12-2022

ENTERPRISE RISK MANAGEMENT: SMALL AND MEDIUM BUSINESS

vasili krespis

ENTERPRISE RISK MANAGEMENT: SMALL AND MEDIUM BUSINESS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology:

Cybersecurity

---

by

Vasili Krespis

December 2022

ENTERPRISE RISK MANAGEMENT: SMALL AND MEDIUM BUSINESS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Vasili Krespis

December 2022

Approved by:

Jesus Canelon, Ph.D., Committee Chair

Barbara Brough, Committee Chair

Conrad Shayo, Ph.D., Committee Member

ABSTRACT

This culminating experience project examined common risk management trends and challenges that SMEs face and provided methods and tools that could limit threats and impact of unforeseeable events. This project demonstrates why business owners should use a risk management planning framework. The research questions were: (Q1) What are risk identification strategies which do not overstrain SMEs' limited resources? (Q2) How may risk analysis be performed effectively in SMEs? (Q3) How does the SMEs risk management system change over time? (Q4) What are the most effective risk analysis techniques and strategies for SMEs with limited resources?

A case study was examined using the COSO Enterprise Risk Management (ERM) process to identify unique risk management challenges that SMEs face and to provide recommendations. The results were as follows: (Q1) Use brainstorming workshops to identify risks. Use face-to-face discussions to share ideas and provide feedback. Use a qualitative top-down approach with stakeholders to identify organizational and strategic risks. Use functional diagrams and interviews with risk owners to understand and identify risks. (Q2) Consider risks in every activity from organizational level to business unit. Hold meetings with stakeholders to gain insight. Understand the enterprise’s risk culture and objectives. Conduct a risk assessment. Involve board members and management throughout the ERM processes. Understand and define

organizational objectives. Define risk tolerance, develop risk response, and control activities.

(Q3) Once ERM was successful in the Portfolio Management Department (PMD) it was expanded throughout the enterprise. Continuous monitoring, assessment, and updating was critical throughout the enterprise life cycle. Routine maintenance was required, and the risk register was updated periodically. Threats and risks are always changing and evolving so they were continuously revisited. Controls were checked for effectiveness and risks were reevaluated. (Q4) Risk tolerance was defined by specifying risk appetite using a financial risk tolerance-based benchmark. A risk map was used to calculate likelihood and impact. The PMD risk map was periodically updated to show current risks.

Likelihood and impact ordinal scales to measure the impact of risks and portfolio management software was used to monitor and receive feedback. This case study shows that SMEs should focus on training and learning, cultivate strong governance and culture, allocate a team to understand and execute strategic objectives, and utilize a framework to help organize and guide internal operations. An enterprise risk management plan strengthened communication and collaboration and helped the enterprise accomplish various objectives that align with the enterprise's mission statement and core values. Areas for further study include the use of artificial intelligence and machine learning to predict both internal and external risks. The use of alternative frameworks such as the NIST

Risk Management Framework (RMF), the ISO 31000, or the COBIT ERM Framework.

ACKNOWLEDGEMENTS

I want to thank my family, my professor Barbara Brough, and my professor Dr. Shayo.

DEDICATION

I want to dedicate this work to my father, Nick Krespis, and my mother, Afrodite Krespis. Thank you for the motivation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

Data breaches are an imminent concern for today's enterprises. The average global cost of a single breach is quickly approaching $4 million (Johnson, 2019). For many enterprises, a data breach can have serious implications, such as regulatory fines and penalties, a loss of reputation, damage to mission-critical systems, and data loss. In fact, 60 percent of small companies go out of business within six months of falling victim to a data breach or cyber-attack (Johnson, 2019). Not all attacks are malicious; they can be caused by human error, environmental disruptions, and equipment failure. Risk management preparation is critical to organize the enterprises internal environment. Without adequate planning, security activities may become too costly, demand too many specialized roles, and produce ineffective solutions (NIST 800-37 R.2, 2018).

Many small and medium-sized enterprises (SMEs) lack the knowledge, resources, tools, and management skills for proper risk management applications (Brustbauer, 2014). Applying risk management in these enterprises may be difficult due to the significant investment of time and resources needed to establish and implement the risk management plan while also maintaining all other operations. Many SMEs are not prepared to resolve the growing challenges that they currently face. While you can never eliminate your risks, many situations can be predicted and managed. This culminating experience project

will examine the security issues SMEs face and investigate tools and methods they can adopt to develop an enterprise risk management plan. How can these enterprises manage risk to increase efficiency and security posture?

Problem Statement

There are many benefits that a risk management plan can provide SMEs, including operational risk awareness, understanding strategic objectives, and increasing shareholder value. Due to the significant increase in the complexity of hardware, software, and evolving threats, this represents a significant increase in attack surface that can be exploited (NIST 800-37 Rev. 2, 2018). Security threats to small business infrastructure are outpacing efforts to reduce vulnerabilities. This creates an urgent need to strengthen information systems. However, these enterprises are not prepared to resolve the growing challenges that they currently face.

Objective

The objective of this project is to explore risk management trends and challenges that SMEs currently face and to provide recommendations to business owners, executives, and security professionals in the form of methods and tools to limit threats and reduce the attack surface. An enterprise risk management plan ensures operational risk awareness across the organization. Furthermore, it strengthens collaboration between internal and external

stakeholders and aims to reduce the likelihood and impact of unforeseeable events.

Research Questions

1. What are risk identification strategies which do not overstrain SMEs' limited resources?
2. How may risk analysis be performed effectively in SMEs?
3. How does the SMEs risk management system change over time?
4. What are the most effective risk analysis techniques and strategies for SMEs with limited resources?

Methodology

To understand how SMEs can benefit from enterprise risk management, this project will first investigate common issues and constraints that are affecting these enterprises and look for patterns or recurring issues. This will entail researching risk management procedures for SMEs exclusively. Next, the project will examine cost-effective risk management techniques, use frameworks, and a case study to provide different perspectives on potential solutions. Finally, the project will draw conclusions and provide recommendations to SME owners, security professionals, and executive decision-makers. The primary research will

consist of scholarly articles, literature analysis, frameworks, and open-source surveys.

Organization of Study

The project is organized as follows: Chapter 2 will review the literature and common challenges that SMEs face; Chapter 3 will review risk management and review the COSO ERM framework; Chapter 4 will review a relevant case study; Chapter 5 will summarize a discussion, conclusions, and further areas of study.

.

CHAPTER TWO

LITERATURE REVIEW

The literature presented in this project has been found using the search terms: risk management SME, SME ERM framework, SME risk management, SME IT constraints, SME risk management practice, SME security, cyber-attack. Due to consistent changes in the threat landscape and the rapid progression of technology, research has been limited to the last nine years to reflect the most concurrent evidence. The research used in this project was collected between 2014 and 2022. A table has been provided on the following page to show databases searched, search words, relevant publications, and authors.

Table 1. Research Methods and Publications

Database Searched	Search Words	Number of Relevant Publications	Number of Relevant Publications Selected	Authors
Google Scholar; Pfau Library's; OneSearch; *Small Enterprise Research*	SME ERM framework	17	3	Bensaada, I., & Taghezout, N., 2019. Crovini, C., et al.,2021. Ciocoiu, C., et al. 2020.
Journals of Risk and Financial Management, Google Scholar	SME risk management	9	2	Chakabva, O., et al. 2021. Krüger, N. A. & Meyer, N. 2021.
Pfau Library's OneSearch	SME risk assessment	13	1	Grondys, K., et al., 2021.
Information Systems Frontiers, Google Scholar; Pfau Library's OneSearch	SME IT constraints	6	1	Heidt, M., et al., 2019.
Google Scholar; Pfau Library's OneSearch	SME risk management practice	13	1	Henschel, T. & Durst, S. 2014.
Pfau Library's OneSearch; Google Scholar	Risk management SME	23	4	Krüger, N. A., 2021;. Martins, Y. et al. 2021.

