaborate effectively with NGOs. These include enhancing online services through open platforms, improving data management and sharing protocols with NGOs and actively enhancing e-government benefits across various departments.

Previous studies have shed light on improving cybersecurity awareness among employees through training programs, although resource constraints in NGOs may pose challenges to implementation. Researchers also underscore the importance of hiring cybersecurity management experts and developing security plans to mitigate risks within NGOs. While existing standards like ISO 27001 and NIST guidelines (NIST, 2012) are recommended for cybersecurity risk assessment, research on their suitability and methodological adaptation specifically for NGOs remains limited.

These previous studies collectively illuminate the nature of NGOs, their general challenges and security concerns, and propose recommendations to mitigate them. Identified threats and risks include data breaches, unauthorized access and modification of sensitive data, reputational harm, virus dissemination, phishing attacks, cyber-attacks, financial losses and donor attrition. Vulnerabilities identified include inadequate adoption of cybersecurity policies and controls due to resource limitations, lack of expertise in handling cybersecurity incidents and insufficient employee awareness (Kędra *et al.*, 2023).

Our research aims to explore appropriate methodologies to assist NGOs in effectively assessing cybersecurity risks, integrating insights from previous studies on identified threats and risks into our assessment approach.

3. Determine the requirements of the proposed approach

A survey conducted on accredited NGOs in Saudi Arabia, using the Ministry of Human Resources and Social Development's (MHRSD) directory, published in 2021, as the sampling frame. The directory listed 648 NGOs, classified mainly as social, health and educational organizations. Given the heterogeneity of the NGO population, a stratified multistage sampling design was used, dividing the sample into homogeneous groups based on administrative regions and further by NGO size (micro, small, medium, large). The sample size was determined using Cochran's formula, aiming for a 5% margin of error and a 95% confidence level. Due to outdated information in the 2014 NGO directory, additional steps were taken to update the sample frame, including excluding NGOs with incorrect contact details and supplementing data with information from social media. After these updates, 290 NGOs were included in the final sample frame, yielding 168 responses from a required 165, with a 75% response rate (Hassan *et al.*, 2023). The key finding from this survey indicates that a significant majority of Saudi Arabian NGOs lack experience and awareness in security practices, compounded by limited financial and human resources. These findings have informed the requirements for the proposed cybersecurity risk assessment tool and approach:

- The tool must prioritize ease of use, particularly for micro and small NGOs, considering their resource constraints and existing expertise.
- The assessment report should be innovative and easily comprehensible for NGOs.
- The proposed approach should enhance NGOs' awareness of potential risks to their assets and the corresponding controls to mitigate those risks.

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

4. Detailed methodology

The research conducted in 2022–2023 recommended the NIST SP 800-30 framework for cybersecurity risk assessment guidelines (van Haastrecht *et al.*, 2021). Accordingly, we chose the NIST SP 800-30 framework to develop our proposed cybersecurity risk assessment approach, as it is highly regarded for NGOs based on existing research (van Haastrecht *et al.*, 2021). Our initial steps in this process involved defining the risk assessment procedure by implementing the following stages:

- delineating the assessment elements; and
- conducting the assessment.

4.1 Assessment elements

In this step, we aim to define and prepare all the elements needed to create the proposed cybersecurity risk assessment approach. This step includes a set of substeps, which are as follows: identifying the risk model, identifying the sources of information to be used as inputs to the assessment, identifying the assessment approaches to be used, identifying the analysis approaches to be used and lastly identifying the assessment scales to be used.

4.1.1 Risk model. The risk model developed for our proposed approach encompasses the identification of key risk factors, namely, threats, vulnerabilities, likelihood and impact, and elucidates their interrelationships:

- *Threats:* These encompass events that possess the potential to adversely affect assets through unauthorized access, destruction, disclosure, modification of information or denial of service (NIST, 2012).
- *Vulnerabilities:* Defined as weaknesses in computer systems, programs, applications, procedures or any entity susceptible to exploitation by threats (NIST, 2012). Our chosen method for identifying cybersecurity vulnerabilities involves analyzing existing cybersecurity controls and policies within the organization.
- *Likelihood:* Refers to the probability that a threat event will lead to a negative impact, irrespective of the anticipated extent of damage (NIST, 2012).
- *Impact:* Represents the severity of damage anticipated from consequences such as unauthorized disclosure, modification, destruction, loss of availability of information systems, organizational processes or assets (NIST, 2012). To evaluate the impact of risks on assets, we categorized them into reputational, financial, productivity, safety and health, and fines/legal penalties. The impact within each category was assessed to determine the overall risk impact.
- *Risk:* Defined as the potential for a threat source to exploit a vulnerability, resulting in adverse effects on the organization (NIST, 2012).

4.1.2 Formulas of combining risk factors. We used the arithmetic mean algorithm to forecast the values of impact and likelihood for each vulnerability and threat. In addition, for assessing the risk level, we utilized a risk matrix comprising inputs from threat likelihood and impact categories. The final determination of the risk level was derived by multiplying the assigned ratings of likelihood and impact.

4.1.3 Sources of information. We identified various sources to compile lists of threats, vulnerabilities and risks, which serve as inputs for our assessment approach:

- *Literature review:* The studies reviewed in our literature survey highlighted numerous threats, risks and vulnerabilities encountered by NGOs. These include data leakage,

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

unauthorized access and modification of sensitive data, reputational damage, malware and phishing attacks, financial losses and donor attrition. Vulnerabilities identified encompass inadequate cybersecurity policies, resource limitations and staff awareness gaps (Ganin *et al.*, 2020; Stergiopoulos *et al.*, 2018).

