Towards a Risk Assessment Matrix for Information Security Workarounds

Eugene Slabbert, Kerry-Lynn Thomson, Lynn Futcher

Towards a Risk Assessment Matrix for Information Security Workarounds

Eugene Slabbert[0000-0002-6342-8712], Kerry-Lynn Thomson[0000-0002-6456-9701] and, Lynn Futcher [0000-0003-0406-8718]

Nelson Mandela University, Port Elizabeth, South Africa
{s215028333, kerry-lynn.thomson, lynn.futcher} @mandela.ac.za

Abstract. Workarounds are often a necessary response to obstructions or inefficiencies within organisations. Their utilisation could, however, introduce information security risk into an organisation. It is, therefore, important for organisations to firstly identify, then determine the reasons for information security workarounds, and how to assess the potential risk they pose to the organisation. Workarounds are generally triggered by human factors which can be explained with the Protection Motivation Theory, as well as environmental influences that exist within an organisation. This is shown in the paper using a flowchart to illustrate the decision-making process of employees regarding information security workarounds. Having understood why workarounds occur within a particular organisation, the value of their information security risk can be determined using a Risk Assessment Matrix for information security workarounds and an accompanying Information Security Workaround Risk Index. Using the tools proposed in this paper, information security officers can respond appropriately to information security workarounds and, where necessary, make modifications to their information security policies, depending on the potential risk associated with the identified information security workarounds.

Keywords: Information Security Policy, Information Security Workaround Risk, Risk Assessment

1 Introduction

Information security is a major concern for modern organisations, all organisations rely on vast numbers of technologies and risk treatment methods, however, the human factor of information security in the form of non-compliance or resistance, remains the weakest link in the chain. One of these forms of non-compliance or resistance are workarounds. Workarounds exist everywhere and have the potential to introduce information security risk nearly every time they are used [2, 10]. Workarounds, therefore, need to be assessed to determine the level of risk introduced into an organisation. Ultimately, organisations should aim to eliminate information security workarounds. Workarounds are often employed by employees who feel that information security policies are irrational or inconvenient when considering their job expectations [10]. It should, however,

be noted that policies should always be designed and contextualised to meet the needs of the employees who are expected to comply with them. Without contextualising these information security policies, employees are less likely to comply them [15]. This paper aims to investigate information security policy workarounds which are a form of non-conformity with organisational policies. Further, the paper will discuss these workarounds and the potential information security risk their use introduces. Furthermore, the paper addresses the influencing factors regarding the utilisation of workarounds. Section 2 discusses information security risk assessment and introduces employee information security behaviour. Section 3 follows by defining workarounds and the various factors that influence them, which include both Human Factors and Environmental Factors in Section 4. Section 5 covers Alter's Theory of Workarounds and relates this to an employee's decision-making process when utilising workarounds. Section 6 presents Workaround Classification and Risk Assessment, and Section 7 concludes the paper.

2 Information Security Risk Assessment

Information security policies, such as the Acceptable Use Policy, are typical organisational documents that should be used to influence employee's information security behaviour, and compliance with these policies is required to minimise potential information security risk in an organisation.

As seen in Figure 1, Risk Management comprises Risk Assessment and Risk Treatment. Potential information security risks in an organisation should be assessed as part of overall organisational Risk Assessment [16].

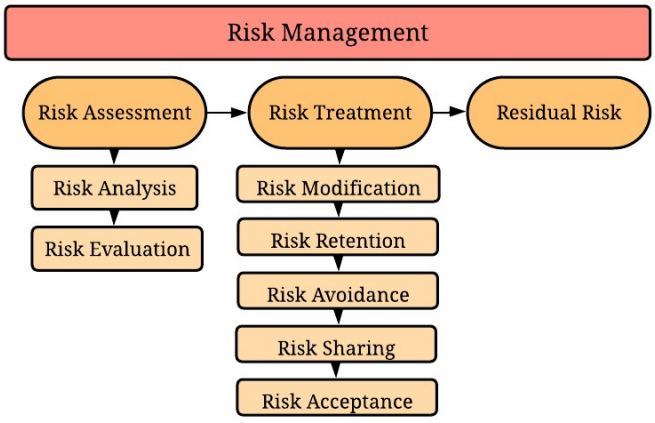

Fig. 1. Risk Management Process (adapted from [16])