				Lima, P. F. D. A, & Verbano, C.,2019. Brustbauer, J.,2014.
Computer Fraud and Security, Google Scholar; Pfau Library's OneSearch	SME security	12	1	Kurpjuhn, T., 2015.
Journal of Cybersecurity and Privacy, Google Scholar; Pfau Library's OneSearch	Cyber-attacks	7	1	Quader, F., & Janeja, V. P., 2021.

The initial OneSearch brought 8,429 results. Filters were then used to ensure the relevance and validity of the sources. Articles were then selected from Peer-Reviewed journals, which were written in English between the years of 2014-2022. After updating the filters, 2,505 results remained. Titles and summaries were read and sorted to determine relevance to the project topic. The following section will summarize relevant risk management findings in SMEs.

Brustbauer (2014) developed a structural model based on a survey. The results show that SMEs either follow an active or passive approach. This directly affects their strategic orientation. An active enterprise risk management approach helps enterprises to gain a competitive advantage. ERM implementation depends on firm size, sector, and ownership structure. Many of these enterprises lack knowledge, resources, tools, and management skills for proper risk management application (Brustbauer, 2014).

Bensaada & Taghezout (2019) created a cost-effective framework to help SMEs engage in Enterprise Risk Management (ERM) practices. Bensaada's comprehensive approach is applicable to all types of SMEs. The Modular Optional and Sequential (MOS) framework is divided into several modules that are broken down into tasks. The modules are straightforward and adjustable; they were designed to be understood by non-professionals. Ciocoiu et al. (2020) conducted a survey that consisted of 146 SMEs in Romania. They then took the data from the survey and created a fuzzy model to identify the behavioral

determinants of risk management in SMEs. The data showed that stakeholder requirements, a strong leader, and knowledge and training were all important determinants of the implementation of risk management. The results provide knowledge to understand the factors that may influence risk management implementation. The study helps SMEs to improve their risk management process.

Henschel & Durst (2014) made a cross-country comparison of SMEs in Scottish, Chinese, and German SMEs. They compared their risk management practices by using a web-based survey. They then followed up with research interviews. They received 270 responses from 121 Chinese firms, 87 German firms, and 62 Scottish firms. The results showed very different levels of risk management styles. All three countries received a low score regarding responsibility for implementation and reviewing risk management. They also all received low scores regarding risk communication and documentation.

The most significant issue among the SMEs was a lack of integration of identified risks into the business planning. The results also reveal that it takes a whole management team of employees to properly maintain a risk management system. The study found that Scottish owners and managers see risks as potential opportunities for innovation. While the German and Chinese enterprises saw risks as threats that needed a consistent organizational response. This study shows a cultural divide between the countries.

Grondys et al. (2021) conducted a survey in Poland among 496 entities including micro and SMEs. The survey was sent electronically to randomly selected enterprises. The respondents were either managers or business owners. They found that the main problems affecting the development of these enterprises were high taxes and finances. They also found that it was too expensive to conduct operational activities such as risk management procedures. Another issue they found was that they received untimely payments from customers, which directly affected their organizational investments.

Crovini et al. (2021) conducted an Advanced Reasoned and Organized (ARO) literature review. They found that SMEs put little effort into risk identification, assessment, and monitoring due to a lack of knowledge and mindfulness. They also found that there is a lack of culture and training procedures in these enterprises. This translates to users with inadequate skills and a lack of awareness. They also found that there is a poor understanding of risk assessment benefits. They found that most of these enterprises do not implement systematic risk assessment strategies. Strategic risk management implementation allows the enterprise to become more resilient and better prepared to adapt to crises and adverse risks. This makes it important to engage in risk management throughout the enterprise life cycle.

Martins et al. (2021) developed a model for risk management and applied it to a Brazilian SME in the context of the ISO 9001:2015 framework. They found that there is a need for continuous internal training to educate employees on risk

management. This training can contribute to risk-based thinking. They also found that risk management is dependent on the level of knowledge on the subject. Availability and commitment were both necessary for effective risk management implementation. Lima & Verbano (2019) created a framework and conducted a pilot case to help a small-sized consulting company adopt project risk management. They found that a project risk management plan improved the project's performance, increased client trust, and improved the decision-making process. The company was also able to manage risk more efficiently by using risk mitigation and risk transfer techniques.

Project risk management (PRM) application gave the company “Alpha” a strategic opportunity to improve client communication. The company had difficulties understanding the interactions between the client’s information system and the Customer Relationship Management (CRM) system. Project risk management helped company “Alpha” identify the risks that were initially difficult to distinguish at the beginning of the project. The PRM application also resulted in a positive cost-benefit ratio between the risk management outcomes and implementation costs. One of the reasons SMEs fail to apply PRM is because CEOs cannot justify the costs. The pilot case verified the validity of the framework.

Krüger (2021) studied the relationships between demographics and risk management components that SMEs faced in South Africa. Risk management consists of the process of risk identification, assessment, treatment, planning for

future and potential risks, establishing communication and reporting procedures, and long-term monitoring (Krüger, 2021). He used correlation analysis to find that as SME owners age, their risk-taking will decrease, and they become more adept at using risk management. The longer a business stays open, the more aware it becomes of external risks (Krüger, 2021). Lastly, he found that it is easier to identify risks when the business owner is older, and the enterprise has more employees (Krüger, 2021).

Research by Heidt et al. (2019) used literature review to identify SME constraints and how these constraints influence IT security decisions. They constructed a conceptual framework to help further analysis. The research follows three steps: the input step, the processing step, and the output step, which helps to summarize findings in SME constraints. Based on literature analysis, they found several environmental factors and constraints affecting SMEs, namely insularity, low formalization level, leadership constraints, small asset base, and limited resources.

Insularity Findings:

This study evaluates the overall insularities of SMEs based on location and culture and their effect on management. Location restrictions made sourcing products and services more difficult. SMEs, especially those in rural areas were limited in sourcing and vendor options. Owners and managers found it difficult to

find IT solutions due to remote rural locations. They also found that there were fewer IT experts in these areas.

Low Formalization Level Findings:

The study shows that at this level, SMEs do not have adequate security personnel. One person is left doing several different security tasks. This can lead to a lack of accountability and authority issues. The second issue was that SMEs are under allocating budget in IT security. Lastly, undocumented processes were the third issue with low formulization constraints.

Leadership Constraints of SME:

Findings show a trade-off between daily business activities and IT security investments. Temporal focus findings concluded that even though managing directors were aware of IT security risks, they prioritized day-to-day business over investments due to short-term or operational focus. Research also showed that managers who were over-emotional in decision-making had a negative impact on IT security decisions.

Small Asset Base:

They found that the firm assets that were linked to the owner's personal assets had a low influence on IT security investments. This is because the owner was more concerned with generating profits. Difficulties obtaining finances through

institutions or government had a low to medium relevance on IT security investments. Also, the Cash flow and revenue stream had a low to medium relevance on IT security investments.

Limited Resources:

Limited budget had a high impact across all SMEs, and this meant less expenditure for IT security. They also found that limited time affected IT security investments and that time should be assessed like budget or capabilities. Limited or no experience employees had a negative impact regarding IT security. They also found that risk assessment is not formalized in SMEs as it is in large enterprises.

Kurpjuhn (2016) authored an article called “The SME security challenge,” where he talks about how limited resources and budget constraints can compromise the SMEs security posture by under-allocating security investments. He argues that security is not appealing to the decision-makers because they would rather focus on profits. Furthermore, he states that outdated security standards can increase downtime and decrease productivity. He recommends that hardware components are purchased from a reputable vendor to ensure adequate security standards. He also states that SMEs may choose to use a third party to overlook compliance issues and outline a plan for best practice. Kurpjuhn recommends that SMEs use a firewall for network protection to create

barriers or network layering. He also states that SMEs should collaborate with vendors to develop unified threat solutions. Kurpjuhn also believes that the increased use of personal devices in the workforce creates new security management challenges. He recommends a guide to outline how employees utilize personal devices at work.

