



# The Effectiveness of Implementing an Information Technology Risk Assessment System in Improving the Performance of the Al-Misk Organization.

Assem I. Mohaidat\*

Department of Cyber Security, Irbid National University, Irbid, Jordan

**\*Corresponding Author:** Assem I. Mohaidat, Department of Cyber Security, Irbid National University, Irbid, Jordan

**Abstract:** The rapid evolution of information technology (IT) infrastructure, coupled with the increasing digitization of data and widespread adoption of digital innovations, has led to transformative changes in various industries. However, this progress has also introduced challenges such as insecure communication, intelligent adversaries, and software vulnerabilities. These complexities necessitate deploying robust IT infrastructure while ensuring security and risk management. This study aims to determine the significance of implementing an Information Technology Risk Assessment System in enhancing the performance of the Al-Misk organization and the difference it makes in safeguarding the information technology infrastructure of this institution when risk assessment is applied. The research followed a descriptive-analytical methodology. The tool used in this paper is form from the Institution of Occupational Safety and Health (IOSH). The findings indicate that the effectiveness of applying risk assessment in improving the organization's management was significant.

**Keywords:** RISK ASSESSMENT / INFORMATION TECHNOLOGY / IMPROVING

## 1. INTRODUCTION

As a result of the widespread digitization of data and information across various fields, the advancement of pervasive computing platforms, and the expansion and utilization of the Internet, industries are entering a new technological era. This transformative shift is rapidly reshaping the IT landscape within these industries. However, challenges arise due to insecure communication channels, intelligent adversaries both within and outside the realm, and software and system development vulnerabilities. These factors contribute complexity to the implementation of robust IT infrastructure.

Moreover, the diverse service-level requirements from customers, service providers, and users and industry-specific implementation policies further complicate this issue. Therefore, evaluating the associated risks when deploying IT infrastructure in industries becomes imperative, ensuring the security of the valuable assets at stake [1].

The rapid advancement of the IT sector is leading to the swift adoption and integration of digital innovations, such as open data, robotics, artificial intelligence, biometric authentication, crowdfunding, and big data. As digital technology progresses, the importance of enhancing information security and ensuring the reliability of these implemented technologies becomes increasingly evident. In contemporary society, the reliance on information technology and its seamless functioning is growing, underscoring the critical need for reliability and security. However, the spread of reported cybersecurity crimes is on the rise.

Risk assessment is one of the most important practical aspects of decision-making in various fields, such as industry, government, finance, and environmental management. It is a valuable tool for evaluating different aspects of complex systems, especially those that can significantly impact community well-being and safety. Hence, risk assessment plays a vital role in making informed

decisions, managing risks, and building robust information systems. Unfortunately, its importance is sometimes underestimated or not given the recognition it deserves. [2]

Information security risk assessment is a critical component of an enterprise's management practices, pinpointing, measuring, and prioritizing risks based on criteria aligned with the organization's risk tolerance and objectives. Risk management encompasses a comprehensive process involving identifying, mitigating, and potentially eliminating events that could negatively impact the resources within an information system. The overarching goal is to mitigate security risks that have the potential to compromise the integrity of the information system while maintaining a reasonable cost of protection.

This process involves thorough risk analysis, evaluating the parameter of "cost-effectiveness," and subsequently, selecting, creating, and testing security subsystems. Through it, we can explore all safety aspects, ensuring a holistic risk mitigation and management approach. [3]

## **2. RESEARCH PAPER PROBLEM**

Recently, there has been an increasing complaint by business owners due to the loss of their data and the inability to retrieve it. Many business proprietors fail to implement adequate data preservation measures, particularly those in industrial or artisanal sectors with limited familiarity with information technology. Consequently, this study has been conducted to raise awareness and provide guidance on the importance of risk assessment and precautionary measures.