Risk Assessment is done by identifying all important assets within an organisation and determining what the assets are vulnerable to, and the frequency at which a threat

may try to exploit the vulnerability [16]. A threat is an entity or natural occurrence, either internal or external to the organisation, that aims to take advantage of vulnerabilities that assets have. The vulnerability of an asset describes how likely an asset is to resist an attack from a threat. Assets are anything the organisation deems to be valuable to their operation. These assets are identified by the asset owner during the risk management process. An asset's impact value is determined by the importance of the asset to the organisation and the consequences of asset loss [16]. Asset impact value of an asset considers public reaction to a data breach, cost of fines and loss of the asset's value that it brought to the organisation. Asset impact value is not an exact value, but rather an organisationally relative value. An example of a risk assessment method can be found in ISO27005 [16].

As seen in Figure 1, following Risk Assessment, various actions could be chosen in Risk Treatment to address the risks identified. These actions are Risk Modification, Risk Retention, Risk Avoidance, Risk Sharing and Risk Acceptance.

Risk Modification considers the financial, time and operational constraints of an organisation when implementing controls to reduce the risk to an asset or group of assets.

Risk Retention is the acceptance of risk in its form if the organisation's operating goals allow for the risk to exist without affecting the organisation negatively.

Risk Avoidance is the process of modifying processes, procedures, or activities to avoid a specific risk that would not be financially viable nor efficient to manage reasonably.

Risk Sharing takes place by splitting risk between parties, sharing the consequences between those parties, such as insurance coverage on assets.

Risk Acceptance is when the identified risk is accepted by an organisation. Accepting the risk may prove to be beneficial, as the risk may allow for operational benefits such as efficiency or the risk may simply not demand enough priority to require treatment [16].

After Risk Treatment there is always going to be residual risk, which is the remaining risk after the above actions have been implemented. Residual risk is accepted and monitored in subsequent rounds of risk assessment in case the priority of these risks changes [16].

The information assets of an organisation could be put at risk if employees do not comply with information security policies. An employee's willingness to comply with information security policies is reliant on many factors. One of those factors is related to employees and their attitude towards the policy itself. According to Beautement *et.* al. [4], how useful an employee perceives an action to be and how easy the employee perceives an action is to perform plays a significant role in the employee's acceptance towards any related information security policies.

An employee's security behaviour is generally understood by considering their intention in the form of acceptance and resistance towards information security policies. When provided with full autonomy, an employee would be expected to be fully conformant and accepting of the organisation's policies, however, this is not always the case [3].

3 Workarounds Defined

Defined by Alter [2] a workaround is "*a goal-driven adaptation, improvisation, or other change to one or more aspects of an existing work system in order to overcome, bypass, or minimize the impact of obstacles, exceptions, anomalies, mishaps, established practices, management expectations, or structural constraints that are perceived as preventing that work system or its participants from achieving a desired level of efficiency, effectiveness, or other organizational or personal goals*" [2]. Therefore, a workaround is used to overcome an aspect of a system that they perceive to be a constraint or an obstruction to the workflow.

Patterson [12] adds to this definition stating that when policies and procedures are designed, procedures are '*work as imagined*' by management versus '*work as done*', which refers to the actual procedures performed by the employees. A further definition suggested by Kobayash *et* al. [9] states that workarounds are "*temporary, informal procedures implemented by employees to overcome workflow bottlenecks*". Workarounds are often utilised to overcome technical malfunctions or perceived inefficient procedures. This is influenced directly by an employee's decision-making strategy and tacit technical knowledge which may be determined by their personal goals, the organisation's operational goals or their motivation to undermine working systems.

Workarounds are viewed as non-conformant and resistant behaviour [3]. They exist throughout all industries and are typically implemented in situations where a procedure may seem inefficient or inadequate by the employee expected to implement an organisation's procedures. Workarounds may develop as innovations, as well as a form of resistance to policies and procedures [8].

Section 4 highlights the main factors that influence employees' use of workarounds.

4 Factors that Influence Workarounds

Workarounds are products of their environments, the employees who exist within them, and the influences that these employees are exposed to. The factors influencing workarounds can therefore be categorised according to the employees and their decision-making processes [11, 3].