- *NCA publications (National Cybersecurity Authority, 2024):* We consulted the NCA's quarterly report, detailing the top cyberthreats in Saudi Arabia for Q4 2020, such as unauthorized activities, malware, hacking attempts, data leaks and domain name spoofing.
- *ENISA taxonomy (Louis Marinos, 2016):* The ENISA taxonomy provided a structured framework to categorize threats, detailing affected assets and contributing factors for each threat.
- *Survey results (Hassan* et al., *2023):* The survey conducted in the first part of this research revealed significant gaps in the cybersecurity preparedness of NGOs, particularly among micro and small-sized organizations. A majority (74.5%) of NGOs lacked dedicated IT or cybersecurity departments, with only 23.6% having staff responsible for these functions. A minimal percentage (1.2%) outsourced their IT and cybersecurity activities. When asked about their commitment to managing information security risks, only 32.2% of respondents reported having implemented policies, primarily within medium and large NGOs. The survey also found that while some basic cybersecurity measures, such as maintaining customer privacy and securing devices with passwords, were relatively well implemented, other critical controls like regular data backups, antivirus activation and firewall deployment were less consistently applied:

> The findings further highlighted that most NGOs lack a standardized approach to information security risk assessment, with 92.4% not adhering to any recognized standard. A significant portion of respondents (56.7%) were unaware of the NCA guidelines, with only a small percentage currently planning to comply. Key obstacles to compliance include a lack of experienced personnel (50%) and financial resources (31.3%). In addition, the survey revealed a deficiency in cybersecurity awareness programs, with only 15.1% of NGOs offering training to their employees. This lack of awareness and training further exacerbates the challenges NGOs face in managing information security risks effectively.

- *NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems (Swanson, 2001):* We used the Security Self-Assessment Guide from NIST to develop assessment questions focusing on vulnerabilities and organizational compliance with controls aimed at mitigating the identified threats.
- *NCA Cybersecurity Controls (National Cybersecurity Authority, 2024):* We referenced Essential Cybersecurity Controls (ECC-1:2018), Cloud Cybersecurity Controls (CCC-1:2020) and Data Cybersecurity Controls (DCC-1:2022) provided by the NCA. These controls informed the development of assessment questions targeting vulnerabilities and adherence to basic cybersecurity requirements aimed at mitigating risks posed by identified threats within our approach.

4.1.4 Assessment approach. A qualitative assessment was used, utilizing questionnaires to gauge the likelihood and impact of scenarios using a risk matrix that categorizes risks as high, medium or low. The qualitative approach is chosen for its suitability in contexts where NGOs may lack sufficient expertise, particularly in security and information technology. It is noted for its efficiency in saving time, effort and costs, as evidenced in previous research

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

(Adrian Munteanu, 2006; Alzhrani *et al.*, 2022; Sajko *et al.*, 2006; Shameli-Sendi *et al.*, 2016). To express likelihood and impact values for each threat, semiquantitative scales were used. These scales enable calculating final likelihood and impact values using the arithmetic mean algorithm, aggregating user-selected responses from assessments of all threats and risks. The resulting likelihood, impact and overall risk levels presented in the final report are communicated using the qualitative approach.

4.1.5 Analysis approach. An asset/impact-oriented approach was adopted as it aligns with the available data, which includes a comprehensive list of risks compiled from a literature review. This approach begins by identifying the potential impacts on assets and subsequently identifies threat events that could lead to these impacts or consequences (NIST, 2012). In the proposed approach, the analysis commences with the identification of assets and their associated risks through a comprehensive literature review. During this phase, qualitative and semiquantitative scales specified by NIST SP 800-30 are applied to determine the values of likelihood, impact and risk levels, as detailed in the subsequent section.

4.1.6 Assessment scales. The assessment questionnaire within the proposed approach was translated into Arabic for broader accessibility and comprehension. Each question was carefully crafted to ensure clarity and to avoid repetition. There are five questions in total that assess the impact of each risk across various categories, including reputational, financial, productivity, safety and health, and fines/legal penalties. The questions are designed to evaluate the potential impact of each risk on these specific areas. Additionally, there are approximately 76 questions assessing the likelihood of threats occurring. These questions assess the organization's compliance with controls designed to mitigate the likelihood of the identified risks. All questions in the assessment are closed-ended, offering choices with semiquantitative scoring values. After aggregating the impact and likelihood scores, the total impact and total likelihood for each risk were then calculated. Finally, the risk level was determined based on predefined levels outlined in the risk assessment scale (refer to Tables 1 and 2).

4.2 Conduct risk assessment

Based on the preceding steps, the inputs for the proposed cybersecurity risk assessment approach were identified. Initially, we compiled a list of asset types as defined by the NCA in Saudi Arabia, encompassing tangible and intangible resources valuable to the organization. These assets include information (digital and physical), hardware, software, systems, services (digital and physical), locations and personnel.

Subsequently, we identified a list of risks associated with each asset type (refer to Table 3). Each risk was then linked to the specific threats that could lead to its occurrence, considering the category of asset involved (physical, digital or personnel). For each threat identified, we pinpointed the controls aimed at addressing the vulnerabilities that could

Table 1. Risk assessment scale

Likelihood \ Impact	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

Source: Garvey and Lansdowne (1998)

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

Table 2. Assessment scale – level of risk

Qualitative values	Semi-quantitative values	Description
High	4	Risk may result in multiple severe or catastrophic adverse effects on organizational operations and assets
Medium	3	Risk may lead to a serious adverse effect on organizational operations and assets
Low	0–2	Risk may result in negligible or limited adverse effects on organizational operations and assets

Source: NIST (2012)

Table 3. List of assets and associated risks

Risks	Asset
Information (digital, physical)	• Modifying the sensitive information of NGO • Exploit the sensitive information of NGO • Loss of information/records • Financial loss • Loss of reputation/donors • Exposure to the penalties stipulated in the relevant laws, legislations and regulations
Hardware	• Financial loss • Loss of hardware
Software	• Financial loss • Loss of software
System	• Financial loss • Disruption or blocking of the NGO's services • Loss of system
Service (digital, physical)	• Financial loss • Disruption or blocking of the NGO's services • Loss of reputation/ donors
Location	• Financial loss • Disruption or blocking of the NGO's services
People	• Disruption or blocking of the NGO's services

Source: Created by authors

trigger the threat. An example of linking the risk to the threats that contribute to its occurrence in Table 4. An example of linking threat to controls that reduce the possibility of a threat occurrence is in Table 5.