## **3. RELATED WORKS**

### **3.1. Cybersecurity Risk Analysis**

Risk analysis is a fundamental process before any organizational evaluation or assessment. It serves as a learning mechanism and a proactive approach for the organization to foresee potential incidents. To achieve this, having analysis indicators in place becomes crucial to anticipate and predict these potential incidents, enabling the organization to respond proactively. [4]

### **3.2. Vulnerability**

Vulnerability encompasses any flaw or weakness within a system's design, implementation, operation, or management that could be taken advantage of to breach the system's security, consequently giving rise to potential threats. These vulnerabilities can manifest in various technical, functional, or behavioral aspects. [5]

Vulnerability can be defined as characterized as a weakness at the software and hardware levels within the components of IT systems. Such weaknesses can potentially be exploited by malicious actors, compromising the security of these components and the underlying network. Put differently, vulnerabilities are the known points of susceptibility that create an avenue for potential attacks on an organization's IT infrastructure.

For instance, if an organization's management inadvertently fails to deactivate access to resources and processes, such as login credentials for internal systems, after an employee has left, this oversight introduces unforeseen risks to the IT infrastructure. In many instances, these vulnerabilities are taken advantage of—deliberately or accidentally—by individuals inside or outside the organization who utilize the IT systems. The outcomes of such exploitation can have a substantial and adverse impact on the organization's valuable assets.

As a result, the initial and crucial step toward effective risk management of the IT infrastructure is to identify these weak points within the IT system's components. By doing so, the organization can ensure its IT resources' reliability, robustness, efficiency, and overall security. [1]

### **3.3. Threats**

A threat represents the possibility of undesirable outcomes arising from a specific circumstance, capability, action, or event that can potentially harm a system or an individual. These threats can emerge from natural occurrences, accidental incidents, or deliberate actions. Essentially, threats are a widespread phenomenon. [5] Threats can inflict varying degrees of harm upon the IT infrastructure of organizations, ranging from minor disturbances to severe damage. These threats emanate from diverse origins: natural, deliberate, or inadvertent. Natural threats encompass catastrophic events like floods, cyclones, and earthquakes. Conversely, unintentional

threats stem from organizational employee errors, such as improper resource access. Deliberate threats are engineered by attackers who disseminate malicious codes through the network, manifesting as spyware, malware, worms, viruses, and the like. Notably, recent instances include the October 24, 2019 incident where Ransomware and Distributed Denial-of-Service (DDoS) attacks incapacitated major South African banks, including Johannesburg, prompting a ransom demand of four Bitcoins, equivalent to approximately R500,000 South African Rand or USD 37,000]. The assessment of vulnerability and exposure of an entity plays a pivotal role in determining its susceptibility to threats. [1]

### 3.4. Risk vs. Hazard

"Hazard" and "Risk" those terms are highly employed in the context of risk assessment and management procedures. However, it is important not to conflate these terms, as they hold special meanings. Hazard pertains to the inherent capability of a machine, equipment, process, or material within the operational environment to cause harm to individuals, the surrounding environment, assets, or production processes. [6]

Risk is defined as an unforeseen event arising from a system malfunction, which significantly influences organizational assets and business goals. Generally, risk constitutes a qualitative evaluation of the probable security threat and its ramifications on the network. To put it differently, risk is characterized as the likelihood of detrimental consequences befalling organizations. [1]



**Figure1.** Comparison between Hazard and the Risk<sup>7</sup>

Referring to Figure 1, the individual is aware of the presence of sharks in the ocean. Hazards transform into risks solely in the presence of exposure. Sharks are categorized as hazards. Nevertheless, if you consistently avoid proximity to the ocean, you eliminate exposure to sharks and consequently, the risk of a shark attack becomes non-existent. [7]

Hence, it can be succinctly summarized as:

Risk = Hazard \* Exposure.OrRisk = probability \* impact

## 4. THE MAIN STEPS OF RISK ASSESSMENT PROCESS

The risk assessment process is a crucial step in ensuring the security and stability of IT infrastructure.