4.1 The Employee Decision-Making Process

All people are unique and are responsible for varying decisions when considering information security related actions. Many behavioral theories and models exist relating to information security behaviour, such as the Theory of Planned Behaviour [1], the Information Security Competency Model [18] and Agency Theory [17]. However, the Protection Motivation Theory will be used as it considers the Threat Appraisal that a person may use when deciding to use a workaround. The Protection Motivation Theory, which relies on a person's threat appraisal and coping appraisal, could provide an explanation for an employee's decision to use a workaround in a specific environment.

Within the context of an organisation, threat appraisal is an employee's perception of environmental threats within the organisation.

Threat appraisal consists of *Perceived Vulnerability* and *Perceieved Severity*. *Perceived Vulnerability* is an employee's perception of the validity of the threats. *Perceived Severity* is the perception of the consequences of the threats being realised [12].

Coping appraisal consists of *Self-efficacy*, *Response Cost* and *Response Efficacy*. *Self-efficacy* is described as an employee's drive to implement procedures that would keep them safe and their belief in their ability to execute those procedures. Habits and personal biases towards activities, for example, may influence an employee's perception of *Self-efficacy*. *Response Cost* is the cost that the employee perceives from the implementation of a prescribed procedure, which may include related consequences for non compliance. Lastly, *Response Efficacy* relates to the employee's perception of how effective a procedure might be in their environment [12]. The Protection Motivation Theory is shown in Figure 2.

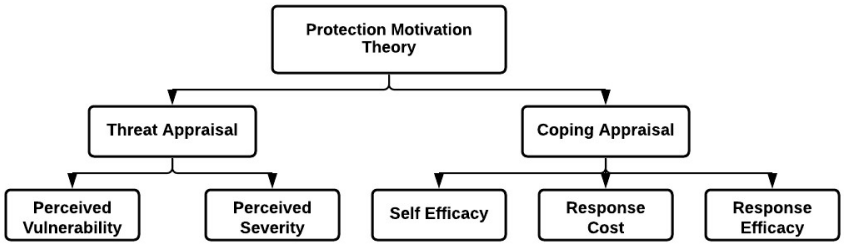

Fig. 2. Protection Motivation Theory [11]

Within the context of information security, employees would employ both threat appraisal and coping appraisal when deciding whether the procedures recommended by the information security policy are efficient and should be employed or not [7].

4.2 Environmental Factors

An organisation represents an environment within which various work activities and procedures exist. The employees of an organisation exist within this environment and their behaviour is influenced by this organisational environment [3].

Lalley and Malloch [11] present four environmental factors that may influence the need for workarounds, namely:

- **Block in Workflow:** These are hinderances to an employee's ability to work.
- **Additional Work Demands**: These may lead an employee to look for shortcuts to lighten their workload.
- **Poor System Design:** This influences the need for workarounds to overcome existing deficiencies.

- **Incompatible Policies:** These are policies that are incompatible with safety and system limitations.

These environmental factors may result in an employee considering the perceived information security vulnerability and perceived severity of threat to an information asset to be low enough to use a workaround. Furthermore, an employee lacking the *Self Efficacy* to execute information security procedures may use their own procedure, which may introduce risk. A lack of *Response Cost* in the form of consequences may also be a missing deterrent for utilising a workaround, resulting in non-conformance with the organisation's information security policies. The employee's *Response Efficacy* may also deem the risk from their workaround to be worth the benefit in efficiency gained. This all culminates in an employee utilising a workaround to meet their personal, perceived needs. The next section discusses Alter's [2] Theory of Workarounds, which provides a solid grounding in helping organisations understand employees' use of workarounds.

5 Alter's Theory of Workarounds

Alter's [2] Theory of Workarounds consists of seven steps associated with the use of workarounds. The original reasoning behind the Theory of Workarounds was to explain the use of workarounds to circumvent organisational processes. Table 1 presents these seven steps leading up to, during and upon utilisation of the workaround. Steps 1, 2 and 3 relate to the environmental factors and human decision-making process that may influence the use of a workaround. Steps 4, 5 and 6 focus on the workaround creation and utilisation, while Step 7 considers the consequences of such workarounds [2].