Research by Quader & Janeja (2021) analyzed many different cyber-attacks to better understand the decision-making process and the remediation strategies used for several types of cyber-attacks. They used case studies to research different attacks and analyzed the major contributing factors of these attacks. They also recommend remediation strategies. Their goal is to help prevent organizations from being victims of cyber-attacks. In most cyber-attacks, human behavioral aspects and the response to malicious stimuli are the weakest links in bringing about a successful cyber-attack (Quader & Janeja, 2021). They found that certain behaviors such as lack of awareness, noncompliance, and ignorance can cause many problems and may lead to a cyber-attack.

They evaluated forty-three different cyber-attack incidents and studied the process, impacts, and outcomes of these attacks. They noticed a lack of systematic study, negligence, and ignorance of cyber-attacks contributed to the problems. Human behavior often influences the progression of cyber threats. Employees are prone to accidents and must be trained. Other factors such as caution, security education, increased awareness, and security competence plays a significant role in avoiding cyber threats (Quader & Janeja, 2021).

Although this study was conducted on large organizations it is still relevant to the topic because it shows how human behavioral aspects affect cyber-attacks.

Krüger & Meyer (2021) developed a Small Business Risk Management Intervention Tool (SBRMIT) for SMEs. This tool helps these enterprises to identify, evaluate, and address risks. The goal is to assign priority to risks and develop business strategies to help SMEs align and respond to compliance requirements. The SBRMIT tool was designed to help small and medium enterprises to incorporate fundamental risk processes. The tool helps to establish a clear understanding of the businesses' limitations and it also helps to implement the requirements needed to develop an internal risk management system. The SBRMIT exists only as a theoretical structure and further testing is needed on real firms.

Chakabva et al. (2021) conducted a survey of 320 SMEs in Cape Metropole, South Africa. Out of the 320 SMEs 289 were included in the final analysis. They used a Resource Based View Theory (RBV) to interpret the results to analyze factors that are limiting effective risk management in emerging market SMEs. They found that both tangible and intangible resources have a positive impact on the effectiveness of risk management in emerging markets. The results also revealed that limited knowledge and finances affect risk management investments. The study found numerous factors limiting effective risk management including a "costs exceeding benefits mentality." Several other limiting factors included: not using risk management frameworks, improper

documentation, and employee refusal. The research suggests that resources are key drivers to performance.

In summary, the review revealed that most of the risk management literature was directed to large organizations. This means, risk management is a new concept that has not been fully explored much by SMEs. The research showed that there is a lack of knowledge and application in SMEs and that further research is necessary to guide application and best-use practices.

Risk Management Challenges

According to an article written by Sam Gutierrez, an overwhelming 76% of Americans believe that businesses in the U.S. will experience a major cyber-attack within the next 12 months (Gutierrez, 2022). Despite SMEs acknowledging the growing risk of cyber-attack, they are slow to adapt, and very few are prepared to defend against an attack. According to a survey conducted by Security Intelligence, only half of small businesses are ready to manage a cyberattack (Gregory, 2022). This shows that a lack of risk management planning is common among SMEs. Risk management is challenging for these enterprises because it requires financial investment, organizational planning, and experienced personnel with specialized skills to orchestrate effectively.

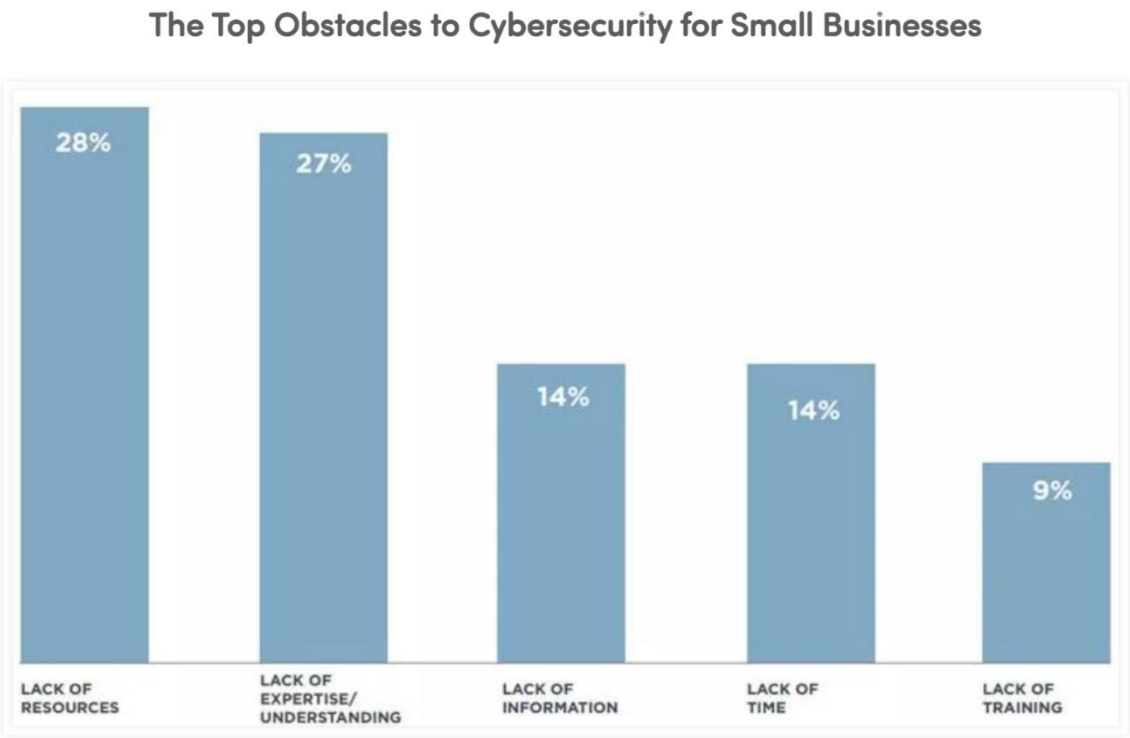

Figure 1. The Top Obstacles to Cybersecurity for Small Business (bbg.org).

Some of the most challenging obstacles that SMEs face when implementing cyber security:

- Inadequate resources – Business owners are often unaware of specialized frameworks such as those provided by the Committee of Sponsoring Organizations (COSO) Enterprise Risk Management framework, the International Organization of Standardization ISO 3100, and the National Institute of Standards and Technology Risk Management Framework. Business owners and managers do not understand technical controls and tools and how to use them properly.

SMEs typically do not have the financial ability to hire specialized employees, hire advisors, and purchase expensive proprietary tools.

- Lack of expertise/understanding - SMEs often lack specialized roles, responsibilities, and skills. These enterprises lack organization and formalized procedures to educate users. They also cannot afford to hire enough IT professionals.
- Lack of information – Owners and managers are often limited in their understanding of risk management procedures and see risks from a limited perspective. They are more concerned with short-term operations and profits rather than long-term security investments.
- Lack of time – Owners and managers are often more concerned with availability. The enterprise does not have the bandwidth or capability to worry about security.
- Lack of training – SMEs often lack specialized role-based training, procedures, and user awareness training. Some common policies include acceptable use policy. Acceptable use and awareness training policies can educate users on how to operate hardware and software, it also communicates to users' expectations for business operations. An example of this is to create a policy that prohibits users from connecting USB and untrusted storage devices on work computers or networks. This reduces the risk of installing a virus.

According to Verizon's 2022 data breach report, this year 82% of breaches involved the human element (Bassett et al., 2022). This includes the use of stolen credentials, phishing, misuse, and user error. Employees are often considered the “weakest link” in cyber security, and this continues to play a significant role in both incidents and breaches. It is important for these enterprises to address the associated risks that employees pose. This can be addressed through cyber security awareness training and implementing policies to help facilitate learning. Workshops are another tool to help reduce user risks. Workshops can reinforce user knowledge, provide specialized training, and communicate management expectations.