Building on these inputs, questions were formulated regarding the identified risks and threats associated with the listed assets, with the aim of assessing the likelihood and impact

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

Table 4. List of assets and associated risks

Risks	Asset
Modifying sensitive information	• Fraud • Sabotage • Theft (devices, storage media and documents) • Unauthorized physical access/unauthorized entry to • Premises • Malicious code and ransomware
Exploit sensitive information	• Fraud • Sabotage • Theft (devices, storage media and documents) • Information leakage/sharing • Unauthorized physical access/unauthorized entry to premises • Eavesdropping • Spam/phishing • Malicious code and ransomware • Information leakage/sharing

Source: Created by authors

Table 5. Threats and associated controls

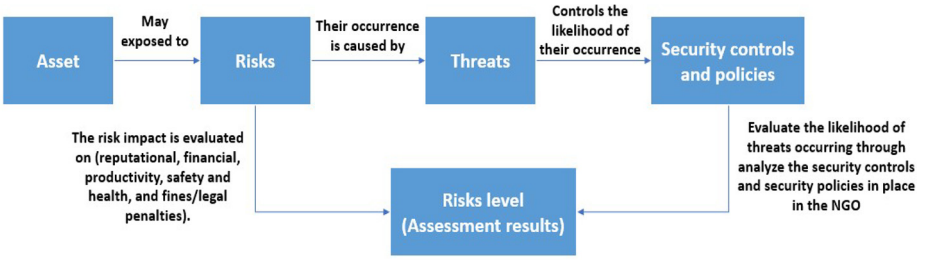
Qualitative values	Threat	Description
Disaster (natural, environmental)	Fire/ explosion/ flood/water damage etc.[…]	• Physical and Environmental Protection (NIST SP 800-26) • 2-2 Identity and Access Management (ECC-1: 2018) • 2-14 Physical Security (ECC-1: 2018)
Physical threats	Fraud	• IT system life cycle (NIST SP 800-26) • Personnel Security (NIST SP 800-26) • Physical and Environmental Protection (NIST SP 800-26) • Production, input/output controls (NIST SP 800-26) • Security Awareness, Training, and Education (NIST SP 800-26) • 1-10 Cybersecurity Awareness and Training • Program (ECC-1: 2018) • 2-2 Identity and Access Management (ECC-1: 2018) • 2-14 Physical Security (ECC −1: 2018)

Source: Created by authors

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

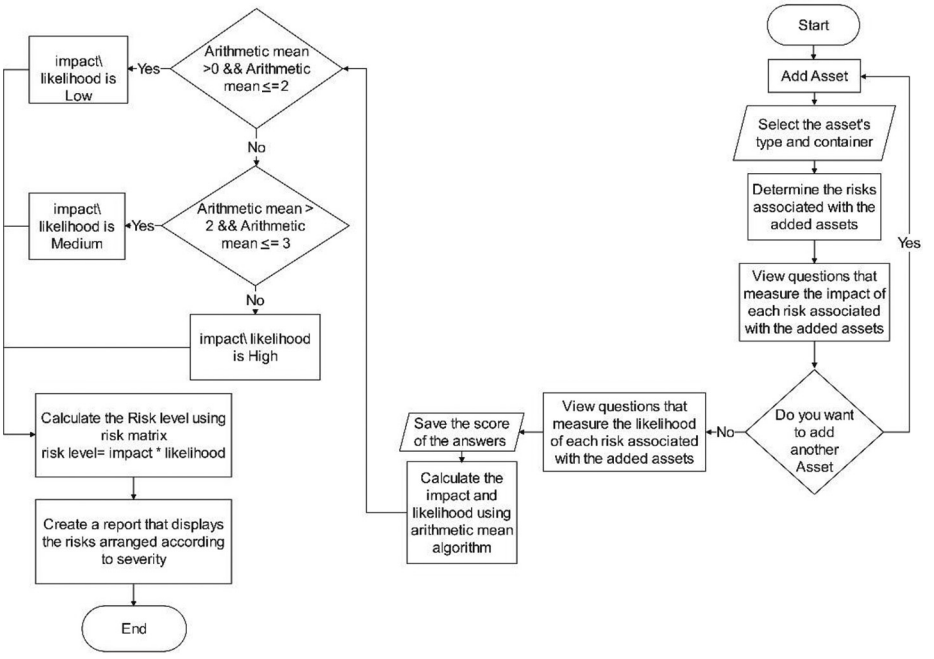
of each risk and subsequently determining its risk level, as depicted in Figure 1. The algorithm of the proposed approach is shown in Figure 2.