Table 1. Steps in the Theory of Workarounds [2]

No.	Steps	Explanation
1	**Intentions, Goals, and Interest**	Understanding the goals of management is important for policy designers to create the procedures employees are expected to meet and the procedures to follow.
2	**Structure**	The structure of policies and procedures, how they are designed, and the performance goals reward systems used, all influence the behaviour of those expected to comply with the procedures.
3	**Perceived need for workaround**	This step is based on the performance goals of procedures, systems structure, constraints, as well as employee goals.

4	**Identification of possible workarounds**	This step is triggered by the perceived need for a work-around. Employees consider costs, benefits, and risks when obstacles are encountered, and they perceive a need for a workaround.
5	**Selection of workaround to pursue, if any**	In this step employees decide on the most appropriate workaround, if any, to utilise to overcome the perceived obstacle in their workflow.
6	**Development and execution of the worka-round**	This step can occur over a short to long period of time depending on the complexity of the situation presented to the employee.
7	**Local conse-quences and broader con-sequences**	A workaround may yield local and broader conse-quences in its utilisation. These consequences may be either positive or negative depending on the risk intro-duced by the workaround.

Figure 3 is a representation of the seven steps in Alter's [2] Theory of Workarounds - the number of each step is indicated in brackets. Figure 3 aims to show the *Work as Imagined* expectations of management and the designers of the policies and procedures (Steps 1 and 2). Next is the constraint or *Obstruction to Workflow* that may occur in a day-to-day work environment. At this point, an employee may or may not perceive the need for a workaround (Step 3). If an employee perceives no need for a workaround, work continues, and the *Expected Work Output* is achieved. However, if an employee perceives that there is a need for a workaround, the employee will then decide what type of workaround to utilise (Step 4). It is possible at this point, that an appropriate workaround does not exist or is not possible to execute and the employee would not be able to utilise a workaround. If, however, a workaround can be used and is decided upon (Step 5), the employee moves to the implementation of the workaround (Step 6). Upon implementation of the workaround, the local and broader consequences (Step 7) may be realised. It must be noted that *Work as Done* may not always equate to the *Work as Imagined*, as envisaged by management in Steps 1 and 2.

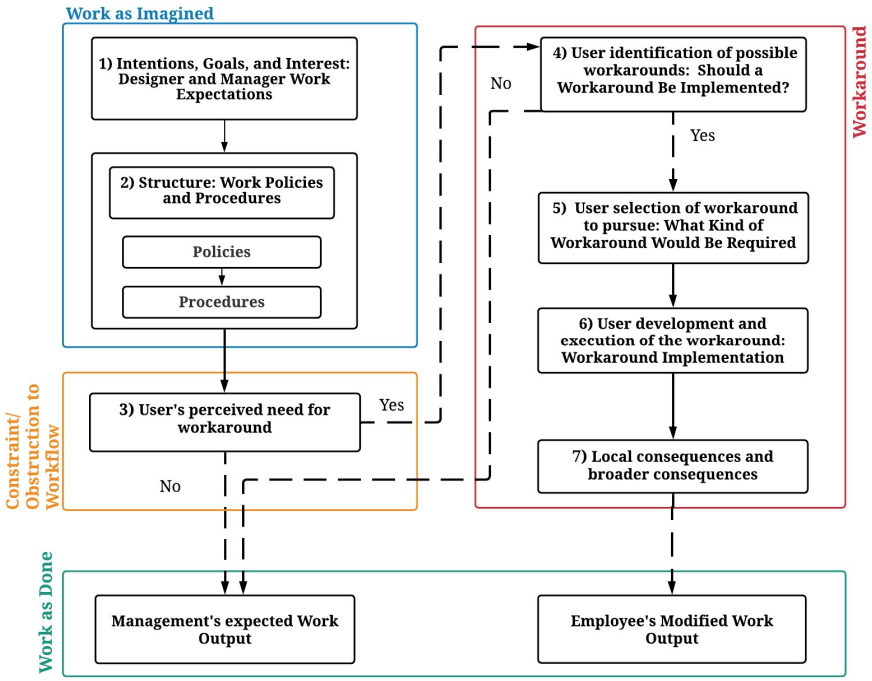

Fig. 3. An employee's decision-making process to utilise workarounds

A hypothetical example takes place in Hospital AB, where a formal information security policy has been implemented and sufficiently supported. A workaround is performed daily in the reception area of Hospital AB, throughout the day and the employees interacts with information assets in the form of employee records and patient information. The information security policy specifies that employees should log out of their account when they are no longer at the computer. The workaround, in this example, allows for employees to remain logged in even when they are not there, as will be discussed in more detail below. Using Alter's [2] Theory of Workarounds as a guide, the decision-making process as to why an employee at Hospital AB may perceive a workaround as necessary can be understood:

- **Step 1** simply aims to add context, the employee is expected to conform with the information security policy of Hospital AB, represented as the Acceptable Use Policy (AUP).
- **Step 2** indicates the work procedure within the AUP that states that employees should log out of their work account when not at their workstation, as an information security best practice, in Hospital AB. A backup automated logout system is implemented to log employees out after 10 idle minutes on the workstation.