According to the Insurance Bureau of Canada research survey conducted on 1,525 Canadian SMEs, only 34% report that their company provides mandatory cyber security awareness training (IBC,2022). A lack of training in these enterprises continues to be a major challenge. Enterprises should incorporate training protocols and best use practices to ensure that users are operating within the expectations of management. Users should be trained to operate hardware and software, how to respond to phishing email attempts, and how to navigate the internet safely. Users tend to underestimate their role in defending against cyber-attack. This creates a huge vulnerability for the enterprise. User training can be reinforced through conversations and periodic meetings to gain further insight.

According to a survey conducted by the U.S Small Business Administration, 88% of small business owners felt their business was vulnerable to a cyber-attack (SBA.gov, 2022). Widespread vulnerabilities are so common now that attackers have multiple entry points to access critical information systems. Vulnerabilities have become too difficult to identify and correct. This makes them an easy target for exploitation. Here is a list of common vulnerabilities found in SMEs:

- Configuration issues – It is common to see hardware configuration issues. An example of this is a firewall with rules that are not set correctly. This can cause unwanted traffic, allowing hackers to easily enter the system.
- Vulnerable business processes – Businesses may not be compliant with rules and regulations. For example, enterprises that store data must govern this data appropriately and are required to adhere to standards set by the Federal Trade Commission.
- Undocumented assets – Lack of documentation makes it difficult to identify assets and this can contribute to system sprawl. When this occurs system administrators are unable to identify assets or retrieve configuration settings.
- Outdated hardware and software – Some hardware and software such as Legacy systems are reaching the end of the life cycle. This means

that they may not be supported by 3rd party vendors. Another common issue is hardware and software that is not being patched.

- Lack of policies and training – Lack of policies can create a host of issues for the enterprise. A common issue is not setting password policies. Users may set weak passwords making them an easy target for a Brute Force Attack. User training is often neglected in these enterprises, this can contribute to user error and confusion. Undertrained users are more susceptible to phishing attacks and accidental errors. Lack of policies and training creates vulnerable business processes throughout the enterprise.

Due to the increased complexity of threats and vulnerabilities, it becomes inherently difficult to defend against attacks. Universally connected devices become a hotbed for attackers. Sophistication of attacks are becoming harder to detect and hackers no longer need to have extensive technical knowledge. Modern attack tools such as Kali Linux are free and easy to execute. An attack can now be launched instantly with minimal effort or skill. The threat landscape is always changing and evolving, this makes it extremely difficult to secure critical business systems.

SMEs face many challenges in risk management application. First, the board members should focus on organizational planning, utilize a top-down approach, and work with management to define risks. Then, the culture, values,

and behaviors must align with the mission statement and key objectives. Finally, user training, policies, and procedures should be prioritized to cultivate an initiative-taking environment. After addressing these issues, the enterprise can work towards implementing an enterprise risk management plan.

Background: Understanding Security

Since an enterprise can never be fully secure, it should focus efforts to control risks in a standardized approach so that results can be measured and replicated throughout the business environment (Ciampa, 2017). The goal of information security is to ensure that controls are in place and are working effectively to prevent a successful attack (Ciampa, 2017). SMEs can use information security to protect assets and valuable information. SMEs can also create a culture of awareness and learning to help prevent cyber-attack. A positive attitude from board directors can help create an environment that encourages learning and collaboration. “Information security involves protecting confidentiality, integrity, and availability” (NIST 800-37 R.2, 2018).

- Confidentiality – An enterprise should protect information from unauthorized access (NIST 800-37 R.2, 2018). An example of this can be to use encryption to protect data. Another type of confidentiality is an access control list. The access control list regulates who can view and access resources. Network segmentation is another confidentiality tool used to keep internal networks separated from the public. Least

privilege is another tool that is used to separate access of data. Users are given the bare minimum access to complete their tasks. This keeps sensitive information safe and adds an extra layer of protection.

- Integrity – It is important for an enterprise to ensure that information has not been altered (NIST 800-37 R.2, 2018). An example of this is when a disgruntled employee can modify payroll and change the amount they are paid. All changes and updates should be thoroughly documented to ensure the integrity of the business systems and networks.
- Availability – It is important for an enterprise to protect against disruption (NIST 800-37 R.2, 2018). An example of this is to utilize an uninterruptible power supply (UPS) to stay online during an equipment failure or power outage. It is also important to keep backup equipment handy in case of malfunction. Downtime can create a host of issues for the enterprise, including loss of revenue, which can also taint the enterprise's reputation.

Information is stored on computer hardware, processed by software, and transmitted by communications, so each of these areas must be protected (Ciampa, 2017). There are many layers involved in information systems therefore, optimal security is achieved in layers. Security layering is often referred to as defense-in-depth. The three layers that an enterprise needs to

protect are assets, people, and policies. An example of security layering can look like an intrusion detection system (IDS) used to track anomalies, combined with best use practices and policies, physical controls such as firewalls, and awareness training protocols.

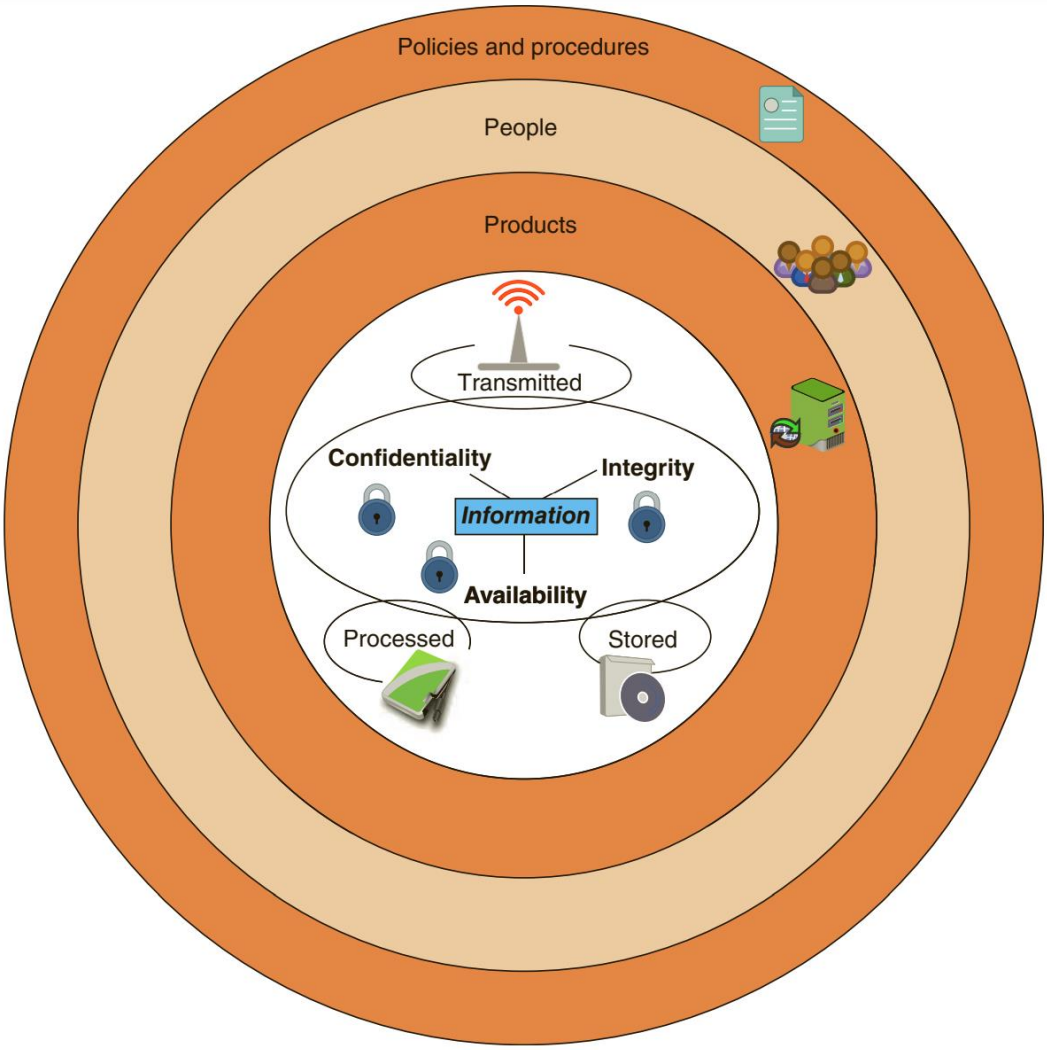

Figure 2. Information Security Layers (Ciampa, 2017).

