THE EFFECTIVENESS OF ELECTRONIC RISK MANAGEMENT SYSTEM (ERMS): A STUDY IN A MALAYSIAN HIGHER LEARNING INSTITUTION

Khalid Abdul Wahid[1,*], Marziana Madah Marzuki[2], Mohamad Rahimi Mohamad Rosman[3], and Mohd. Zafian Mohd. Zawawi[4]

Abstract

The risk management process has been identified as a mechanism to help organizations proactively manage and monitor the risk associated with the organization's strategic objectives. Nevertheless, implementation of the risk management process in Universiti Teknologi MARA (UiTM), Malaysia, has become an issue as it has been highlighted that there is ineffective communication among all parties involved in the process. The finding shows that the existing risk management system causes a delay in action, it is tedious, costly, and leads to less monitoring. The purposes of this study are to identify problems in the risk management process practiced by Universiti Teknologi MARA (UiTM) in Malaysia and to compare the effectiveness of two systems. A new electronic risk management system was implemented after identifying problems in the current system. In order to make a comparison, data were collected from 95 respondents, consisting of risk management coordinators, and unit heads of faculties or departments. The results showed that the problems of the existing system are that it is not user-friendly, it is complicated to use, and time-consuming for actions to be taken. A paired-sample T-test was used for the data analysis. The results showed that there was a significant difference between the current system and the new proposed system in terms of perceived usefulness, perceived ease of use, trust, personal initiatives and characteristics, context, and system effectiveness.

Keywords: Risk, Risk management process, Electronic risk management system, Technology acceptance model (TAM)

1. Introduction

The increasing volatility and competition that organizations must face in this era has forced them to implement risk awareness. Due to notorious international scandals such as the Enron case, WorldCom, and more recently Lehman Brothers, organizations in general, are facing new legal requirements enforced by authorities and regulators, who

[1,*] Dr. Khalid Abdul Wahid is currently working as a senior lecturer in the department of Information System Management, Faculty of Information Management, Universiti Teknologi MARA, Kelantan branch, Malaysia. He obtained a Ph.D. in Business Administration from Kasetsart University, Thailand. Email: awkhalid@uitm.edu.my

[2] Assoc. Prof. Dr Marziana Madah Marzuki is currently working as Associate Professor in Faculty of Accountancy in Universiti Teknologi MARA, Kelantan branch, Malaysia. She obtained a Ph.D. degree in Financial Reporting and Corporate Governance from Universiti Sains Malaysia.

[3]Dr. Mohamad Rahimi Mohamad Rosman is currently working as a senior lecturer in the department of Information System Management, Faculty of Information Management, Universiti Teknologi MARA, Kelantan Branch, Malaysia. He obtained a Ph.D. in Information Management from Universiti Teknologi MARA, Malaysia.

[4]Mohd. Zafian Mohd. Zawawi is currently working as a senior lecturer in the department of Information System Management, Faculty of Information Management, Universiti Teknologi MARA, Kelantan branch, Malaysia. He obtained a master degree's in Information Management from Universiti Teknologi MARA, Malaysia.

are demanding the implementation of increasingly more sophisticated risk management practices. Technological advancement has helped organizations to become more efficient but has also exposed them to significant new threats which differ from threats faced in the past. Thus, the adoption of good risk disclosure practices by organizations can provide insights for investors and other stakeholders in assessing the organization's quality and the prospective volatility of the organization's earnings and cash flows.

The risk management process should have at least five stages, namely determining objectives, identifying risks, evaluating risks, considering alternatives, selecting risk treatment devices, and implementation and review (Van Staveren, 2009). Nevertheless, despite a comprehensive theoretical framework of the risk management process, implementation of the process has been criticized in previous research, stating that it carries little benefit for such firms and their stakeholders. This is due to a lack of effective communication among the parties concerned, ranging from those who describe the risks that affect the firm's strategies, to those who take action on leveraging emerging risk opportunities and minimizing the risk of failures (Beretta & Bozzolan, 2004; Togok, Isa & Zainuddin, 2016).

Higher learning institutions are similar to other business firms, in that they are required to deal with strategic, operational, financial, compliance, and reputational risks (Sabri, 2011). According to the Higher Education Funding Council for England (HEFCE), the risks faced by higher learning institutions become threats that affect the institution's ability to achieve its objectives (Perera, Rahmat, Khatibi & Azam, 2020). The purpose of risk management in higher learning institutions is to achieve institutional objectives and reduce damage to the institutions. There are 20 public universities and 443 private universities and colleges in Malaysia.

Universiti Teknologi MARA is one of the public universities, established in 1956. It is the biggest university in Malaysia, consisting of 13 state campuses and 21 satellite campuses throughout the country. There are 24 faculties, accomodating a total of 160,957 students and 500 programs. It is expected that the risk management system should be an integrated system which effectively monitors the risk from all campuses. However, the risk management system employed in UiTM is ineffective in handling reported risks reported in a timely manner, especially regarding risks on specific branch campuses. Therefore, the objectives of this study are to identify the problems of the risk management process practiced in Universiti Teknologi MARA, Malaysia, and to experimentally compare the effectiveness between the current system and the new electronic risk management system (ERMS).