- **Step 3** presents an opportunity for a *Block in Workflow* to occur. In this case, logging out and then having to log back into their work account is perceived by employees to take up a lot of time and may be viewed as tedious by the employees. For employees who do not perceive this requirement as being tedious, their work continues as normal and the employee logs in and out as required.
- **Step 4** occurs when an employee finds the logging in and out to be tedious or counterproductive to their workflow and seeks an alternative. The Protection Motivation Theory (Figure 2) can be used to theorise the outcome of the decision. In this example, the threat appraisal of the employee considered the vulnerability of an unlocked computer as low, as well as a low severity if there were to be some type of associated breach. With regards to coping appraisal, an employee may be confident in their *Self-efficacy* for relogging onto their work account but may see more benefit in not complying. The *Response Cost* of not complying with the procedure may be high, as consequences are outlined in the AUP, but the employee may either not be aware of the AUP, and its contents, or may regard the workaround as more beneficial to them than following the correct procedure. Lastly, considering *Response Efficacy*, the employee does not feel that logging out of their account may result in a more significant information security risk than what they could possibly gain back in time when it comes to treating patients. In this example, the employee ultimately chooses to utilise the identified workaround.
- **Step 5** occurs when the workaround is chosen, and the employee decides that defeating the automatic logout system will be most effective. The employee does not log out of the workstation as this introduces too much delay into their work.
- **Step 6** is the actual utilisation of the workaround. The employee asks a co-worker to tap their computer's spacebar before the 10-minute automatic logout has occurred, which would keep them logged in for longer periods of time. The computers, while still logged in, may be left unattended for a period of time.
- **Step 7** occurs when the employee has completed their work and logs out at the end of the day. The employee has 'got the job done' but has used a workaround of information security procedures to achieve their goals. The risk introduced in this example is that leaving a logged-in computer unattended may give unauthorised access to patient information to someone who would not have had access if the correct procedure was followed.

A workaround is often viewed by employees as a necessity for quick reactions when changes occur in dynamic work environments or there are hinderances to the expected workflow [14]. When employees use workarounds, they may inadvertently introduce information security risk into the organisation. These workarounds need to be documented, understood and their risk assessed. Low risk workarounds should be viewed as an opportunity to improve existing information security policies and procedures. These workarounds are good candidates to incorporate into information security policies and procedures, as they are low risk and reflect what employees are doing. Medium to high risk workarounds, however, should be incorporated as examples of unacceptable behaviour and the related consequences clearly outlined.

Ultimately, workarounds need to be identified, assessed, and eradicated through their assimilation into the information security policies and procedures, either as adaptations of existing procedures or as unacceptable behaviour.

6 Workaround Classification and Risk Assessment

As discussed, a risk assessment of information security workarounds is needed to determine the risk employees may be introducing by not conforming to information security policies and procedures. Before a risk assessment for workarounds can be conducted, however, identification of the workarounds must occur. Information security workarounds may be identified through observation, reporting or in the aftermath of a security breach.

Burns *et al.*. [5] present a workaround assessment method to be used by management to classify workarounds. Used together with the workaround descriptors of Friedman *et al*. [6], Burns *et al.* suggest both the classification and descriptions of workarounds as follows:

Workaround General Classifications:

- **Harmless:** These workarounds generally tend to be user-made procedures that allow for missing system features to be substituted by an employee's own creativity. These workarounds are generally *good*.
- **Essential:** The essential workaround is a user-made procedure that is used to accomplish *Work as Done* as close to imagined as possible. This is generally a *good* workaround.
- **Hinderance:** This serves the purpose of overcoming any procedures or work activities that employees may deem too difficult or time consuming. This workaround could be deemed *good* or *bad*, depending on the context.