Understanding Risk

Risk is a function of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have on the business (Paulsen & Toth, 2016). Threats may negatively impact or disrupt the enterprise's information systems. Common threats to information security systems come from environmental factors, business resources, and bad actors. An enterprise must understand its unique risks, so they know where to focus security efforts. Understanding risk requires an awareness of procedures and policies, aligning business objectives with the enterprise's mission and goals, and establishing a culture that reflects moral and ethical values.

Here are a few examples of common threats:

- Environmental factors – ex: earthquake, fire, and flooding.
- Business resources – ex: hardware, architecture/design flaws, and policies.
- Bad actors – ex: hackers, criminals, and disgruntled employees.

A vulnerability is a weakness that could be used to harm the business (Paulsen & Toth, 2016). When information is not being protected effectively this becomes a vulnerability. Most information security breaches can be traced back to only a few types of common vulnerabilities (Paulsen & Toth, 2016). Some common vulnerabilities are public-facing servers, weak passwords, and untrained users. By actively minimizing vulnerabilities an enterprise is taking action to minimize the likelihood of a security incident.

When targeting small and medium enterprises, the criminals access victim networks via Microsoft's Remote Desktop Protocol (RDP) either via unpatched vulnerabilities or weak passwords (Widup et al., 2013). Figure 3. Shows that 40% of Ransomware incidents gained access to the business network using stolen password credentials. Thirty percent of Ransomware attacks entered the system through phishing emails, and 13% of Ransomware attacks entered the system through exploiting a vulnerability. Phishing attacks can target many different entities. When a phishing attack targets the CEO, this is called whaling. Phishing attacks may be directed toward employees at all levels including board members, third-party vendors, and even customers.

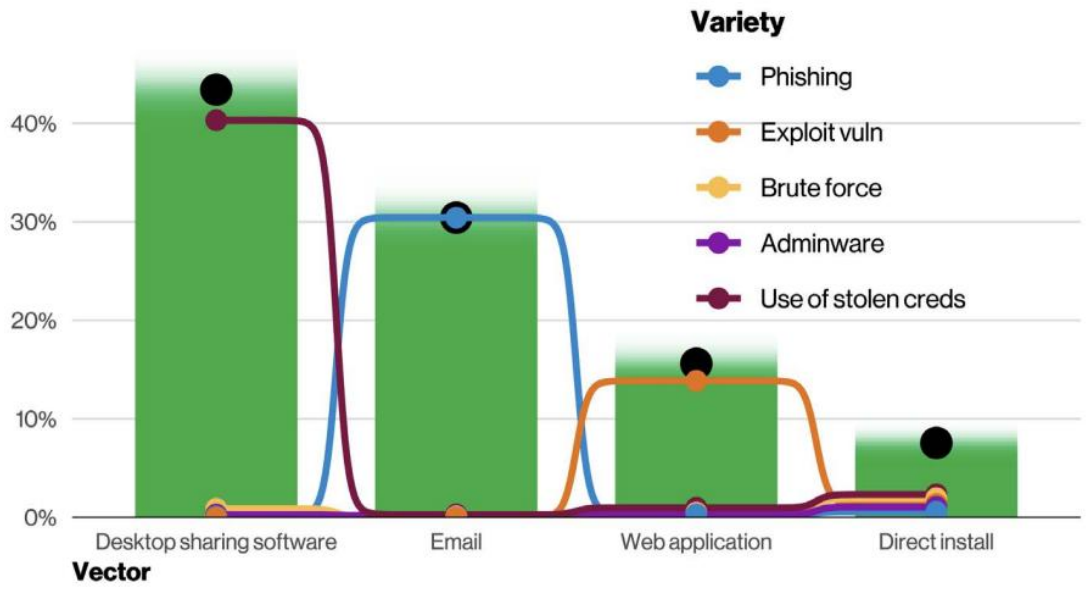

Figure 3. Action Varieties Within Ransomware Incidents (Bassett et al., 2022).

CHAPTER THREE

RESEARCH METHODOLOGY

Risk management requires setting the internal environment, identifying risks, setting controls, monitoring, and making the necessary adjustments. Risk management requires collaboration from board members, management, system owners, employees from various departments, and even customers. The risk management plan should be updated and reviewed when changes have been made to the business systems. It is recommended to update the risk management plan at least annually. This involves updating documentation and diagrams, testing to validate that control implementation is correct, updating/patching systems, and updating the risk register.

Stakeholders and leaders are becoming more transparent and accountable when managing risk (Everson et al., 2017). Management is responsible for maintaining security risks and collaborating with board members. Management is also in charge of selecting and defining a risk management strategy. Once the enterprise has chosen a strategy, management will than appoint a team to complete goals and objectives. Effective communication strategies help to create a risk dialogue that will enhance communication throughout the enterprise. This creates trust, confidence, and a universal dialogue that can help stakeholders collaborate and reach objectives.

Board members should assist management throughout all risk management activities. Their oversight responsibilities include reviewing

changes, providing insight, and acting as a checks and balances for management (Everson et al., 2017). Board members are expected to help select strategies and define the risk appetite. These stakeholders help to align strategy with the enterprise's objectives, mission statement, and core values. Board members are expected to help with capital allocation and funding as well as respond to the enterprise's performance needs. Board members that instill a positive attitude and are open to discussion and collaboration with management and other stakeholders. This can help create a positive culture that promotes change and is adept to problem solving.

Various comprehensive risk management frameworks are available to help guide the internal control process, enhance stakeholder value, and help protect the enterprise. The ISO 31000 and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework are two of the most popular. The case study in this project uses the COSO Enterprise Risk Management framework. The COSO ERM was published in 2003 and was revised in 2017. The framework has been used around the world by many SMEs. The COSO ERM framework can help an enterprise to identify and manage risk while also helping to achieve goals and objectives (Everson et al., 2017).

COSO ERM Framework

To help small and medium enterprises to develop a cyber mindset and manage both internal and external risks, the COSO ERM Framework was utilized throughout this project. The COSO ERM framework is divided into five overlaying themes. The first theme is related to “Governance and Culture” *(*Everson et al., 2017*)*. Governance helps the enterprise to establish a risk philosophy. It also provides oversight to the management decision making process (Everson et al., 2017). Culture has to do with the enterprise’s unique values and behaviors. Board members are responsible for setting the enterprises culture and values. The next theme is “Strategy and Objective Setting.” Once risks have been identified the enterprise will establish the risk appetite, and then choose an appropriate strategy based on likelihood and impact. Objectives can be referred to as the individual goals that align with the enterprises mission statement. Strategy and objective setting are the plans to identify, assess, and respond to risk.

The third theme is “Performance.” Once risks have been identified and the risk appetite has been established, it is now time to perform the risk assessment. The risk assessment classifies risks based on likelihood and impact estimates. The enterprise will develop a risk response strategy based on the risk assessment results and then report this information to key stakeholders. If the enterprises performance is low the strategy will need to be revised. The fourth theme is *“*Review and Revision” (Everson et al., 2017*)*. Performance should be

monitored and reviewed so that the enterprise can gauge how well the risk management plan is working overtime (Everson et al., 2017). A well-prepared enterprise will have back up strategies and weigh out options to choose the most effective course of action.