4.2.1 Validation of inputs. To validate the lists of asset types, risks, threats and controls created as inputs for the proposed approach, we engaged two experts renowned for their expertise in cybersecurity relevant to this research. These experts were selected based on their extensive experience and specialized knowledge in the field. Using a survey tool designed for evaluation purposes, the experts meticulously reviewed tables that link assets to



Source: Created by authors

Figure 1. Inputs of the proposed approach of cybersecurity risk assessment



Source: Created by authors

Figure 2. Flowchart of the proposed approach algorithm

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

their associated risks, as well as tables detailing the relationships between threats and the resulting risks. In addition, they assessed the alignment between threats and controls, ensuring that the controls effectively addressed the vulnerabilities leading to threat occurrences. Following the survey, the experts affirmed the overall validity of the lists while providing constructive feedback for refinement. We carefully considered their suggestions and incorporated them before finalizing the lists for adoption in the proposed approach.

5. Implementation and evaluation

We used Apache NetBeans, an open-source integrated development environment for Java, to develop a tool supporting our proposed approach. This tool functions as a lightweight, portable desktop application that does not require installation, facilitating easy transfer between devices. A key feature of the tool is its capability to generate assessment result reports in PDF format. In addition, we created a document linking the identified assets and risks from our approach with NCA controls aimed at mitigating these risks, aiding NGOs in focusing on controls relevant to their high-value assets. Screenshots of the tool developed are found in Appendix.

To evaluate the proposed approach of cybersecurity risk assessment in NGOs, we used multiple descriptive case studies to describe and document the assessment process. Multiple descriptive case studies were used because they are one of the tools that can be used to evaluate programs and provide researchers with a complete description of the phenomenon being studied (Bokolo, 2023; Qi and Chau, 2012; Saeedi *et al.*, 2023; Stockbridge, 1998). Also, multiple case studies are considered more convincing and increase the confidence of the results(Martinson and O'Brien, 2015; Stockbridge, 1998).We select study cases using the convenience sample and purposive sample approaches (Stockbridge, 1998). Because direct access to people and organizations is important when conducting a case study (Stockbridge, 1998), provided that the location of the case does not affect the evaluation (Stockbridge, 1998), the convenience sample approach is considered appropriate when it is difficult to obtain enough information from cases that are difficult to reach or locate (Stockbridge, 1998). Regarding the purposive sample approach, it is one of the often-used techniques in the study of program assessment (Stockbridge, 1998). Also, in the field of program evaluation, generalizability is crucial (Martinson and O'Brien, 2015), so it is important to choose the best cases, or what are referred to as exemplary cases, through which the effectiveness of programs may be explained (Martinson and O'Brien, 2015; Qi and Chau, 2012). In addition, according to studies, cases should be chosen at the organizational level based on their specific characteristics, such as their size or industry (Stockbridge, 1998).

In this research, we choose three cases, which are NGOs of micro, small and medium size; since micro and small-sized NGOs are considered the most widespread in Saudi Arabia, as we indicated in the survey that we conducted in the first stage (Hassan *et al.*, 2023). In Saudi Arabia, MHRSD classify organization according to number of employees. Large (250 and more full-time employees), medium (50–249 full-time employees), micro (1–5 full-time employees) and small (6–49 full-time employees) (MHRSD, 2024; monshaat, 2024), the same classification is used to classify NGOs in this research. Medium-sized NGO was chosen to make the cases diverse and represent an adequate range of cases. The selection criteria included the following:

- NGOs that participated in the first-stage survey;
- NGOs located in the Makkah Al-Mukaromah region and easily accessible; and
- NGOs that agreed to participate in this study to evaluate the proposed approach.

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

Direct observation is used to record factual data of what has happened and to clarify the context in which the program is being tested (Stockbridge, 1998; Martinson and O'Brien, 2015). While observing NGOs' experience with the proposed approach tool, we made sure that NGOs received the assessment report and successfully concluded the tool testing procedure. Also, we took notes on what is observed of their ability to use the tool without the need for assistance, as well as the time it takes for them to conduct the assessment using the tool.

Structured questionnaires are generally used when uniform information is desired from all participants and when the researcher can develop all the appropriate questions and all the possible answers according to his perception of what will happen (Stockbridge, 1998).

We developed a series of closed questions using a Likert-scale survey and we listed all possible choices. Through the survey we will investigate the extent to which the tool meets the requirements of NGOs. We decided to use closed questions in the survey after reviewing the literature and conducting the first stage survey of the methodology of this thesis, as it is the easiest and most straightforward way to take evaluation results from NGOs.

To evaluate our proposed approach, we conducted a case study involving three NGOs selected from survey participants in Stage 1. Data collection involved direct observation and structured questionnaires. We designed closed questions using a Likert-scale survey format, ensuring clarity and ease of evaluation based on insights from the literature review and our initial survey methodology. During the case study, we paid attention to monitoring the use of the tool by NGOs and the following evaluation criteria:

- assessing NGOs' ability to use the tool with their existing expertise and resources, without requiring additional external expertise or funding;
- evaluating the clarity of cybersecurity risk assessment results produced by the tool and NGOs' satisfaction with the presentation of these results in the final report;
- measuring the tool's effectiveness in enhancing NGOs' awareness of cybersecurity risks;
- determining NGOs' authorization and willingness to use the tool for periodic cybersecurity risk assessments in the future; and
- gauging NGOs' satisfaction with the document linking risks to NCA controls and its impact on their awareness of controls aimed at mitigating cybersecurity risks.

These criteria were essential in evaluating the tool's functionality and its potential to support NGOs in managing cybersecurity risks effectively.

6. Discussion

The results of this study underscore the pressing need for NGOs, particularly micro and small-sized organizations, to adopt robust cybersecurity risk assessment practices. Our proposed approach, based on the NIST SP 800-30 framework, was evaluated through detailed case studies involving three NGOs in Saudi Arabia, each varying in size. The findings from these case studies reveal significant insights and implications for the broader NGO sector, especially in regions where cybersecurity resources and expertise are limited.