Workaround General Descriptors:

- **Temporary/Routinised:** *Temporary* workarounds are short term solutions, whereas *routinised* workarounds are part of day-to-day routines. A *temporary* workaround example is an employee opening a secured door for another employee that left their key card at home, once. A *routinised* workaround is that staff member opening the secured door for the other staff member every day.
- **Avoidable/Unavoidable:** The *avoidable* workaround is a workaround that could have been solved with an acceptable solution. *Unavoidable* workarounds happen when an external force creates a situation that requires a workaround for continuation of work. An *avoidable* workaround example is when an employee introduces a workaround to save time on a task by skipping a few steps. An *unavoidable* workaround is where an employee needs to skip over steps in their work process as their capturing program is not functioning correctly and their job has a time requirement.
- **Deliberate/Unplanned:** *Deliberate* workarounds are purposefully put into place to address the limitations of existing systems or a deliberate act of non-compliance such as a malicious action. *Unplanned* workarounds tend to occur dynamically based on

the tasks needing to be accomplished. A *deliberate* workaround is like an avoidable workaround; however, the intent is the major difference. A *deliberate* workaround example can be a workaround implemented maliciously by an employee such as leaving secured doors open as that employee may find the keypad system to be a nuisance or out of spite for their employers. An *unplanned* workaround example is when an employee notices a system does not have the functionality they require in that moment, and they take physical notes instead of recording the information on the computer program as prescribed.

These workaround classifications and descriptors are shown in a matrix format in Table 2. In the example used in Hospital AB, the workaround is performed due to the perceived inconvenience of repeatedly logging in and out of computers when not in use. Therefore, the *Hinderance* row will be selected to classify the workaround. Next, the workaround descriptors are addressed. In the Hospital AB example, the workaround is performed daily which leads to it being *Routinised*. The workaround is very much *Avoidable*, as it is not caused by an unexpected event. Finally, the workaround is *Deliberate*, as the employees have arranged to reset all the login timers whenever each of them enter the office.

Table 2. Workaround Classification Matrix

	Temporary or Routinised	**Avoidable or Unavoidable**	**Deliberate or Unplanned**
Harmless			
Essential			
Hinderance	*Routinised*	*Avoidable*	*Deliberate*

While Table 2 categorises and describes a workaround, the potential risk introduced by a workaround is not taken into consideration at all and no objective way of determining the risk of a workaround is provided. Furthermore, another disadvantage of using this workaround classification method is that there is no final, singular output, it merely aims to classify the workaround.

Using the ISO27005 standard [16] as a guideline, a risk assessment matrix can be used for assessing the potential risk incurred through the utilisation of workarounds. The *Risk Assessment Matrix for Information Security Workarounds* requires the selection of three workaround aspects:

- *Frequency of Workaround Utilisation* is how often a particular workaround is utilised by employees.
- *Workaround Vulnerability* refers to the information security vulnerability that the workaround introduces to the associated assets. *Asset Impact Value* is determined by the cost of an information security breach being realised for a specific information asset [14]. The asset value is relative to an organisation.

Based on the risk assessment matrix in ISO27005 [16], Table 3 presents the *Risk Assessment Matrix for Information Security Workarounds*. *Frequency of Workaround Utilisation* is the rate at which workarounds are implemented, *Low* being a once off, *Medium* being occasionally and if part of a daily routine, the frequency is *High.* The *Perceived Workaround Vulnerability* is determined by accounting for the vulnerability of the asset using the level of security considered when implementing the workaround. *Asset Impact Value* is determined by considering the intangible, relative impact cost of a threat being realised.

Table 3. Risk Assessment Matrix for Information Security Workarounds

		Frequency of Workaround Utilisation								
		Low (L)			**Medium (M)**			**High (H)**		
		Perceived Workaround Vulnerability			**Perceived Workaround Vulnerability**			**Perceived Workaround Vulnerability**		
		L	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Asset Impact Value	0 - Negligible	0	1	2	1	2	3	2	3	4
	1 - Low	1	2	3	2	3	4	3	4	5
	2 - Medium	2	3	4	3	4	5	4	5	6
	3 - High	3	4	5	4	5	6	5	6	7
	4 – Very High	4	5	6	5	6	7	6	7	8