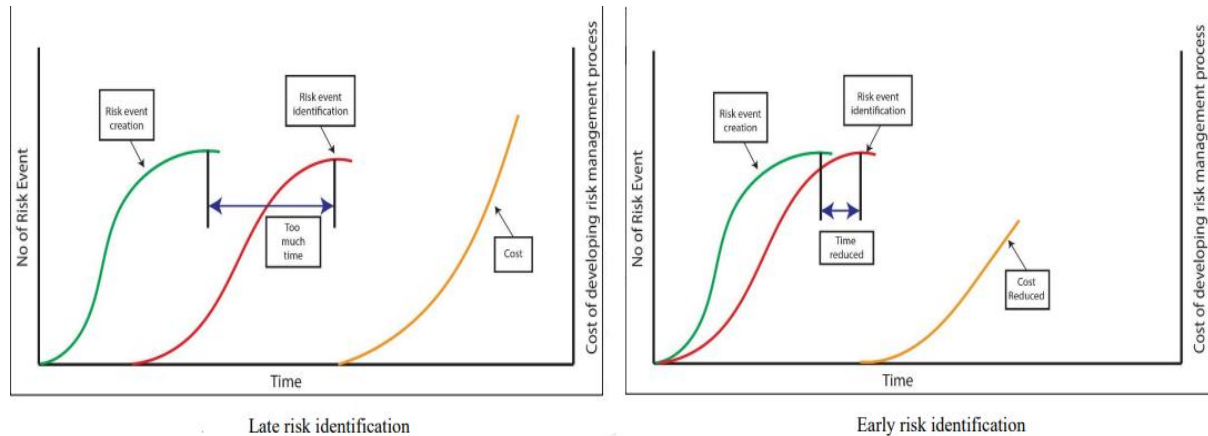
The process involves five essential steps:

### Step-1: Identify the hazard:

The main goal of this phase is to outline the process of identifying hazards that hold the potential to cause harm within a particular work task or environment. This procedure entails methodically observing and analysing each work area and task to reveal potential risks and hazards that exist while carrying out the job. These hazards are essentially inherent to the nature of the work itself. The scope

of this process encompasses a range of settings including machine workshops, laboratories, office spaces, agricultural and horticultural environments, storage and transportation areas, maintenance and outdoor spaces, reprographics facilities, as well as lecture halls and teaching spaces. All of this is primarily conducted for the purpose of assessment. [7]

The consequences of delayed hazard identification and timely hazard identification are illustrated in Figure 2, respectively. It's evident that a prolonged duration for recognizing all potential hazards leads to a substantially higher cost for establishing the management process compared to the scenario where hazards are identified early on. [6]



**Figure2.** *The impact of late hazard identification [6]*

**Step-2: Determine who and what might be harmed:**

Once the different risks are differentiated, it becomes necessary to ascertain who could be harmed and in what way [6]. Critical resources include process flows, enterprise information, and IT infrastructure assets critical to the operational and security aspects of the business. This understanding later helps to understand the implications of losing important information and facilitates decision-making regarding allocating resources that require protection.[1]

**Step 3: Evaluate the risks and decide on the precautions:**

Following the stages of "identifying the risks" and "determining who might be harmed and how," the subsequent step involves implementing protective measures [6]. This entails recognizing and reporting the vulnerability of elements within IT systems that could be susceptible to different types of attacks. In broader terms, the exposure of entities within IT systems is computed by comparing the potential vulnerable segment of an entity to the entity's overall volume. [1]

**Step 4: Record the findings and put them into place**

It is crucial to document your findings, and by doing so, you demonstrate that you have successfully identified hazards, determined potential harm and its sources, and outlined strategies for mitigating risks and hazards. This record should include specific details of identified hazards from the risk assessment and the actions taken to mitigate or eliminate those risks. This record serves as tangible evidence that the assessment was conducted and a foundation for future reviews of operational procedures. The risk assessment is an active document that should be accessible and readable rather than stored in a secluded location. [6]

**Step-5: Review the risk assessment:**

The risk assessment must be documented, as well as the mitigation strategies. Then, the concerned persons, like information technology staff and management, must contact this information to ensure that everyone is aware of the risks that may occur and how to address them. To ensure that the business continues safely, taking into account any new work practices or new technologies, it is necessary to review the risk assessment.