6.1 Finding

6.1.1 Tool usability and accessibility. The tool developed to support the proposed cybersecurity risk assessment approach was well-received by the participating NGOs. It was found to be user-friendly, requiring minimal prior cybersecurity knowledge or technical

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

expertise. This is particularly significant for smaller NGOs that often lack dedicated IT departments or cybersecurity professionals. The ease of use of the tool enabled these organizations to conduct comprehensive risk assessments without the need for external assistance, which is crucial given their limited resources.

6.1.2 Awareness and understanding of cybersecurity risks. The study highlighted a gap in cybersecurity awareness among the participating NGOs, particularly in micro- and small-sized organizations. During the observation phase, it was noted that these NGOs often did not have documentation of their organizational controls and security practices. This lack of documentation led to delays in completing the risk assessment process, as staff were unsure about the consistent implementation of specific controls. The tool, however, played a pivotal role in increasing their awareness of potential risks and the necessary controls to mitigate them. By linking risks to specific NCA controls, the tool helped NGOs understand the importance of adhering to these guidelines.

6.1.3 Challenges in adopting cybersecurity standards. The study identified several barriers that hinder NGOs from adopting standardized cybersecurity risk assessment practices. The most prominent challenges include a lack of financial and human resources, insufficient cybersecurity training and awareness, and the absence of a structured approach to cybersecurity management. For smaller NGOs, these challenges are particularly acute, making it difficult for them to comply with NCA controls and other cybersecurity standards. The tool developed in this study addresses some of these challenges by providing a structured and accessible means for NGOs to assess their cybersecurity risks, even with limited resources. The summarized results of the evaluation of the proposed approach by NGOs are presented in Table 6 below. Various obstacles hinder NGOs, particularly small and micro-organizations, from adopting cybersecurity risk assessment standards. These challenges include a lack of experience and resources – both financial and human – as well as inadequate security awareness. The push toward e-government in Saudi Arabia has necessitated NGOs to undergo digital transformation, mandating compliance with NCA controls. Hence, an effective approach to assessing cybersecurity risks is essential for NGOs, influencing their adherence to NCA controls and aiding in the mitigation of potential risks and threats.

The three case studies provided valuable insights into the practical application of the proposed approach. Each NGO, varying in size, faced unique challenges, but all benefited from the structured process and guidance provided by the tool. The micro-sized NGO, for example, found the tool particularly useful in identifying risks that were previously overlooked due to their limited resources. The small-sized NGO appreciated the tool's ability to provide clear and actionable recommendations, which helped them prioritize their cybersecurity efforts. The medium-sized NGO, while more advanced in their cybersecurity practices, still found the tool beneficial in enhancing their existing processes and ensuring compliance with NCA controls.

6.1.4 Impact on digital transformation and compliance. The push toward digital transformation, especially in the context of e-government initiatives in Saudi Arabia, has made it imperative for NGOs to strengthen their cybersecurity posture. The study found that the proposed approach and tool could significantly enhance the ability of NGOs to comply with NCA controls, which are crucial for safeguarding their operations in an increasingly digital environment. The tool's alignment with these controls ensures that NGOs can systematically address potential vulnerabilities and threats, thereby reducing the risk of cybersecurity incidents that could disrupt their operations or damage their reputation.

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

Table 6. Summary of the findings from the NGO evaluation of the proposed approach

Case study	Main requirements	Tool evaluation results	Favorite features
Organization A	-Identify risks easily -The ability to use the tool without the need for experience in the field of cybersecurity. -Considering the budget and available resources of the organization	Satisfaction with the tool's features and that it fits the NGOs' requirements	The assessment report is easy to understand. It contains sufficient information to distribute to all organization staff
Organization B	-The ability to use the tool without the need for experience in the field of cybersecurity. -Considering the budget and available resources of the organization	-The tool meets the specifications suitable for NGOs -The tool should be used by an experienced employee who is familiar with the organization's internal processes to get more accurate results	The structuring of the report's contents and the use of color to denote risk level make it simpler for readers to understand and can aid the NGO in identifying priority risks for mitigation
Organization C	-The ability to quickly identify risks and propose countermeasures to mitigate cybersecurity risks -Considering the available budget and resources	Satisfaction with the tool's features and that it fits the NGOs' requirements	Clarity of the steps involved in adding assets and conducting assessment

Source: Created by authors

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

6.2 Implications

6.2.1 For NGOs. The findings suggest that NGOs, especially those with limited resources, can greatly benefit from adopting the proposed cybersecurity risk assessment approach. The tool not only simplifies the risk assessment process but also empowers organizations to take proactive steps in managing their cybersecurity risks. This is particularly important as NGOs increasingly rely on digital platforms for their operations, making them more vulnerable to cyber threats. By adopting this approach, NGOs can enhance their resilience against such threats and ensure the continuity of their services.

6.2.2 For policymakers. The study highlights the need for policymakers to prioritize cybersecurity awareness and capacity-building initiatives for NGOs. Given the challenges identified in this study, there is a clear need for targeted support programs that provide NGOs with the resources and training necessary to implement effective cybersecurity measures. Policymakers should also consider promoting the adoption of standardized risk assessment frameworks, such as NIST SP 800-30, to ensure a consistent approach to cybersecurity across the sector.

6.2.3 For future research and development. The successful implementation of the tool in this study opens up opportunities for further research and development in this area. Future work could explore the customization of the tool for different types of NGOs or expand its capabilities to include more advanced risk analysis features. In addition, longitudinal studies could assess the long-term impact of the tool on the cybersecurity posture of NGOs, providing further insights into its effectiveness and areas for improvement.