2. Literature Review

2.1 Risk Management

Risk management refers to decisions made under conditions of known probabilities (Knight, 1921). Risk is the combination of the probability of an event and its consequences (Kaplan & Garrick 1981; Kaplan 1991, ISO, 2002). Nevertheless, the dictionary definition of this term relates risk to the chance of injury, damage, or loss (Webster, 1983). Previous research has equalized risk with expected disutility (Campbell, 2005) and expected loss (Willis, 2007). Many researchers also relate risk with the probability of an adverse outcome (Graham & Weiner, 1995) and the severity of adverse effects (Lowrance, 1976). Technically risk can be defined as the cause of, or the probability of, an unwanted event that may or may not occur, where something of human value (including humans themselves) is at stake (IRGC, 2005) and where the outcome is uncertain (Rosa, 2003). Thus, risks are probabilities that are more related to unfavorable rather than favorable effects.

Consequently, organizations should proactively manage risk, monitoring in a continuous and conscious way, the risks associated with their strategic objectives. Risk must be monitored in order to maintain an overall risk profile aligned with the strategic objectives of an organization (Van Staveren 2009). The

management of risk is therefore an integral part of the organization management, allowing for the understanding of potential upside and downside factors that can affect the organization. The main objective of risk management is to develop understanding in advance, concerning the impacts of each risk and their alternative solutions, in relation to the future performance of the organization (Hopkin 2002).

2.2 Risk Management Process

According to Van Staveren (2009), the risk management process (Figure 1) is not a one-time activity, but rather an ongoing process of identification, assessment, and action, which must be well integrated into every part of the organization. Effective risk management involves taking a holistic approach to risk, developing a risk management policy, establishing clear accountabilities and responsibilities, balancing risk exposure against controls, being open about risks to reduce conflicts and information hiding, enforcing risk management practices, and learning what works and what does not from past experience (Smith, McKeen & Staples, 2001).

The objectives of a risk management program should therefore be formalized in a "corporate organizational risk management policy". In order to formalize risk management as an organizational policy, the first step of the risk management process is to understand the objectives and importance of the fraud risk management process. With the increase in volatility and competition among organizations, managers have been forced to implement at least some level of risk awareness. In addition, the legal requirements enforced by authorities and regulators have demanded the implementation of increasingly more sophisticated risk management practices. Current technology has also exposed organizations to different sorts of significant new threats which create new risks and increase the impact and frequency of existing risks. Therefore, risk management is a process that allows organizations to balance the operational and economic costs of protective measures and achieve gains in supporting the organization's mission. This process is not unique to the business environment but indeed pervades decision-making in all areas of daily lives (Stoneburner, Goguen & Feringa 2002).

The second step of a standard risk management process is related to the identification of the risks that the organization might face. The identification stage is normally performed by using several instruments such as the internal records of the organization, an insurance policy checklist, risk analysis questionnaires, flow process charts, analysis of financial statements, inspection of the firm's operations, and interviews, among others (Vaughan, 1997). The third step which is the evaluation step involves measuring the potential size of the loss and the probability that it will actually occur, providing some ranking that classifies the risks in order of priority. As a consequence, the evaluation step provides critical information that can determine the attention that the organization requires in considering certain risks.

The fourth step in the risk management process is to do with the techniques or strategies that are used in dealing with each risk. The basic strategies frequently discussed in the literature are avoidance, reduction, retention, and transfer. Therefore it is interesting to appreciate that this phase of the risk management process is primarily a problem in decision making, where the organization must decide among various types of risk management strategy (Cienfuegos, 2012). In the next step, the implemention stage, decisions that were established in the previous phase must be implemented. The final step of the process of risk management involves evaluating and reviewing the risk management program, and establishing check and balance procedures in order to make sure that the objectives of the risk management program are accomplished.

Figure 1 Risk Management Process

2.3 Risk Management System in Universiti Teknologi MARA (UiTM)

UiTM has 13 branch campuses and 21 satellite campuses distributed throughout Malaysia. It has appointed coordinators of risk management for each branch campus who are led by the head of risk management on the main campus in Shah Alam. The head of risk management supervises and monitors all risk management processes in all branches. In higher learning institutions, the main organizational objectives are to enhance the knowledge and expertise of students in all fields of study through continuous improvement efforts in the various programs offered, research work, and community service, based on moral values and professional ethics. Among the main departments that exist in the institution are academic affairs, student affairs, research and industrial linkages, finance, library, administration, and facilities departments. Some of these departments are divided into several centers with units of specific functions which ensure the organizational objectives can be well achieved and successful. Recently, each higher learning institution has been required to establish a risk management department that will coordinate the risks identified within the organizations. This unit monitors and ensures that identified risks can be eliminated, reduced, or transferred, to ensure the effectiveness of the organization.