When using the Risk Assessment Matrix for Information Security Workarounds to assess the risk of the workaround used in Hospital AB, the Frequency of Workarounds Utilisation, the Workaround Vulnerability, as well as the Asset Impact Value must be determined by information security officers. In the workaround identified in the Hospital AB example, the Frequency of Workaround Utilisation is High, as the workaround is used in day-to-day operations. The Perceived Workaround Vulnerability in the example is determined to be Medium. While there may be technical measures in place to protect the patient information, the computers in question are located in the reception area of the hospital and are easily accessible. If no employees are present in the reception area and the computers are left logged in, nobody would be aware of unauthorised access, as security cameras are not monitored live. The Asset Impact Value in the example is determined to be Very High, as the information assets are patient records. Therefore, in the Hospital AB example, the result from the Risk Assessment Matrix for Information Security Workarounds is 7.

Once a resultant value has been calculated through the *Risk Assessment Matrix*, it can be referenced to the *Information Security Workaround Risk Index*, shown in Table 4, to determine the final risk level. In the Hospital AB example, the calculated value from the *Risk Assessment Matrix* is 7. Therefore, the Information Security Risk Index for the workaround example is determined to be *High*. The *Risk Assessment Matrix for Information Security Workarounds* can play an important role in identifying the risk exposure that a workaround may introduce in an organisation.

Table 4. Information Security Workaround Risk Index

Information Security Workaround Risk Value	
0-2	Low
3-5	Medium
6-8	High

Using the proposed *Risk Assessment Matrix for Information Security Workarounds* and the *Workaround Risk Index*, the risk associated with identified workarounds can be identified and appropriate action taken. Medium to high risk workarounds should be explicitly identified in information security policies and procedures as unacceptable behaviour, and the resultant consequences detailed. Low risk workarounds should be considered for incorporation into the information security policies and procedures by adapting the relevant procedures to reflect the way employees are actually working.

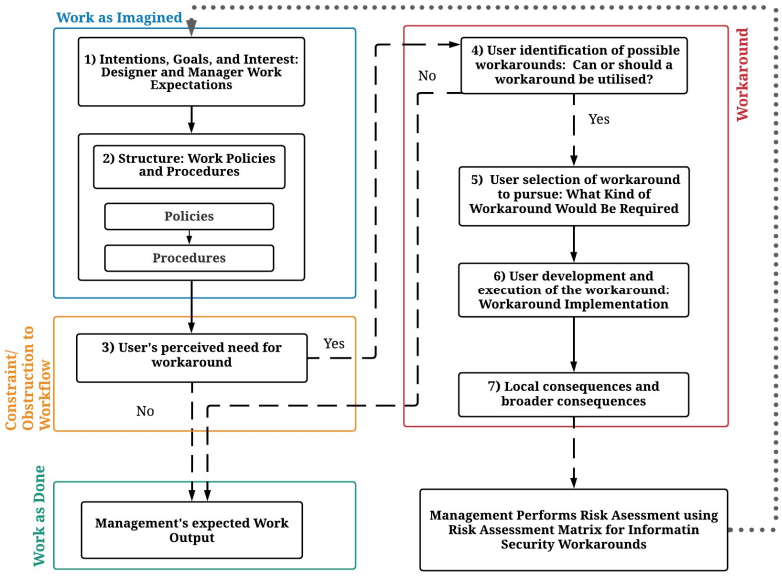

Fig. 4. An employee's decision-making process to utilise workarounds accounting for the risk assessment process.

Therefore, as seen in Figure 4, identified workarounds should be assessed for risk according to the *Risk Assessment Matrix for Information Security Workarounds*. The results of the Matrix should provide information security officers with the risk level associated with a workaround. Depending on the identified risk levels, information security workarounds should be addressed through the appropriate actions of *Risk Modification*, *Risk Retention, Risk Avoidance, Risk Sharing* or *Risk Acceptance*. Through these actions, the information security risk introduced through workarounds should be

'treated' and result in workarounds being incorporated into information security policies, either as 'acceptable' or 'unacceptable' behaviour.