The fifth and final theme is “Information, Communication, and Reporting” (Everson et al, 2017). Enterprise risk management is a continuous process that requires constant monitoring and collaboration from various stakeholders (Everson et al., 2017). The information and communication flows up, down, and across the enterprise (Everson et al., 2017). These five overlaying themes can be applied to any enterprise regardless of size or sector. The COSO ERM framework provides enterprises with a model to help stakeholders better understand their risk-related activities and their impacts (Moeller, 2007).

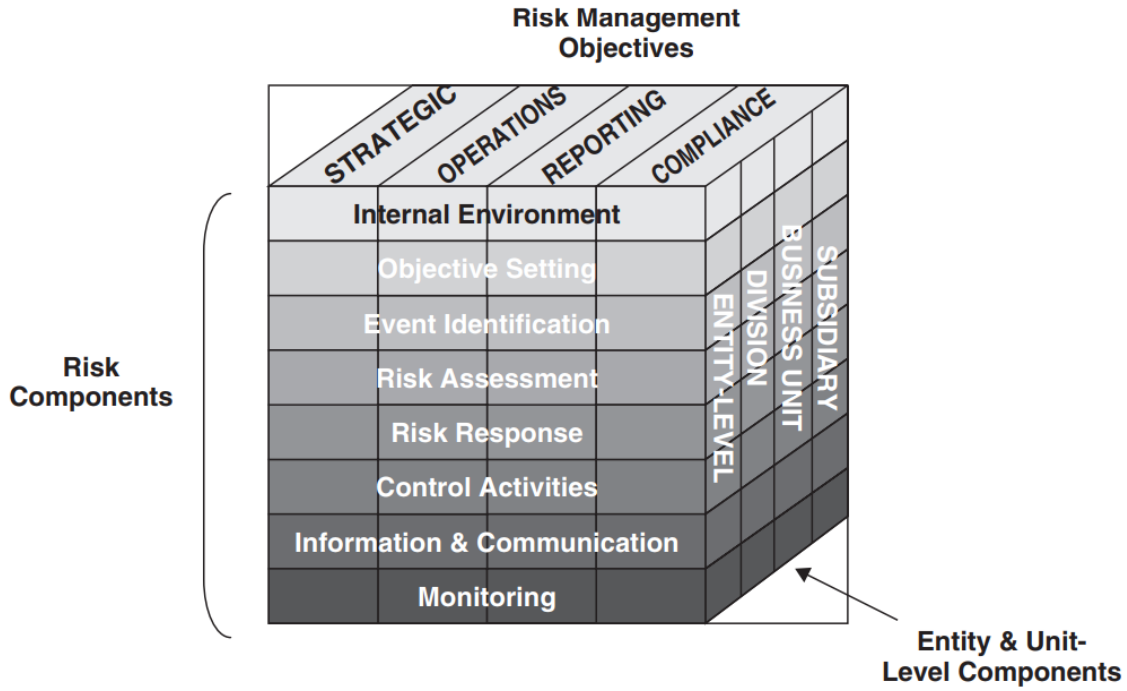

Figure 4. COSO ERM Cube (Moeller, 2007).

The COSO Enterprise Risk Management framework can be represented by a three-dimensional cube as shown above in figure 5. The top of the cube represents the risk management objectives. These objectives are identified by the enterprise's strategy, operations, reporting, and compliance objectives. The right side of the cube represents the multiple hierarchical levels of the enterprise from organizational level down to the individual business unit. The front of the cube represents the seven components of the internal environment. Each side of the cube must work together to complete the risk management objectives.

Internal Environment

The internal environment is considered the cornerstone to the COSO ERM framework. It is the foundation that sets the tone for all other parts of the COSO ERM model. The internal environment determines how the enterprise will develop strategy and objectives. The internal environment influences how risk-related business activities are structured, and how risks are identified and acted upon (Moeller, 2007). The internal environment consists of several foundational elements. These elements include:

- Risk management philosophy – This refers to the enterprises unique attitude and belief system (Moeller, 2007). The risk management philosophy should be considered in all activities to ensure alignment with goals and objectives.
- Risk appetite – This refers to the amount of risk the enterprise is willing to accept (Moeller, 2007). Risk appetite can be measured in either quantitative or qualitative measures or both. All management levels should understand the enterprise's risk appetite.
- Board of directors' attitudes – The board of directors should be willing to work closely with management and various stakeholders. When senior directors have a positive attitude, they can help answer challenging questions that the enterprise risk management team may have. When the board of directors have a positive attitude, this can

help boost employee morale and guide the enterprise risk management process.

- Integrity and ethical values – This refers to the enterprises unique corporate culture. Integrity and ethical values help guide the enterprise at all levels (Moeller, 2007). Ethical values provide the enterprise with the direction needed to help manage risk. The enterprises mission statement and code of conduct are key elements that affect the enterprises integrity and ethical values (Moeller, 2007).
- Commitment to competence – This refers to the knowledge and skills that are necessary to perform scheduled tasks (Moeller, 2007). Management will develop strategies and assign stakeholders to perform them. An enterprise with a strong commitment to competence will do whatever is necessary to achieve its goals (Moeller, 2007).
- Organizational Structure – This refers to responsibility, reporting, and lines of authority within the enterprise (Moeller, 2007). A poor organizational structure will make it difficult for the team to complete tasks and execute various risk management activities. A strong organizational structure will help the enterprise thrive and complete objectives.
- Assignments of authority – This refers to how authority and responsibility are delegated within an enterprise (Moeller, 2007). By

eliminating middle management levels organizational structures this can encourage employees to operate more efficiently, have better customer service, and be more creative. A code of conduct is a key element to assigning authority and responsibility. A code of conduct should be written out and communicated to all stakeholders. All stakeholders that receive the code should acknowledge, agree, and comply with the code.

- Human resource standards – This refers to the practices regarding employee hiring, training, disciplining, and all other actions regarding what is favored, tolerated, or forbidden (Moeller, 2007). A set of standards should be addressed and enforced to all stakeholders. Disciplinary action should be taken when employees are not following the rules.

These are all necessary components to create an effective internal environment. The internal environment has two major functions to support the organization's risk management philosophy and to determine the enterprises risk appetite (Moeller, 2007). Risk appetite helps the enterprise to determine if it will accept some risk and reject others based on the likelihood and impact. A risk appetite map is a tool to help the enterprise decide on the range it is willing to accept (Moeller,2007).

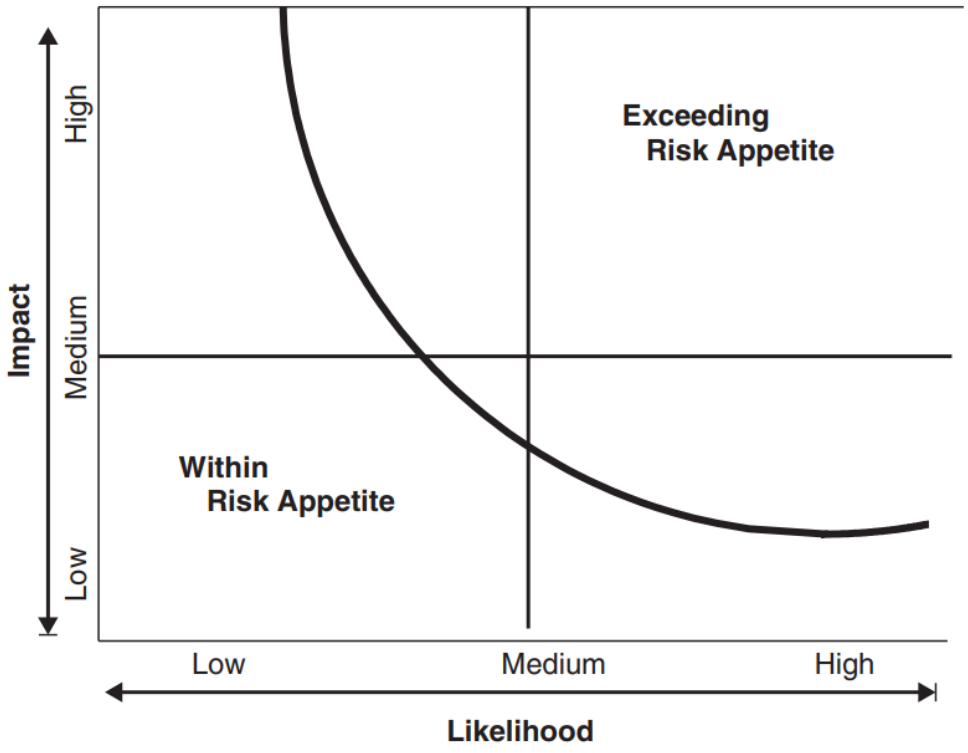

Figure 5. Risk Appetite Map (Moeller, 2007).