In this university, the risk management process is done manually. Risks are identified and evaluated by the head of the department/supervisor as they are involved directly with their department's strategic objectives and control of operations in the department. Figure 2 shows the risk management form used by the departments in the organization to identify, evaluate, and control risks. Based on the risks identified in column 2, the evaluation of its severity in column 4 is done by multiplying its probability (column 5) and its impact (column 6) depending on the type of risk. Based on the level of its severity (column 7), the head of department will identify the controlled action that has been taken (column 8) suggesting preventive action that is expected to reduce the severity of the risk (column 9). Column 10 identifies the person who identified or registered the risk, which is the respective head of department. Meanwhile column 11 identifies the person responsible for the suggested preventive action. It should be reminded that the person who registered the risk and the person responsible for the action taken might be a different person. All columns will be filled in by the head of department. The form will then be submitted to the risk management coordinator for further checking to ensure that the risks that have been identified are well-evaluated.

The coordinators in the risk management office will monitor the risk management process, ensuring that especially severe risks are identified, regularly monitored, and that action is taken to reduce the risk to a lower level. This monitoring process is done by holding

Department: Academic Affairs

Risk Register Form

Risk Identification			Risk Evaluation				Risk Controlling				Risk Monitoring		
Risk category	Risk explanation	Risk Causes	Impact of Risk	Probability of Risk	Level of Risk Impact	Risk Severity	Existing Preventive Action	Suggested Preventive Action	Risk Owner	Responsible Department /Unit	Date registered	Date Updated	Risk Status
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
Operational Risk/Reputational Risk		High failure rate on critical courses	Need greater allocation of class facilities i.e college/fail to achieve universities' key performance indicator such as GOT (Graduate on Time)	4	3	12	Students' counselling	Students' Advisor Programme Additional hours of teaching for critical courses	Academic Affairs Department	Academic Affairs Department	01/01/18	31/06/18	Failure rate has been reduced. GOT percentage increase to 90%. Achive the organizational quality objective (level of risk reduced)

Figure 2: Sample of Risk Register Form in UiTM

regular meetings to discuss prevailing risk and the effectiveness of the preventive actions suggested by the head of the department. Usually, in the first meeting, the risk management coordinator will highlight all the risks identified, with special attention given to severe risks. Severe risks will be monitored regularly. Since the maximum number of meetings held in the university for this purpose is four times annually, severe risks will be discussed and monitored every three months. For any severe risk that can not be prevented at the branch level, new preventive action will be suggested or the issue will be raised to the Risk Management Council for further action. Low and moderate risks are usually audited and monitored every six months to ensure that preventive action is being taken and is effective. Figure 3 illustrates the flow of the risk management process in UiTM.

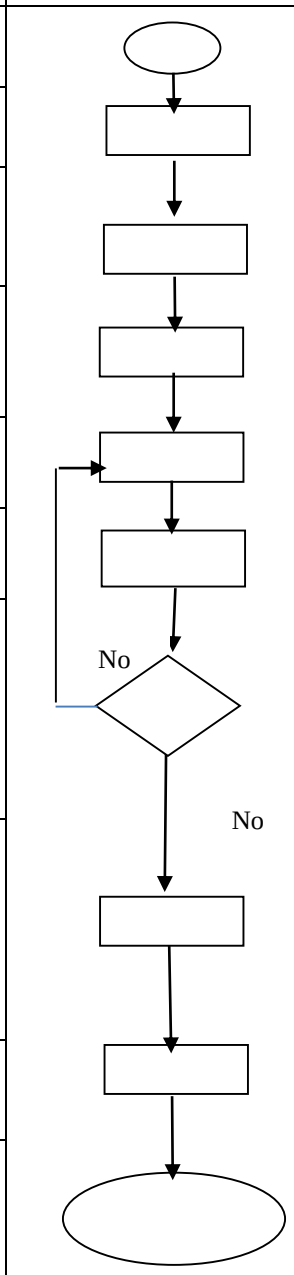
Person in charge	Flow of Risk Management Process	Activities	Forms
		Start	
Head of Department		Identify risks	Risk Register Form
Head of Department		Determine type of risks and risk casues	Risk Register Form
Head of Department		Evaluate Risk Level by multiplying probability of risk to happen with the impact of risk.	Risk Register Form
Head of Department		Determine preventive action	Risk Register Form
Responsible Department		Implement the preventive action	
Head of Department/ Risk Management Coordinator		Does the preventive action taken effective or not? Evaluate the effectiveness of preventive action taken and update the status of its implementation and effectiveness	Risk Register Form
Risk Management Coordinator		Prepare Preventive Action Report (whether solved or not) to the Head of Risk Management & Risk Management Council Any unsolved issue will be raised to Risk Management Council	Preventive Action Report
Risk Management Coordinator		Presenting the Report	Preventive Action Report
		End	