7. Conclusion

This study addresses a critical gap in cybersecurity risk management for NGOs, particularly those constrained by limited resources, expertise and funding. By developing a guided risk assessment tool tailored to NGOs' unique needs and aligning it with the NIST SP 800-30 framework and NCA controls, the research provides a practical solution to the cybersecurity challenges faced by NGOs in Saudi Arabia.

The evaluation of the tool through a qualitative case study involving three NGOs demonstrated several key outcomes. NGOs expressed high satisfaction with the tool's user-friendly design and its alignment with their operational and financial constraints. The tool effectively presented risk assessment results and linked them to NCA controls, meeting the practical needs of the organizations. However, challenges emerged, particularly for micro and small-sized NGOs, due to a lack of documented cybersecurity controls and procedures. This gap often led to delays in completing assessments, highlighting the need for NGOs to maintain and update their cybersecurity documentation regularly.

Moreover, the tool served as an educational resource, enhancing cybersecurity awareness among NGOs and underscoring the importance of adhering to NCA controls. This indicates that even organizations with limited expertise and resources can engage in effective cybersecurity risk assessments with the right tools.

The findings have significant implications for policymakers and practitioners. There is a clear need for enhanced cybersecurity education and resource allocation to support NGOs in developing and maintaining necessary cybersecurity documentation and procedures. In addition, future research should focus on customizing the tool for various types of NGOs and sectors, and expanding its features to address emerging cybersecurity threats.

In conclusion, this research contributes a novel framework and tool specifically designed for NGOs, enabling them to comply with cybersecurity policies and improve their cybersecurity practices. By addressing the practical challenges faced by NGOs and

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

enhancing their awareness of cybersecurity controls, this study supports the broader goal of strengthening cybersecurity across the NGO sector, particularly in regions undergoing rapid digital transformation.

References

Adrian Munteanu (2006), "Information security risk assessment: the qualitative versus quantitative dilemma", *Managing Information in the Digital Economy: Issues and Solutions - Proceedings of the 6th International Business Information Management Association (IBIMA)*, pp. 227-232.

Akingbola, K., Rogers, S.E. and Baluch, A. (2019), *Change Management in Nonprofit Organizations*, Springer International Publishing, Cham, doi: 10.1007/978-3-030-14774-7.

Alzhrani, F.E., Saeedi, K.A. and Zhao, L. (2022), "A taxonomy for characterizing blockchain systems", *IEEE Access*, Vol. 10, pp. 110568-110589, doi: 10.1109/ACCESS.2022.3214837.

Bokolo, A. Jr (2023), "Data driven approaches for smart city planning and design: a case scenario on urban data management", *Digital Policy, Regulation and Governance*, Vol. 25 No. 4, pp. 351-367, doi: 10.1108/DPRG-03-2022-0023.

Bowen, P., Hash, J. and Wilson, M. (2006), "Information Security Handbook", doi: 10.6028/NIST.SP.800-100.

Carey-Smith, M., Nelson, K. and May, L. (2007), "Improving information security management in nonprofit organisations with action research", The 5th Australian Information Security Management Conference, pp. 38-46.

Enisa (2024), "Enisa", available at: www.enisa.europa.eu/(accessed 19 August 2024).

Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D. and Linkov, I. (2020), "Multicriteria decision framework for cybersecurity risk assessment and management", *Risk Analysis*, Vol. 40 No. 1, pp. 183-199, doi: 10.1111/risa.12891.

Garvey, P.R. and Lansdowne, Z.F. (1998), "Risk matrix: an approach for identifying, assessing, and ranking program risks", *Air Force Journal of Logistics*, Vol. 22, pp. 18-21.

Ghani, E.K., Nor Hassin, N.H. and Muhammad, K. (2019), "Effect of employees' understanding on risk management process on risk management: a case study in a non-profit organisation", *International Journal of Financial Research*, Vol. 10 No. 3, p. 144, doi: 10.5430/ijfr.v10n3p144.

Hassan, M., Saeedi, K., Almagwashi, H. and Alarifi, S. (2023), *Information Security Risk Awareness Survey of Non-Governmental Organization in Saudi Arabia*, Springer International Publishing, Cham, pp. 39-71, doi: 10.1007/978-3-031-19560-0_4.

Imboden, T.R., Phillips, J.N., Seib, J.D. and Fiorentino, S.R. (2013), "how are nonprofit organizations influenced to create and adopt information security policies?", *Issues In Information Systems*, doi: 10.48009/2_iis_2013_166-173.

Kędra, A., Maleszyk, P. and Visvizi, A. (2023), "Engaging citizens in land use policy in the smart city context", *Land Use Policy*, Vol. 129, p. 106649, doi: 10.1016/j.landusepol.2023.106649.

Kolb, N. and Abdullah, F. (2009), "Developing an information security awareness program for a non-profit organization", *International Management Review*, Vol. 5 No. 2, pp. 103-107.

Lin, Y. (2019), "Government management model of non-profit organizations based on E-government", Proceedings of the 2019 7th International Conference on Computer and Communications Management, pp. 164-168, doi: 10.1145/3348445.3348464

Louis Marinos (2016), "ENISA threat taxonomy: a tool for structuring threat information.pdf".

Lyons, M., McGregor-Lowndes, M. and O'Donoghue, P. (2006), "Researching giving and volunteering in Australia", *Australian Journal of Social Issues*, Vol. 41 No. 1, pp. 385-397, doi: 10.1002/j.1839-4655.2006.tb00026.x.

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

Martinson, K. and O'Brien, C. (2015), "Conducting case studies", *Handbook of Practical Program Evaluation*, Wiley, New York, NY, pp. 177-196, doi: 10.1002/9781119171386.ch8.