**Figure3.** *Steps of risk assessment process*

## **5. RISK ASSESSMENT TOOLS AND TECHNIQUES IN IT INFRASTRUCTURE:**

One of the critical aspects of performing a risk assessment in IT infrastructure is the effective utilization of appropriate tools and techniques. Several tools are available that aid in identifying vulnerabilities, evaluating risks, and prioritizing actions for mitigation. Let us delve into some of these tools and techniques:

### **5.1. Vulnerability Scanners:**

These specialized utilities are engineered to autonomously scrutinize networks, systems, and software applications for discernible vulnerabilities and weaknesses. A Vulnerability Scanner examines a predetermined array of ports on a remote host, aiming to evaluate the services operational on each port for any identifiable vulnerabilities. Notable examples of such tools include:

- 1- Nessus: This is among the most widely utilized vulnerability scanning utilities. It offers extensive tests to unearth vulnerabilities within networks and systems[8].
- 2- OpenVAS: This open-source utility leverages a perpetually updated vulnerability analysis and scanning database.
- 3- Nexpose: This tool offers vulnerability analysis capabilities that detect and categorize vulnerabilities, subsequently generating comprehensive reports.
- 4- Qualys: This platform provides an all-encompassing security assessment suite, encompassing features such as vulnerability scanning, threat response, web security, and patch verification.

### **Penetration Testing (Pen Testing)**

#### *5.1.1. What is Penetration Testing?*

The procedure of evaluating a computer system's vulnerabilities encompasses the identification of prospective threats and the simulation of attacks on the system. This form of testing is quintessential for maintaining an elevated security standard within an organization's IT infrastructure. It is advisable to conduct such assessments on a recurring basis or at least annually. Below are the five principal categories of penetration testing:

- 1- Targeted Testing
- 2- Internal Testing

3- External Testing

4- Blind Testing

5- Double Blind Testing

Here are some key importance of penetration testing:

- **Proactive Cybersecurity Measures:** Penetration testing serves as a preemptive strategy, enabling organizations to identify vulnerabilities and frailties in their systems prior to their exploitation by malevolent entities.
- **Risk Quantification:** This form of testing facilitates a nuanced understanding of the risks inherent in an organization's IT infrastructure. Such insights are instrumental in prioritizing security initiatives and optimally allocating resources.
- **Error Minimization:** Reports generated from penetration testing offer invaluable intelligence on system vulnerabilities. These insights contribute to reducing errors during the software development lifecycle, culminating in more secure applications and software platforms. [9]