Figure 3: Flow of Risk Management Process in UiTM

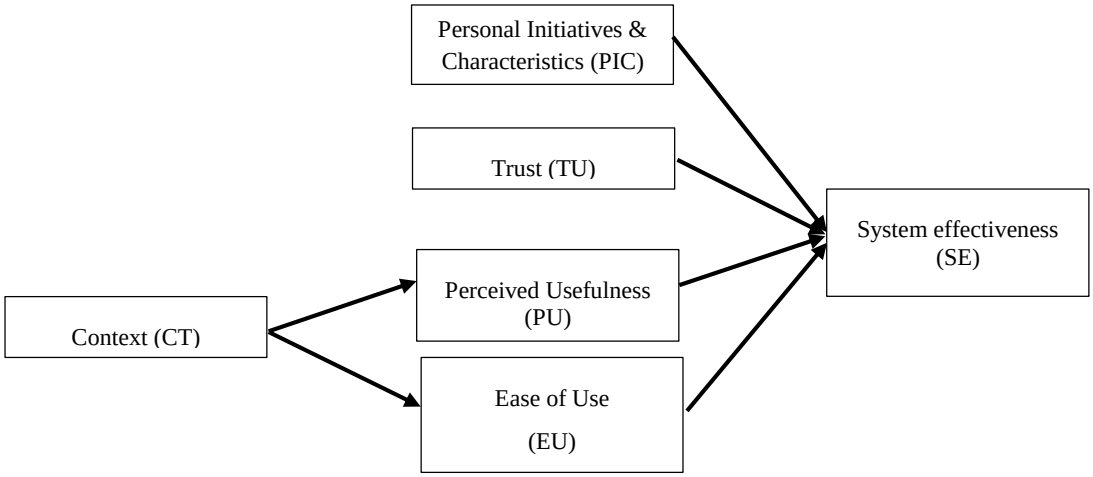


Figure 4: The Electronic Risk Management Model (ERMM)

2.4 Technology Acceptance Model (TAM)

Several models have been developed to test users' adoption of new technologies. These models include the Technology Acceptance Model (TAM) (Davis, 1989), Theory of Planned Behavior (TPB) (Ajzen, 1991), and Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis & Davis, 2003). Among the different models, TAM appears to be one of the most accepted. E-business has been tested using TAM in some studies. The model has proven to be quite reliable to predict user acceptance of new information technologies (Horton, Buck, Waterson. & Clegg, 2001; Lederer, Maupin, Sena & Zhuang, 1976; Gefen, 2003).

There are two primary constructs in TAM, perceived usefulness (PU) and perceived ease of use (PEU), which determine users' adoption of a new technology or information system. Perceived usefulness refers to the degree to which a person believes that using a particular system would enhance his or her job performance (Davis, 1989). Perceived ease of use refers to the extent to which a person believes that using a particular system would be free from effort (Davis, 1989). However, a single model can not cover all constructs which would potentially affect users' adoption of various new technologies, particularly in an electronic risk management system. Evaluating users' adoption of an electronic risk management system must take some additional factors into account.

The risk management acceptance model (RMAM) is an extension of the technology acceptance model (TAM) adopting the mobile services acceptance model (MSAM) (Gao, Krogstie & Gransæther, 2008). RMAM adds context, trust, personal initiatives, and characteristics factors to the study as well as the perceived usefulness (PU) and perceived ease of use (PEU) in the original TAM (Figure 4). Meanwhile, MASAM (Gao, et al., 2008) only studies the intention to use mobile services without measuring the effectiveness of using the mobile services. The intention to use mobile services does not guarantee the effectiveness of using a system. Therefore, this study includes the effectiveness of using ERMS through mobile services in the model. Context refers to any information that can be used to characterize the situation of entries (i.e. a person, place, or object) that is considered relevant to the interaction between a user and an application, including the user and the application themselves (Dey, 2001). Context provides an understanding of the way in which an activity is performed and the circumstances under which the action is performed (Basole, 2004). The use of an electronic risk management system (ERMS) is able to provide independent access to time and place data, which is incorporated into the context construct in the research model. When a system needs to be accessed immediately regardless of time and place restrictions, the usefulness of the ERMS is perceived to be at its highest, so that it will influence the user to use the system. The system that can meet the

user's needs in a specific context will provide the best value to the user. Therefore, it is believed that users' perceptions of the ease of use and usefulness of ERMS may vary in different contexts.

Personal initiatives and characteristics refer to the willingness to experiment with new services (Gao et al., 2008). User willingness and needs play an important role in the adoption of ERMS. ERMS is designed for individuals who may have different expectations and needs in accordance with their preferences. ERMS is a technology-based application, which demands a certain level of knowledge and skills from the users. It may be difficult for people without a technology background to comfortably adopt them. Hence, personal initiatives and characteristics have a significant influence on a user's adoption of ERMS.

A user's beliefs or faith in the system are also important when a new mobile service is introduced to him/her. For ERMS developers, cultivating users' trust is a time-consuming process. Trust is hard to gain, but it is easy to lose. Trust refers to the user's beliefs or faith in the degree to which a specific service can be regarded to have no security and privacy threats (Gao et al., 2008). Many factors may influence users' trust in the process of system adoption. The perception of security and privacy, and integrity of the application are important antecedents of trust in the system. Reputation may be used to bring trust to adopt ERMS. Based on the above discussion our hypothesis is;

H1: There is a significant difference between the existing risk management system and the electronic management system (ERMS).