MHRSD (2024), "Ministry of human resources and social development", available at: https://hrsd.gov.sa/

Mierzwa, S. and Scott, J. (2017), "Cybersecurity in non-profit and non-governmental organizations", ICIT, The Cybersecurity Think Tank.

monshaat (2024), "SMEs-definition", available at: www.Monshaat.Gov.Sa/En/SMEs-Definition

Nações Unidas (2003), *Handbook on Non-Profit Institutions in the System of National Accounts*, UNSD.

National Cybersecurity Authority (2024), "Essential cybersecurity controls", National Cybersecurity Authority, available at: https://nca.gov.sa/en/regulatory-documents/frameworks-and-standard-list/198/

Ngamboé, M., Berthier, P., Ammari, N., Dyrda, K. and Fernandez, J.M. (2021), "Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)", *International Journal of Information Security*, Vol. 20 No. 4, pp. 621-645, doi: 10.1007/s10207-020-00522-7.

NIST (2012), "Guide for conducting risk assessments", doi: 10.6028/NIST.SP.800-30r1.

Qi, C. and Chau, P.Y.K. (2012), "Relationship, contract and IT outsourcing success: evidence from two descriptive case studies", *Decision Support Systems*, Vol. 53 No. 4, pp. 859-869, doi: 10.1016/j.dss.2012.05.018.

Rice, L.E. (2012), "Non-profit organizations' need to address security for effective government contracting", *International Journal of Network Security and Its Applications*, Vol. 4 No. 4, pp. 53-71, doi: 10.5121/ijnsa.2012.4404.

Saeedi, K., Visvizi, A., Alahmadi, D. and Babour, A. (2023), "Smart cities and households' recyclable waste management: the case of Jeddah", *Sustainability*, Vol. 15 No. 8, p. 6776, doi: 10.3390/su15086776.

Sajko, M., Rabuzin, K. and Bača, M. (2006), "How to calculate information value for effective security risk assessment", *Journal of Information and Organizational Sciences*, Vol. 30 No. 2, pp. 263-278.

Shamala, P., Ahmad, R. and Yusoff, M. (2013), "A conceptual framework of info structure for information security risk assessment (ISRA)", *Journal of Information Security and Applications*, Vol. 18 No. 1, pp. 45-52, doi: 10.1016/j.jisa.2013.07.002.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016), "Taxonomy of information security risk assessment (ISRA)", *Computers and Security*, Vol. 57, pp. 14-30, doi: 10.1016/j.cose.2015.11.001.

Shrivastava, U., Han, B., Zhou, Y. and Razi, M. (2024), "The impacts of multiple privacy regulations and national security infrastructure on health information exchange: a study of hospitals across Europe", *Digital Policy, Regulation and Governance*, Vol. 26 No. 3, pp. 225-243, doi: 10.1108/DPRG-07-2023-0105.

Stergiopoulos, G., Gritzalis, D. and Kouktzoglou, V. (2018), "Using formal distributions for threat likelihood estimation in cloud-enabled IT risk assessment", *Computer Networks*, Vol. 134, pp. 23-45, doi: 10.1016/j.comnet.2018.01.033.

Stockbridge, K. (1998), "Case studies", *International Journal of Aromatherapy*, Vol. 9 No. 1, pp. 36-39, doi: 10.1016/S0962-4562(98)80045-3.

Stoneburner, G., Goguen, A. and Feringa, A. (2002), "Risk management guide for information technology systems", *NIST Special Publication*, Vol. 800 No. 30, pp. 800-830, doi: 10.6028/NIST.SP.800-30.

Swanson, M. (2001), *Security Self-Assessment Guide for Information Technology Systems*, doi: 10.6028/NIST.SP.800-26.

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W. and Spruit, M. (2021), "A threat-based cybersecurity risk assessment approach addressing SME needs", Proceedings of the 16th International Conference on Availability, Reliability and Security, pp. 1-12, doi: 10.1145/3465481.3469199.

Vermeulen, C. and Von Solms, R. (2002), "The information security management toolbox – taking the pain out of security management", *Information Management and Computer Security*, Vol. 10 No. 3, pp. 119-125, doi: 10.1108/09685220210431872.

Visvizi, A. and Lytras, M.D. (2020), "Government at risk: between distributed risks and threats and effective policy-responses", *Transforming Government: People, Process and Policy*, Vol. 14 No. 3, pp. 333-336, doi: 10.1108/TG-06-2020-0137.

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

Appendix

The user interface of the tool is in Arabic language which is the official language of the Kingdom of Saudi Arabia. We have developed a document that connects the assets and risks that we identified in the proposed approach with the NCA controls that contribute to mitigating those risks and to assist NGOs in concentrating on controls related to risks of the organization's high-value assets. We developed this document based on the inputs of the proposed approach, shown in Figure A1.

The screen in Figure A2 allows an NGO to enter its basic data, which includes the size of the NGO, the NGO's sector, address, phone numbers and other basic data.

In the adding assets section, the NGO selects the asset type and container type in addition to the asset name and its ID, shown in Figure A3. Then, when clicking on "Next," the risk impact assessment questions will be displayed based on user selected asset type, shown in Figure A4.

After adding all the assets, the user clicks on the "Start assessment" button, shown in Figure A5. Then, the tool will present the questions that assess the likelihood of the occurrence of threats associated with the assets added by the NGO, shown in Figure A6.