7 Conclusion

This paper proposes an objective *Risk Assessment Matrix for Information Security Workarounds* by assigning a *Frequency of Workaround Utilisation*, *Perceived Workaround Vulnerability*, and *Asset Impact Value* to an identified workaround. Risk assessment using the proposed *Risk Assessment Matrix for Information Security Workarounds* allows for understanding risk exposure of a workaround. The *Information Security Workaround Risk Index* then allows an associated risk value to be determined by comparing the *Risk Assessment Matrix for Information Security Workarounds* output to the *Information Security Workaround Risk Index*.

Using the *Risk Assessment Matrix for Information Security Workarounds* and the *Information Security Workaround Risk Index*, the *low risk* and *medium to high risk* workarounds can be distinguished. *Low risk* workarounds could be used to update and improve the existing policies and procedures. *Medium to high risk* workarounds could be used as examples of misuse and unacceptable use for future policy and procedure revisions.

Future research opportunities exist in researching the information security risk workarounds within various industries, as well as investigating the challenges of workaround identification.

8 References

1. Ajzen, I. (2012). The theory of planned behavior. *Handbook of Theories of Social Psychology: Volume 1*, 438–459. https://doi.org/10.4135/9781446249215.n22
2. Alter S (2014) Theory of workarounds. Commun Assoc Inf Syst 34(1):1041–1066. https://doi.org/10.17705/1cais.03455
3. Bagayogo F, Beaudry A, Lapointe L (2013) Impacts of IT acceptance and resistance behaviors: A novel framework. Int Conf Inf Syst (ICIS 2013) Reshaping Soc Through Inf Syst Des 3:2077–2095
4. Beautement A, Sasse MA, Wonham M (2009) The compliance budget: Managing security behaviour in organisations. Proc New Secur Paradig Work :47–58. https://doi.org/10.1145/1595676.1595684
5. Burns AJ, Young J, Roberts T, Courtney J, Ellis TS (2015) Exploring the Role of Contextual Integrity in Electronic Medical Record (EMR) System Workaround Decisions: An Information Security and Privacy Perspective. AIS Trans Human-Computer Interact 7(3):142–165. https://doi.org/10.17705/1thci.00070
6. Friedman, A. *et al.* (2014) 'A typology of electronic health record workarounds in small-to-medium size primary care practices', *Journal of the American Medical Informatics Association*, 21(E2). doi: 10.1136/amiajnl-2013-001686.

7. Ifinedo P (2012) Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput Secur 31(1):83–95. https://doi.org/10.1016/j.cose.2011.10.007
8. Ignatiadis I, Nandhakumar J (2009) The Effect of ERP System Workarounds on Organizational Control: An Interpretivist Case Study. Scand J Inf Syst 21(2):59–90
9. Kobayash M, Fussell SR, Xiao Y, Seagull FJ (2005) Work coordination, workflow, and workarounds in a medical context. Conf Hum Factors Comput Syst - Proc :1561–1564. https://doi.org/10.1145/1056808.1056966
10. Koppel R, Smith S, Blythe J, Kothari V (2015) Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient? Stud Health Technol Inform 208:215–220. https://doi.org/10.3233/978-1-61499-488-6-215
11. Lalley C, Malloch K (2010) Workarounds: The hidden pathway to excellence. Nurse Lead 8(4):29–32. https://doi.org/10.1016/j.mnl.2010.05.009
12. Maddux JE, Rogers RW (1983) Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. J Exp Soc Psychol 19(5):469–479. https://doi.org/10.1016/0022-1031(83)90023-9
13. Patterson ES (2018) Workarounds to Intended Use of Health Information Technology: A Narrative Review of the Human Factors Engineering Literature. Hum Factors 60(3):281–292. https://doi.org/10.1177/0018720818762546
14. Röder N, Wiesche M, Schermann M, Krcmar H (2014) Why managers tolerate workarounds - The role of information systems. 20th Am Conf Inf Syst AMCIS 2014 (2008):1–13
15. Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information and Computer Security*, *28*(3), 467–483. https://doi.org/10.1108/ICS-01-2019-0010
16. ISO/IEC (2011) ISO/IEC 27005: 2012 International Organization for Standardization— Information technology — Security techniques — Information security risk management, International Organization for Standardization
17. Shapiro, S. P. (2005). Agency theory. *Annual Review of Sociology*, *31*, 263–284. https://doi.org/10.1146/annurev.soc.31.041304.122159
18. Thomson, K. L., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud and Security*, *2006*(5), 11–15. https://doi.org/10.1016/S1361-3723(06)70356-6