- H1a: There is a significant difference in context
- H1b: There is a significant difference in ease of use
- H1c: There is a significant difference in perceived usefulness
- H1d: There is a significant difference in trust
- H1e: There is a significant difference in personal initiative and characteristics
- H1f: There is a significant difference in system effectiveness

3. Research Methodology

In order to identify problems in the risk management process of UiTM, focus group discussions were conducted to evaluate the risk management process. The risk management process has been implemented in all branches of UiTM since the year 2016. This study was conducted in the year 2020 allowing the informants to be familiar with the process and thus enabling them to give an in-depth view of the process. Group discussion participants were risk management coordinators from branch campuses on the east coast who are directly involved with the risk management process in their respective campuses. This was important to ensure the validity of the results obtained from the focus group discussions. The informants were representative heads of risk management and risk management administration officers and consisted of 10 members in total. Including all the risk management coordinators from those branches in the focus group discussion reflects a comprehensive set of persons who understand the risk management process in UiTM. This provides validity of the results obtained from the focus group discussions. According to Chioncel et al. (2003), the validity of focus group data requires that informants are competent to answer the research questions. The participants were asked to identify disruption factors in each step of execution in the current risk management process, namely risk identification, risk evaluation, risk controlling, and risk monitoring.

The focus group session took four and a half hours. We started the session by giving an overview of the objectives of the study. The participants were also informed how they should discuss and act during the session to ensure that their opinions provided a genuine representation of the situation. The researchers worked as facilitators of the session by motivating the participants to discuss particular aspects by leading the

discussion. In the second part of the group discussions, participants were asked to explain the problems that they were facing in the risk management process during their work as risk coordinators. The highlighted problems were divided into the four main processes of the risk management process. During the discussion, another researcher collected all the information and made notes. This researcher also acted as a moderator in order to ensure that participants answered each of the research questions, clarifying the questions and providing a brief summary of each research question. In addition to the notes, all discussions were audio recorded. Chioncel et al. (2003) highlighted that descriptive validity (factual accuracy) and interpretative validity (grounded in the language of participants) require a recording technique. This technique is regarded as the best way to capture data accurately.

After identifying the problems in the existing system, an electronic risk management system (ERMS) was proposed as an alternative system to the existing one for all users in the UiTM system which consists of 13 branches nationwide. ERMS is an electronic risk management system that has been developed in response to the need for an electronic system by the UiTM to manage risk effectively. This system allows users to identify, evaluate, control, and monitor risks electronically. Using this system, users can register risks electronically with these risks being evaluated automatically by the system which determines their priority level as high, medium, or low. Using this system, the person in charge will be notified electronically of risks that have been registered, making them alerted of the risks and allowing the correct action to be taken immediately, solving the risks before they actually happen. The risks can also be monitored electronically to know the status of the actions taken.

In order to achieve the second research objective, a purposive sampling method was used. A total of 95 respondents who were involved directly with the risk management system of UiTM including representative heads of risk management and risk management administration officers, participated at this stage. In order to answer the second objective, data were collected from those who were involved in using the ERMS directly. The instrument used was a questionnaire which allowed for a comparison of the effectiveness of the existing system and the newly proposed electronic system. The questionnaire was adopted and adapted from the study of Gao, Krogstie, and Siau (2011). The questionnaire consisted of 7 sections; Perceived Usefulness (PU), Perceived Ease of Use (EU), Trust (TU), Personal Initiatives and Characteristics (PIC), Context (CT), System Effectiveness (SE), and Demographic Information. The questionnaire was distributed online.

The combination of the qualitative method used for analysis of the first objective and the quantitative method used for the second objective enabled this study to explore a more complex aspect of risk management practices in higher learning institutions. Qualitative methods were used for the first objective to allow the informants to express as many problems as they could regarding the risk management process in UiTM. Malina, Norreklit, and Selto (2011) highlight that qualitative research can persuade respondents to provide a rich description and thus enhance strategic comparison across cases. In the end, this benefit allows researchers to make theory generalizations. In contrast a quantitative study was also used to provide guidance to the informants on the established procedures and thus provide results that are more generalizable to the population (Firestone, 1987). Malina, Norreklit, and Selto (2011) stressed that the use of a mixed method can provide new empirical insights as qualitative methods allow readers to understand social phenomena while quantitative study provides valid conceptual grounding.

4. Findings

This section explains the findings from the focus group discussion with 10 informants. The findings were structured in line with the risk management process above:

4.1 Risk Identification

In the focus group discussion, many delegates confirmed that the risk identification process carried out by filling in the risk register form was quite tedious. The form consisted of many items to be filled in which made the process more tiresome. If it was printed on one page, the font was too small and difficult to read. One of the participants highlighted that:

The font in the form is too small. We have to adjust the row and column in order to enlarge the font and this will affect the view of the form.

Another participant added that:

The size of the font in the form sometimes demotivates us to identify more risks as the space given is very limited.

There are a lot of items that need to be filled in the form, making our job more tedious.