الضوابط الأساسية للأمن السيبراني

- سياسات إدارة الأمن السيبراني 1-2
- سياسات وإجراءات الأمن السيبراني 1-3
- الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني 1-7
- المراجعة والتدقيق الدوري للأمن السيبراني 1-8
- برنامج التوعية والتدريب بالأمن السيبراني 1-10
- إدارة الأصول 2-1
- إدارة هويات الدخول والصلاحيات 2-2
- الأمن المادي 2-14
- صمود الأمن السيبراني 3-1

تساهم الضوابط السابقة في التخفيف من المخاطر التالية:

الأصول	المخاطر
بيانات (الحاوية: مادي، رقمي)	• تعديل البيانات الحساسة من قبل أشخاص غير مصرح لهم • استغلال البيانات الحساسة للمنظمة • فقدان البيانات أو السجلات • التأثير السلبي على السمعة وفقد ثقة المتبرعين • التعرض للعقوبات المنصوص عليها في القوانين والتشريعات واللوائح ذات العلاقة
الأجهزة	• فقدان أو تلف الأجهزة
البرمجيات	• فقدان أو تلف البرمجيات
الأنظمة	• فقدان أو تلف الأنظمة • تعطل أو حجب خدمات المنظمة
الخدمات (الحاوية: مادي، رقمي)	• تعطل أو حجب خدمات المنظمة • التأثير السلبي على السمعة وفقد ثقة المتبرعين
مواقع	• تعطل أو حجب خدمات المنظمة
أشخاص	• تعطل أو حجب خدمات المنظمة

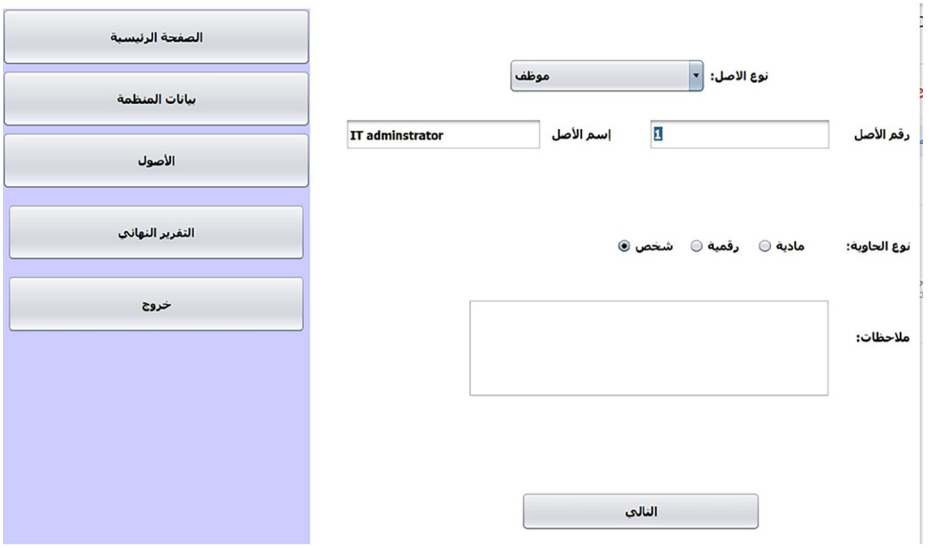
Source: Created by authors

Figure A1. Document that links the assets and risks identified in the proposed approach

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

Source: Created by authors

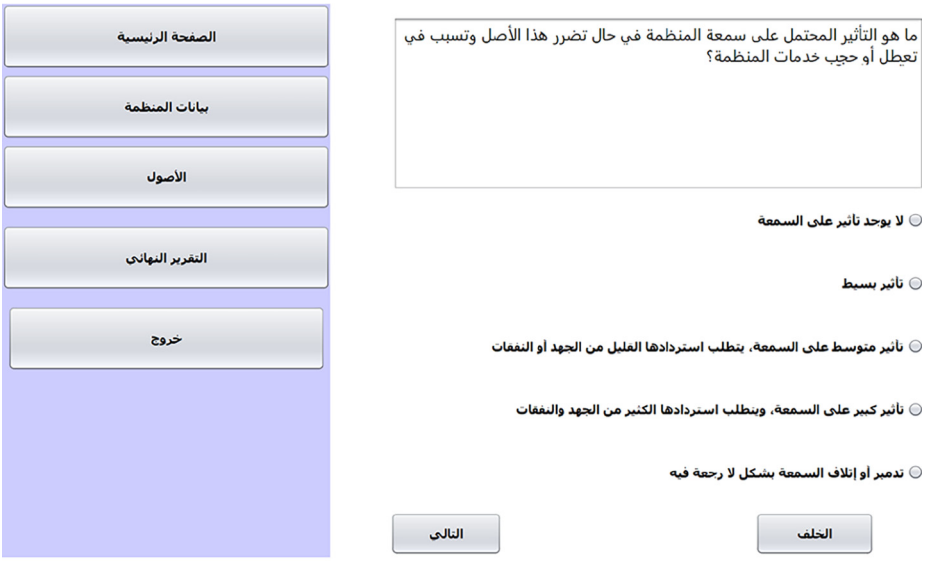
Figure A2. NGO basic data interface



Source: Created by authors

Figure A3. The interface of adding assets

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026



Source: Created by authors

Figure A4. Example of an impact assessment question interface

Source: Created by authors

Figure A5. Asset list interface

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

Source: Created by authors

Figure A6. Example of likelihood assessment questions interface

Source: Created by authors

Figure A7. Risk matrix of the assessment results

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026

After answering all assessment questions, the tool will display the results of the assessment and rank the risks on a risk matrix, shown in Figure A7. Also, through the "PDF" tab, the user can download the final assessment results report, which contains a list of assets and risks arranged by risk level, shown in Figure A8.

Source: Created by authors

Figure A8. The final report for the assessment results

Corresponding author
Kawther Saeedi can be contacted at: ksaeedi@kau.edu.sa

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**

Downloaded from http://ftp.nowpublishers.com/tg/article-pdf/19/1/159/9686005/tg-08-2024-0201.pdf by guest on 03 June 2026