Objective Setting

An enterprise should establish a series of strategic objectives to help guide operations (Moeller,2007). These objectives can be considered as the enterprise's goals. After setting strategic objectives the enterprise will develop operational, reporting, and compliance objectives (Moeller, 2007). The COSO framework suggests that goal setting should align with the mission statement, vision, and core values of the enterprise. This ensures that objectives reflect the overall direction that the enterprise wishes to pursue.

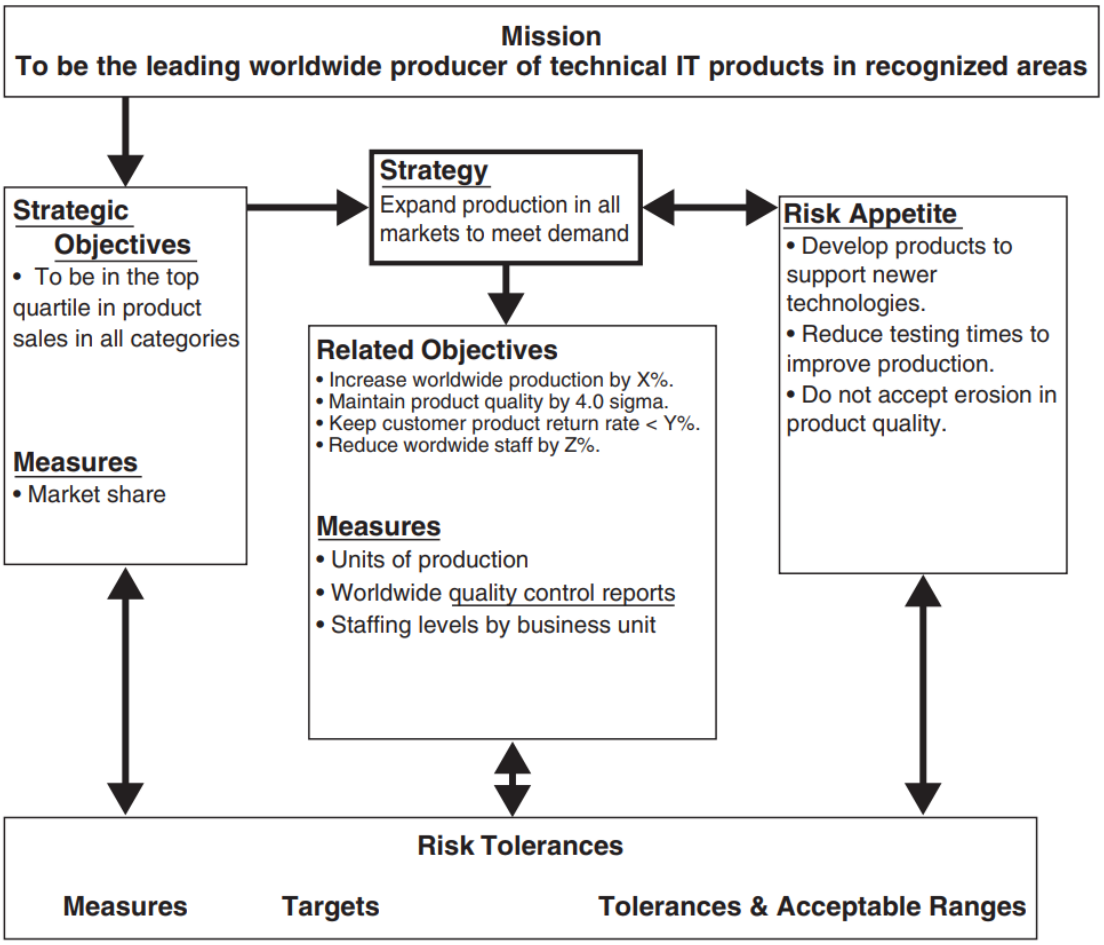

Figure 6. COSO ERM Risk Objective Setting Components (Moeller,2007).

To manage and control risks effectively an enterprise must first set objectives and define its risk tolerance (Moeller, 2007). The table above is an example that represents objective setting components in a fictitious company. The COSO ERM framework can help an enterprise to develop strategic objectives that support the goals related to its mission statement. The COSO ERM helps to create a strategy that defines objectives and the risk appetite

(Moeller, 2007). The enterprise must set objectives and define the risk tolerance, to effectively manage and control risks at all levels.

Event Identification

Events are incidents both external and internal to the enterprise, which affect the achievement of its objectives (Moeller, 2007). Events can be positive, negative, or both. There are many external events that need to be monitored to help the enterprise achieve its objectives (Moeller, 2007). External events can have a major impact on enterprises. Whether accidental, malicious, or environmental, events can be classified as incidents (Moeller, 2007). Impact from events may cause damage to office facilities, limit availability, and even cause power outages.

Risk Identification Tools

Risk identification tools can help identify both risks and potential opportunities. The COSO ERM techniques can help an enterprise establish a formal process to review risks and take action to remediate them. The COSO ERM framework recommends taking inventories to help keep track of these events. Workshops are another risk identification tool that can be used to discuss potential risk factors. Workshops help to create action plans so that the enterprise can correct potential risks (Moeller, 2007). Interviews, questionnaires, and surveys are also effective tools to gather information regarding risk events.

An enterprise can gather information from a wide variety of sources including customer satisfaction letters and even exit interviews from employees (Moeller, 2007).

Process flow analysis is another tool an enterprise may use to review processes (Moeller, 2007). This involves drawing diagrams of business processes to help identify potential risk events (Moeller, 2007). Flow diagrams show internal controls, these visual aids can help an enterprise to identify control effectiveness (Moeller, 2007). Software tools dashboards can also be used to monitor organizational performance. Dashboards show real time graphical representation of the systems health. The key to successful risk identification tools is to have a good analysis of data and a strategic plan of action.

Risk Assessment

The risk assessment can be considered as the core of the COSO ERM framework. The risk assessment helps the enterprise to understand its potential risks and how the risk event may impact the enterprises objectives (Moeller, 2007). The risk assessment classifies risk events based on likelihood of occurrence and potential impact. Management should consider both inherent and residual risks during the assessment (Moeller, 2007). Inherent risk may be considered as waste due to the activity (Moeller, 2007). Factors that can affect inherent risk are budget, management, and business activities (Moeller, 2007).

Residual risk may be considered as the risk that is left over after responding to the risk event (Moeller, 2007).

Likelihood is the probability of a risk event. It measures risk by classifying it as a high, medium, or low likelihood of occurrence. To estimate the impact of a potential risk event, an enterprise can use estimates such as the cost to replace hardware or software equipment. Both qualitative and quantitative measures can be used to analyze the likelihood and impact of a risk event (Moeller, 2007). Once the identified risks have been assessed they can be ranked based on likelihood and impact level (Moeller, 2007).

Table 2. On the next page illustrates how a series of risks can be evaluated and assigned values. Risks are identified and assigned by relevant rankings. The idea of this analysis is to identify high-impact and high-likelihood risks for the enterprise. These are the most critical events for management to assess. The view of potential risks should be analyzed on a total organizational level. This requires a team of stakeholders to work together in a top-down approach. The risk assessment is used to evaluate potential risk and to consider the likelihood and impact (Moeller, 2007). The next step is to respond to the various identified risks.

Table 2. Risk Likelihood and Impact Mapping Example (Moeller, 2007).