4.2 Risk Evaluation

Regarding the risk evaluation step, most interviewees stated that in order to evaluate the severity of risk, which is derived by multiplying the risk probability and with the risk impact, they needed to refer to a risk probability table and risk impact table to calculate and write it down manually. This process was quite tedious as the tables were not attached to the Risk Register Form and thus they had to flip to the tables several times to confirm the scale chosen.

4.3 Risk Control

In the risk Register Form, the head of the department assigns the person in charge of the action to be taken regarding the suggested prevention strategies. The focus group discussions revealed that in this process, the person in charge would not be informed unless a meeting was held to highlight the identified risk. This weakness made the risk management process ineffective and caused a delay in the action taken. The discussion participants highlighted that:

The person that is responsible for the action to be taken on risk prevention strategies does not know their responsibility unless a meeting is held.

It takes time to conduct a meeting as we have to wait for all the top management and parties involved in the risk management process to have free time.

4.4 Risk monitoring

The final step of the risk management process requires the head of department to monitor all the identified risks in order to ensure that all the determined actions have been implemented and the risk consequently eliminated, reduced, or transferred. This monitoring process was done by having regular meetings and discussions to ensure that those who were responsible for the actions to be taken, implemented the risk preventive strategies. Therefore, based on the focus group discussions, the coordinators of risk management explained that the seriousness of the risks would not be informed unless a meeting was held or the person in charge cared strongly about the issue and was alert to the risks identified. The participants of this focus group discussion highlighted that:

Some of the important persons in the risk management process are not aware of their responsibility and are thus absent from the meeting.

Many of those involved in the risk management process can not see the importance of this process to the organization as the action taken is very slow and therefore they can not see the impact of having this process.

Based on the discussion held, it was found that the existing risk management system executed by UiTM was ineffective and caused a delay in action. The process was quite tedious as was carried out manually which involved high paper costs. Thus, it was proposed that the process should be done using an electronic risk management system. The electronic system should allow the risk identifier to key in their risk at the click of a button and to submit the risk identity electronically to the responsible departments in just

a few seconds. This saves time and cost as is a paperless system. The submitted risk is also notified to top management using the electronic system, thus allowing preventive action to be taken in a short period of time. This allows risk to be monitored from top to bottom.

Nevertheless, having a good electronic risk management system alone will not lead to an effective risk management process unless everybody in the system is aware of the importance of the process. Having a good combination of the electronic risk management system and awareness of the importance of the risk management process can lead to a more effective risk management process and eventually can help the organization to achieve its strategic objectives.

This is consistent with previous research which stressed that the funtion of the risk management department was ineffective if the chief risk officer (CRO) did not have the resources, leadership, and support, to communicate his or her understanding of the company's strategic risks proactively and authoritatively throughout the organization (Kaplan & Mikes, 2016). Gao, Sung, and Zhang (2013) highlighted that informal knowledge about risk management may complicate the effective building of risk management capacity among the employees.

After ERMS was introduced to all branch campuses and all parties involved in the operating the system became familiar with the system, a comparative study was conducted between the existing system and the newly proposed electronic system to measure the effectiveness of both systems. There were 95 respondents involved in this study. Tables 1, 2, and 3 show the demographic information of the respondents.

Table 1: Branches involved in the study

UiTM Branches	No. of respondents
UiTM Selangor Branch	69
UiTM Kelantan Branch	10
UiTM Pahang Branch	6
UiTM Negeri Sembilan Branch	3
UiTM Melaka Branch	2
UiTM Perlis Branch	2
UiTM Terengganu Branch	1
UiTM Kedah Branch	1
UiTM Penang Branch	1

Table 2: Designation of the Respondents

Designation	No. of Respondents
Head/Coordinator of a Unit	38
Risk Coordinator	49
Dean	5
Deputy Dean of Research	1
Deputy Rector of Research	1
Deputy Rector of Academics	1

Table 3: Period of Holding the Post

Period (Years)	No of Respondents
0-2	49
2-4	25
More than 4	21

Data were analyzed using a Paired-Sample T-Test. The findings are shown in Table 4. The Cronbach's alpha (α) of all constructs exceeded 0.8 (PU = 0.977, EU = 0.962, TU = 0.959, PIC = 0.899, CT = 0.938 and SE = 0.905). A Paired-Sample T-Test was employed to examine the differences between the two systems. The data analysis in Table 5 shows that the p-values of the hypotheses were less than 0.05, indicating a significant difference between the existing system and ERMS in terms of context, perceived usefulness, ease of use, trust, personal initiative, and characteristics, as well as system effectiveness. Therefore, the hypotheses were supported. In other words, ERMS was more effective than the previous risk management system.