#### *5.1.2. Penetration Testing Steps:*

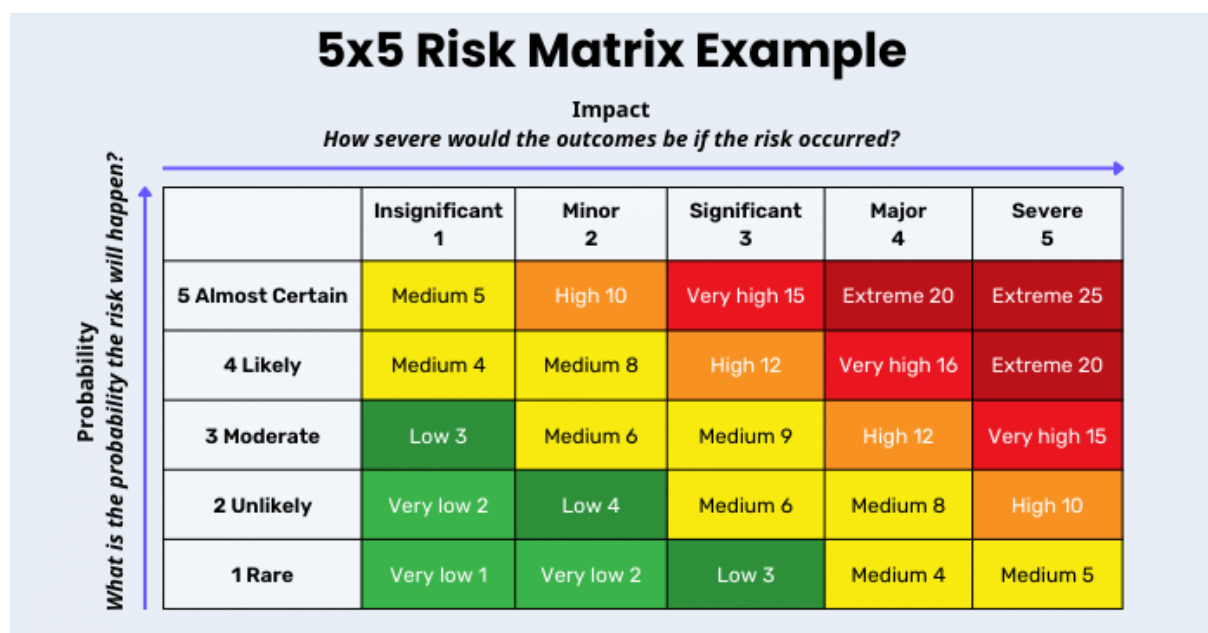
- 1. Reconnaissance and Data Aggregation:** Constituting the inaugural phase of penetration testing, this stage entails either active or passive accumulation of pertinent information about the target system. The objective is to amass data on variables such as open ports, network components, and operating systems. This phase can be executed utilizing publicly accessible information and specialized tools.
- 2. Scanning and Vulnerability Identification:** As an extension of the reconnaissance phase, scanning employs sophisticated technical utilities to pinpoint vulnerabilities within the target system. This phase encompasses the identification of operational systems, the compilation of vulnerability inventories, the detection of open listening ports, and the recognition of potential Internet gateways.
- 3. Attack and Gaining Access:** Upon identifying weaknesses, penetration testers exploit security vulnerabilities to gain unauthorized access to the target infrastructure. They may escalate privileges to demonstrate the extent of their intrusion. Tools like Metasploit are often used for exploiting vulnerabilities.
- 4. Maintaining Access and Penetration:** This phase evaluates whether the initial breach can be exploited to establish a persistent presence within the compromised system. The aim is to mimic advanced threats that can linger undetected for an extended period. Techniques such as planting rootkits and installing backdoors are common methods to maintain access.
- 5. Risk Analysis and Reporting:** The final phase involves generating a comprehensive report after the penetration testing project concludes or when the testers' activities are detected. This report encompasses a detailed account of identified vulnerabilities, step-by-step penetration methods, test summaries, recommendations for security improvements, and assessing potential damage. The report also includes the estimated cost of a breach. Penetration testing tools are used to gather this data.

In summary, penetration testing constitutes a methodical procedure that commences with the aggregation of information and scanning activities, progresses to the exploitation of identified

vulnerabilities, sustains access to emulate sophisticated threats, and culminates in generating a comprehensive report. This report delineates the findings and prescriptive measures for fortifying the system's security posture. [9]

### 5.2. Risk Matrices

Risk matrices function as graphical instruments designed to facilitate evaluating and prioritizing risks according to their likelihood and consequential impact. These matrices are indispensable for gauging the probability of risk occurrence and the prospective ramifications of such risks, as illustrated in Figure 4. The matrices quantify the recurrence probability of each event and assess the potential outcomes associated with each delineated risk. This evaluative process is visually encapsulated within a risk matrix, where risks are categorically sorted based on their probability and impact magnitudes. The matrix thus serves as an elucidative tool that assists in discerning the relative gravity of various risks.