5. Discussion

The results of the study indicated that both methods show the influences of information systems implementation on the effectiveness of the risk management process, as asserted by the previous studies of Halliday, Badenhorst, and Von Solms (1996), Susilowati, Rofi'ah, and Avira (2022), and Alsabti and Khalid (2022). The use of an information system reduces the possibility of duplicating risk records, enhances the management of risk records, as well as reducing the probability of missing risk records. On the other hand, the introduction of a risk management system also enhances the trust of the user towards the risk management process – as an information system is considered

Table 4: Internal Consistency

Factors	Cronbach's Alpha
Perceived Usefulness (PU)	0.977
Ease of Use (EU)	0.962
Trust (TU)	0.959
Personal Initiatives and Characteristics (PIC)	0.899
Context (CT)	0.938
System Effectiveness (SE)	0.905

Table 5: Hypothesis Testing

Hypotheses		Mean	S.D.	P value	Decision
H1	There is a significant difference between the existing risk management system and the newly proposed electronic management system (ERMS).				Supported
H1a	Perceived Usefulness (PU)	-1.234	1.459	0.000	Supported
H1b	Ease of Use (EU)	-1.224	1.268	0.000	Supported
H1c	Trust (TU)	-1.064	1.343	0.000	Supported
H1d	Personal Initiatives and Characteristics (PIC)	-1.045	1.212	0.000	Supported
H1e	Context (CT)	-1.015	1.306	0.000	Supported
H1f	System Effectiveness (SE)	-1.198	1.931	0.000	Supported

a trusted source of information that enables a better understanding of organizational risk records.

Additionally, the results of the study are also in line with the findings of previous research in the Information System (IS) field, which indicate the importance of having an automated system rather than manual handling of resources. The automation process of the manual transaction can help to reduce processing time, and minimize human error, helping an organization to make decisions more quickly, at the same time enhancing the competitive advantage of the organization. Relying on manual transactions can cause many problems such as poor decision-making, repetitive work, and missing reports.

Moreover, the findings also indicate the importance of digital transformation toward an electronic risk management system. The results indicate the importance of Perceived Usefulness (PU), Ease of Use (EU), Trust (TU), Personal Initiatives and Characteristics (PIC), and Context (CT) as the enablers or antecedents of System Effectiveness (SE). Researchers studying information system effectiveness may use the results of this study to further explore and contribute to new findings in the field of information systems and other related fields of study. This study extends previous knowledge on information system acceptance and adoption by empirically validating the research model in the context of risk management implementation in Malaysia.

6. Conclusion

The objectives of this study were to identify the problems in the risk management process adopted by UiTM, Malaysia. Based on the focus group discussions conducted among risk coordinators of the specified higher learning institution, it was found that problems arise in every step of the risk management process, namely risk identification, risk evaluation, risk control, and risk monitoring. The focus group discussions also revealed that the existing risk management process practiced by UiTM was tedious and costly, incurring high costs in terms of time consumption, while it also caused a delay in action and less frequent monitoring. It was found that the adoption of an electronic risk management system made the process of risk management much easier and more effective. The result of the comparative study showed that there was a significant difference between the existing system and the ERMS.

Based on the problems and findings from the above study, it can be concluded that ERMS should be implemented in order to overcome the identified problems. Having an electronic system can save significant amounts of time especially regarding the monitoring of risks identified in the electronic system. It can stimulate the behavior of alertness, care, cautiousness, responsibility, and accountability, among the persons involved in the process in respect of every action determined. Nevertheless, the electronic system may not be effective if there the awareness of the importance of the process to the organization is too low. Thus having a combination of both a good electronic system and knowledge of the importance of the risk management process is important to ensure the effectiveness of the risk management process.

This study is limited to only one higher learning institution, UiTM. Thus future research may extend this research to encompass other learning institutions, strengthening the implications of the study. In addition, the use of a mixed method in this study may provide discrepancies in terms of data interpretation from qualitative and quantitative approaches. Nevertheless, the advantages of using a mixed method outweigh its limitations as it creates a stronger research outcome than either method individually. Future research may extend the objectives of the study by using another quantitative or qualitative method to enhance the understanding of the implementation of risk management practices in higher learning institutions.

References

Ajzen, I. (1991), The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, 50, 179–211.

Alsabti, H. A., and Khalid, A. A. (2022). Factors Influencing Internal Accounting And Financial Audit Effectiveness: Evidence From Oman. Academy of Accounting and Financial Studies Journal, 26, 1-11.

Basole, R.C. (2004). The value and impact of mobile information and communication technologies, in *IFAC Symposium on Analysis, Modelling & Evaluation of Human-Machine Systems*, Atlanta GA, USA.

Beretta, S. and Bozzolan, S. (2004). A framework for the analysis of firm risk communication. *The International Journal of Accounting*, *39*(3), 265-288.

Campbell, S. (2005). Determining overall risk. *Journal of risk research*, 8(7-8), 569-581.

Chioncel, N. E., Veen, R. V. D., Wildemeersch, D., and Jarvis, P. (2003). The validity and reliability of focus groups as a research method in adult education. International Journal of Lifelong Education, 22(5), 495-517.

Cienfuegos Ignacio, (2012). Decision Theory and Risk Management in Public Organizations: A Literature Review. *Revista de Gestión Pública*, 1(1), 101-126

Davis, F. D. (1989), Perceived usefulness, perceived ease of use and user acceptance of information technology, *MIS Quarterly*, 13, 319–340.

Dey, A. K. (2001). Understanding and Using Context. *Personal Ubiquitous Comput*, 5, 4-7.

Firestone,W.A. (1987). Meaning in method: The rhetoric of quantitative and qualitative research. *Educational Researcher*,16(7), 16-21.

Gao, S. S., Sung, M. C., and Zhang, J. (2013). Risk management capability building in SMEs: A social capital perspective. *International Small Business Journal*, 31(6), 677-700.

Gao, S., Krogstie, J. and Gransæther, P.A. (2008). Mobile services acceptance model, in: *Proceedings of the 2008 International Conference on Convergence and Hybrid Information Technology*, IEEE Computer Society, Daejeon, Korea.

Gao, S., Krogstie, J., and Siau, K. (2011). Developing an instrument to measure the adoption of mobile services. *Mobile Information System*, 7, 45-67.

Gefen, D. (2003). TAM or just plain habit: a look at experienced online shoppers. *Journal of End User Computing*, 15, 1–13.

Graham, J.D. and J.B. Weiner, (1995), *Risk vs. risk: Trade-offs in protecting health and the environment*. Cambridge, MA: Harvard University Press.

Halliday, S., Badenhorst, K., and Von Solms, R. (1996). A business approach to effective information technology risk analysis and management. *Information Management & Computer Security*, 4 (1), pp. 19-31. https://doi.org/10.1108/09685229610114178.

Hopkin, P., (2002), *Holistic risk management in practice*. Witherby.

Horton, R.P., Buck, T., Waterson. P.E. and Clegg, C. W. (2001). Explaining intranet use with the technology acceptance model, *Journal of Information Technology*, 16, 237–249.

IRGC, International Risk Governance Council, (2005). *White paper on risk governance. Towards an integrative approach*, Geneva: IRGC.

Kaplan, R. S., and Mikes, A. (2016). Risk management — The revealing hand. *Journal of Applied Corporate Finance*, *28*(1), 8-18.

Kaplan, S., and Garrick, B. J., (1981), On the quantitative definition of risk. *Risk analysis*, *1*(1), 11-27.

Kaplan, S., (1991), Risk assessment and risk management – basic concepts and terminology, In *Risk management:*

Expanding horizons in nuclear power and other industries, 11–28. Boston, MA: Hemisphere Publ. Corp.

Knight, Frank H., (1921), *Risk, Uncertainty, and Profit*. New York: Hart, Schaffner, and Marx.

Lowrance. W.W. (1976). *Of Acceptable Risk: Science and The Determination of Safety*. Menlo Park, Ca: William Kaufmann Inc.

Lederer, A.L., Maupin, D.J., Sena, M.P. and Zhuang, Y. (1976). The technology acceptance model and the World Wide Web, *Decis Support Syst* 29 (2000), 269–282. Lowrance, W. W. Of Acceptable Risk: Science and the Determination of Safety.

Malina, M. A., Nørreklit, H. S., and Selto, F. H. (2011). Lessons learned: advantages and disadvantages of mixed method research. Qualitative Research in Accounting & Management, 8(1), 59-71.

Perera, A.A.S., Rahmat, A. K., Khatibi, A., Azam, S. M. F. (2020). Review of literature: implementation of enterprise risk management into higher education. *International Journal Journal of Education and Research*, 8(10), 155-172.

Rosa, E.A., (2003), The logical structure of the social amplification of risk framework (SARF): *Meta*theoretical foundations and policy implications". In *The social amplification of risk*, Edited by: Pidgeon, N., Kasperson, R.E. and Slovic, P. 47-79. Cambridge: Cambridge University Press.

Sabri, H. A., (2011). The impeding drivers of risk at private higher education institutions in jordan: an analytical approach. *Journal of Education and Vocational Research*, 2(4), 120-131.

Susilowati, E., Rofi'ah, R., and Avira, S. (2022). The Relationship of Technology Advancement, Company Management, and Manager Knowledge on the Effectiveness of Accounting Information Systems. *International Journal of Information System and Technology*, 5(6), 736-742.

Smith, H. A., McKeen, J. D., and Staples, S., (2001), New developments in practice I: Risk management in information systems: Problems and potential. *Communications of the Association for Information Systems*, *7*(1), 13.

Stoneburner, G., Goguen, A., and Feringa, A., (2002), Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-830.

Togok, S. H., Isa, C. R., and Zainuddin, S. (2016). Enterprise risk management adoption in Malaysia: A disclosure approach. *Asian Journal of Business and Accounting*, *9*(1), 83-104.

Van Staveren, M. T. (2009). *Risk, innovation & change: Design propositions for implementing risk management in organizations, PhD Dissertation*. Enschede, The Netherlands: University of Twente.

Vaughan, E. J., (1997), *Risk Management*, New York: Wiley

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003). User Acceptance of Information Technology: Toward a Unified View, *MIS Quarterly*, 27, 425–478

Webster, N. (1983). *Webster's Desk Dictionary of The English Language*. Portland House: London.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis: An International Journal*, *27*(3), 597-606.