**Figure4.** (5x5) Risk Matrix[10]

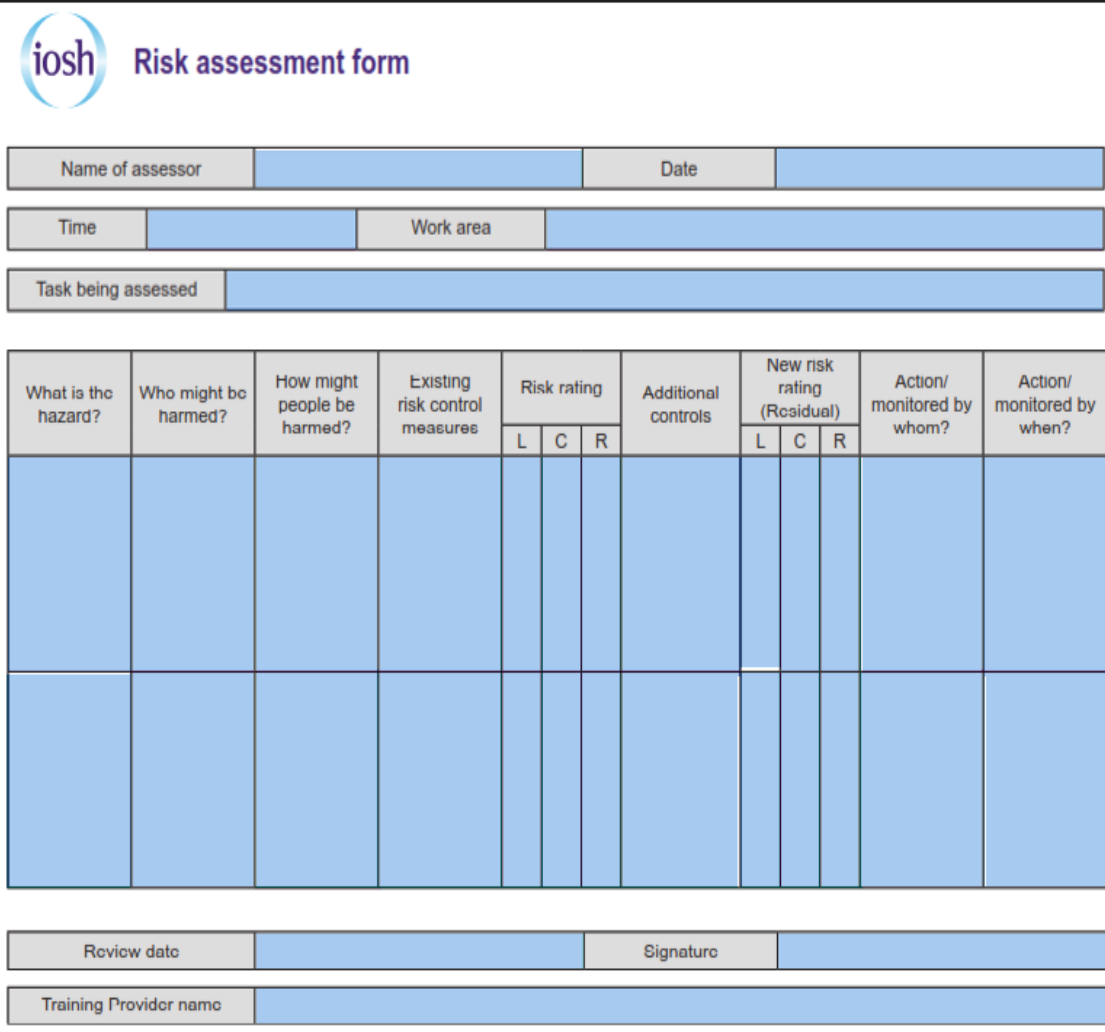
Moreover, impact assessment is an evolving procedure subject to ongoing refinement. Domain experts within the organization engage in periodic reviews to update the evaluations concerning the potential impacts of each identified risk. These experts leverage their specialized knowledge and insights to reassess the prospective outcomes associated with specific risks. This iterative process ensures that the impact assessment remains current and accurate, considering any shifts in organizational operations, technological landscape, or external variables that could influence the potential ramifications of risks.

Upon these experts' refinement of the impact assessment, it is integrated into a comprehensive risk assessment framework. This model amalgamates the probability and impact data derived from the risk matrices while incorporating other pertinent variables, such as organizational risk tolerance thresholds and objectives. This synthesized model executes either a quantitative or qualitative risk analysis, culminating in a prioritized inventory of risks based on their aggregate likelihood and potential impact.

The risk assessment framework has no universally prescribed model; its structure is contingent upon the specific organization and its extant procedures. Nonetheless, the chosen model must encapsulate the five stages previously delineated under "Risk Assessment Process." Figure 5 serves as an exemplar of a risk assessment form from IOSH.

**The Effectiveness of Implementing an Information Technology Risk Assessment System in Improving the Performance of the AI-Misk Organization.**

Ultimately, this risk assessment process generates final results that guide decision-making and risk management strategies within the organization. By integrating expert insights, updating impact assessments, and using a structured risk assessment model, organizations can make informed decisions to mitigate and manage risks effectively, safeguarding their IT infrastructure and valuable assets.



The form is titled "iosh Risk assessment form". It contains several input fields and a large table for risk assessment.

Input fields include:

- Name of assessor
- Date
- Time
- Work area
- Task being assessed
- Review date
- Signature
- Training Provider name

The main table has the following structure:

What is the hazard?	Who might be harmed?	How might people be harmed?	Existing risk control measures	Risk rating			Additional controls	New risk rating (Residual)			Action/monitored by whom?	Action/monitored by when?
				L	C	R		L	C	R		

**Figure5.** Form from the Institution of Occupational Safety and Health (IOSH)

**6. CASESTUDY**

In the following chapter, our focus will center on the execution of a hands-on risk assessment of the information technology infrastructure within AI\_MISK For Conditioning and Electromechanical Systems. This assessment will be carried out within the geographical context of Irbid Governorate in Jordan. We aim to arrive at a conclusive outcome by employing the exemplars provided above.

We intend to utilize the 5 x 5 Risk Matrix (illustrated in Figure 4) as an integral component of our risk assessment process and apply it to the model derived from the Institution of Occupational Safety and Health (IOSH) as depicted in (Figure 5). To facilitate this, we are in the process of engaging an expert affiliated with the Misk Foundation. The expert's role will be to provide estimations regarding the potential impact associated with each identified risk. Additionally, they will assist in determining the frequency of occurrence for each risk over a year, thereby enabling us to gauge its overall impact comprehensively.

Analyzing the collected data, we will assign a severity level to each risk, employing the risk mentioned above matrix. With this information, we can work out and implement appropriate corrective measures. Our ultimate aim is to investigate the desired outcome, as illustrated in Figure 6.



# The Effectiveness of Implementing an Information Technology Risk Assessment System in Improving the Performance of the Al-Misk Organization.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Name of assessor		Assem Mohaidat & Nour Al-Rashdan						Date		21/08/2023			
Time		09:00		Work area									
Task being assessed		IT Infrastructure											
What is the hazard?	Who might be harmed?	How might Information be harmed?	Existing risk control measures	Risk rating			Additional controls	New risk rating (Residual)			Action/monitored by whom?	Action/monitored by when?	
				L	C	R		L	C	R			
1. Cybersecurity Threats: 2. Data Breaches:	computerized information	1-Sensitive Information Theft 2- Infrastructure Disruption 3- Critical Service Disruption 4- Productivity Impairment	non	4	5	20	1- Implement strong firewalls 2- intrusion detection systems 3- Regularly update and patch software to address vulnerabilities 4- Conduct regular security audits and employee training on identifying and responding to threats.	1	5	5	IT department / Cybersecurity department		
												L = likelihood / probability	
												C = Consequences / impact	
												R = Risk = L * C	

A	B	C	D	E	F	G	H	I	J	K	L	M
3. Insider Threats (employees)	Archived papers / computerized information	1- Sensitive Information Leakage 2- Privacy Violations 3- Misuse of Information 4- Service Disruption	1- Policies and Procedures	4	4	16	1- Training and awareness 2- Access Management 3- Monitoring and Surveillance	1	4	4	IT department	
4- Natural disasters	Archived papers / computerized information	1- Infrastructure Destruction 2- Power and Communication Outages 3- Data Loss	non	1	5	5	1- Backup and Redundancy 2- Cloud Storage 3- Disaster Recovery Plan 4- Physical Security Measures	1	2	2	IT department	
5- Epidemics	Archived papers / computerized information	1- Work Disruption and Productivity Loss 2- Infrastructure Disruption 3- Increased Data Demand	1- Remote Work Solutions	3	5	15	2- Cybersecurity Awareness 3- Business Continuity Planning 4- Virtual Collaboration Tools	2	3	6	IT department	
6- Accidents	Archived papers / computerized information	1- Data Destruction 2- Operational Halts 3- Service Interruptions	1- Fire Suppression Systems	4	5	20	1- Off-Site Data Storage	3	3	9	IT department	

Figure 6. Applying the Five Steps in Risk Assessment

## 7. RESULTS

The assessment results clearly demonstrate a substantial enhancement in security levels and a noteworthy decrease in risk factors. Before undergoing the assessment, the organization had been confronted with significant threats. Nevertheless, through the thorough execution of the risk assessment process and the subsequent application of suitable corrective measures, these threats have been significantly alleviated.

Recommendations:

1. Promote adopting a risk assessment system within organizations and emphasize its importance.
2. Mandate implementing a risk assessment system when establishing new institutions.
3. Activate a monitoring system to oversee compliance with the risk assessment system.

## 8. CONCLUSION

In summary, this research underscores the critical significance of risk assessment within the dynamic landscape of information technology infrastructure. As industries undergo rapid digital transformation, the paper emphasizes the need for robust security strategies to mitigate evolving challenges such as cyber threats and vulnerabilities. The study elucidates the pivotal role of

identifying, quantifying, and prioritizing risks to align with organizational objectives by dissecting the fundamentals of risk assessment and illuminating its integral steps. Exploring risk assessment tools and techniques, encompassing vulnerability scanners, penetration testing, and risk matrices, further augments the comprehension of effective risk management strategies. Through a real-world case study, the practical application of these concepts reaffirms their pertinence and impact.

In conclusion, the paper advocates proactively incorporating risk assessment practices to fortify contemporary IT infrastructure. The call for broader acknowledgment of risk assessment's significance in decision-making and risk management strategies resonates with the imperative of adapting to the ever-evolving IT landscape. As industries navigate the intricate technology domain, risk assessment emerges as a pivotal pillar for preserving assets, upholding reliability, and fostering informed decision-making.

#### REFERENCES

- [1] Tripathy, B. K. (2020). Risk Assessment in IT Infrastructure. *In Security and Privacy From a Legal, Ethical, and Technical Perspective*. InTechOpen. DOI: 10.5772/intechopen.90907.
- [2] Zenonas Turskis, Nikolaj Goranin, Assel Nurusheva (2019). *Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach*. *Informatics*, 30(4), 851-864. Vilnius University. DOI: <https://doi.org/10.15388/Informatica.2019.203>
- [3] Ievgeniia Kuzminykh, Bogdan Ghita , Volodymyr Sokolov and Taimur Bakhshi (2021). *Entry Information Security Risk Assessment*. *Encyclopedia*, 1(3), 602-617. <https://doi.org/10.3390/encyclopedia1030050>
- [4] Daniel Jorge Ferreira, Nuno Mateus-Coelho, Henrique S. Mamede (2023). *Methodology for Predictive Cyber Security Risk Assessment (PCSRA)*. *Procedia Computer Science*, 219, 1555–1563. <https://www.sciencedirect.com/science/article/pii/S1877050923004581>
- [5] Ahonen, P., Alahuhta, P., Daskala, B., De Hert, P., Delaitre, S., Friedewald, M., Gutwirth, S., Lindner, R., Maghiros, I., Moscibroda, A., Punie, Y., Schreurs, W., Vildjiounaite, E., & Wright, D. (2008). *Safeguards in a World of Ambient Intelligence* (pp. 143-178). DOI: 10.1007/978-1-4020-6662-7\_4
- [6] Tanmoy Sinha. (2019). *Risk Assessment and Management*. DOI: 10.13140/RG.2.2.13427.48160.
- [7] © Udara S.P.R. Arachchige (2021). *Hazard Identification And Risk Assessment*. University of Sri Jayewardenepura. [https://www.researchgate.net/publication/356645393\\_Hazard\\_Identification\\_and\\_Risk\\_Analysis](https://www.researchgate.net/publication/356645393_Hazard_Identification_and_Risk_Analysis)
- [8] Avi Kak (2023). Lecture 23: Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing. In *Computer and Network Security*. ©2023 Avinash Kak, Purdue University.
- [9] Chamoth Madushan Jayasekara (2022). *Network Security & Penetration Testing: Case Study Analysis*. University of Plymouth. DOI: 10.13140/RG.2.2.20741.01768.
- [10] <https://safetyculture.com/topics/risk-assessment/5x5-risk-matrix/>

**Citation:** Assem I. Mohaidat , (2023). “The Effectiveness of Implementing an Information Technology Risk Assessment System in Improving the Performance of the AI-Misk Organization.”. *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)*, 9(2), pp.35-44. <http://dx.doi.org/10.20431/2349-4859.0902004>.

**Copyright:**© 2023 Authors, this is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.