Risk Name	Risk Definition	Impact	Likelihood	Risk Ranking
1. Accounting risk	Failure to record sales activity accurately and timely may misstate financial reports.	**High**: Accounting errors may have a material impact on financial and operational information.	**Medium**: Despite strong procedures, newer personnel in various locations may make errors.	8
2. Legal risk	Failure to understand current and changing laws and regulations may result in inability to comply with laws in multiple operation jurisdictions.	**Medium**: Even small, technical violations of most regulations should not have a material effect on operations.	**High**: With worldwide operations in multiple jurisdictions, violations—if only technical—can occur.	7
3. Segregation of duties	Inadequately controlled segregation of duties may allow employees to process unauthorized, fraudulent transactions.	**High**: Fraudulent operations could have significant impacts on company operations.	**Low**: Ongoing internal audits and stronger management control practices should prevent such control breakdown events.	5

Risk Response

Management is responsible to review risk likelihood, potential impact, and to consider the associated costs and benefits (Moeller, 2007). By doing so management can develop appropriate risk response strategies (Moeller, 2007). There are four key risk response strategies, avoid, reduce, share, and accept. Avoidance refers to walking away from the risk (Moeller, 2007). Reduction is the action taken to reduce the risk. Sharing, can be considered as purchasing insurance or transferring risk to a third party (Moeller, 2007). A sharing method is a joint venture agreement where another party accepts some of the risk. Acceptance in when the enterprise decides to take no action.

An enterprise should look at the risk's likelihood and impact before deciding whether to accept that risk (Moeller, 2007). It is common for an enterprise to assume a risk that will never happen, this may leave the enterprise vulnerable. Management must consider the cost vs. benefits of each risk response strategy in alignment with its unique risk appetite (Moeller, 2007). The enterprise should go back, and review established risk objectives and the tolerance ranges for each objective. This encourages stakeholders to understand how various risks align with risk tolerances.

Risk response planning requires input from management and approval from the board of directors (Moeller, 2007). Alternative risk response strategies should be weighed out (Moeller, 2007). Other factors that influence risk response include time, cost, and project planning. Table 3. below shows a sample that

management can use to consider alternatives and to develop effective responses (Moeller, 2007). For each identified risk, management will estimate the risk likelihood and impact. In the example, the team estimates the likelihood that a competitor will be first to market (Moeller, 2007). All risks listed in the worksheet should be measured against the same impact factors (Moeller, 2007). This ensures standardization and the ability to analyze risk across the enterprise in a consistent manner.

Table 3. Risk Response Planning Worksheet (Moeller, 2007).

Risks	Inherent Risk		Risk Response Alternatives		Residiual Risk	
	Likelihood	Impact on Revenue			Likelihood	Impact on Revenue
1. Competitor reaches market first with new product under development.	40%	($5,000,000)	A. Accept	Provide additional resources to speed up R&D to complete new products.	30%	($25,000) less profit due to development costs.
			B. Avoid	Take no specific action. Keep current product offerings in place.	10%	Estimated 10% reduction in profits for line each year.
			C. Share	Offer incentives to current customers to encourage use of current product versions.	20%	
			D. Reduce	Lower prices on current product offerings to discourage conversions to new versions.	40%	
2. Identified Risk # 2	X%	$$	A. Accept B. Avoid C. Share D. Reduce			

Risks should be summarized into a risk portfolio (Moeller, 2007). This analysis should be performed in a consistent manner across the entire enterprise. Senior management and the board of directors can use a risk portfolio to assess the overall impacts of potential risks. The risk portfolio helps management and the board of directors to develop risk response priorities and to better understand the unique risks that the enterprise is facing (Moeller, 2007). The risk portfolio shows the various identified risks, the frequency of occurrence, and the impact dollar value it may have on the enterprise (Moeller, 2007). Figure 7. Is a sample of the risk portfolio.

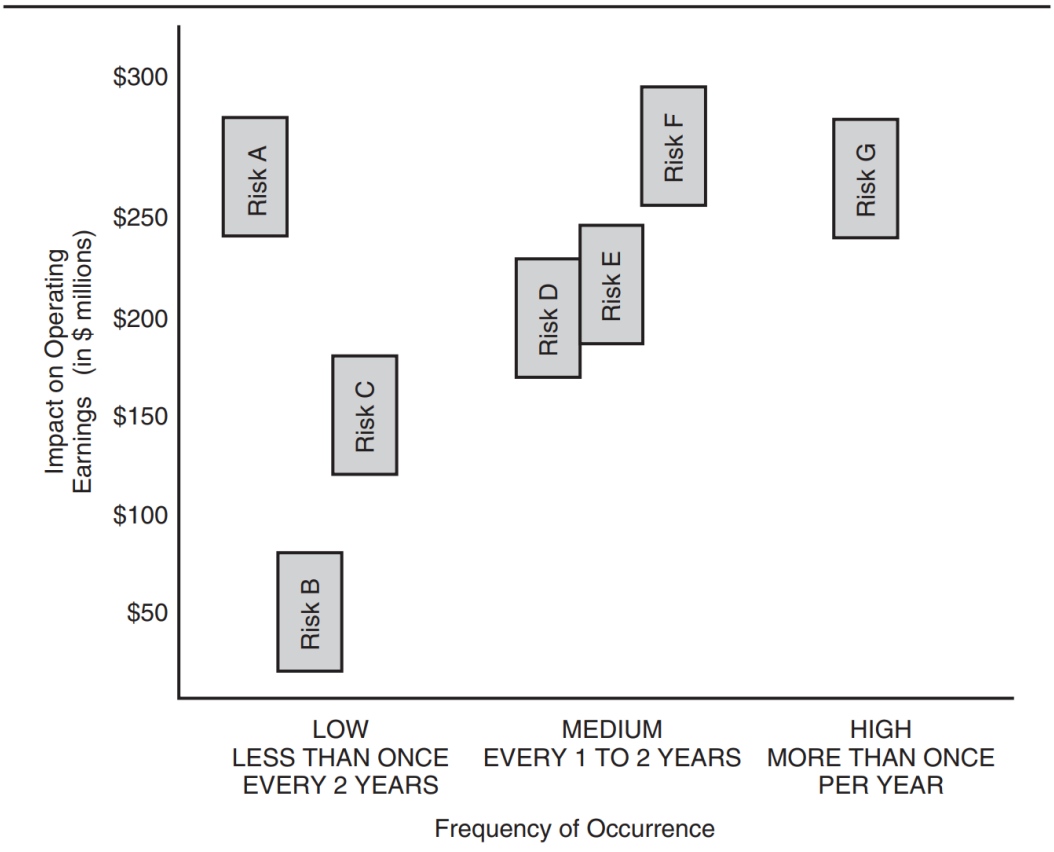

Figure 7. Risk Portfolio Example (Moeller, 2007).

Control Activities

Control activities can be defined as the policies and procedures that are necessary to ensure that risk responses are completed (Moeller, 2007). After identifying risks, completing the risk assessment, and choosing the risk responses, the next step is to monitor risk. The COSO ERM framework uses a four-step monitoring process:

- Step 1. Ensure that the risk management team, board of directors, and upper management fully understand the identified risks. This can be accomplished through control procedures that are used to monitor and control risks (Moeller, 2007).
- Step 2. Create a testing environment to identify if the controls are working correctly (Moeller, 2007). Each control should be thoroughly tested before bringing it into production.
- Step 3. Perform control procedures to determine if monitoring is operating effectively (Moeller, 2007).
- Step 4. Adjust when necessary to improve monitoring (Moeller, 2007).

Information and Communication

The information and communication component links together each of the other components (Moeller, 2007). Information and communication show how

information flows across the COSO ERM framework (Moeller, 2007). The communication flow provides a risk response and uses the risk portfolio data to assist in activity control. In the COSO ERM framework, it is important to organize and establish strong internal communication so that all stakeholders understand the risk management process (Moeller, 2007).

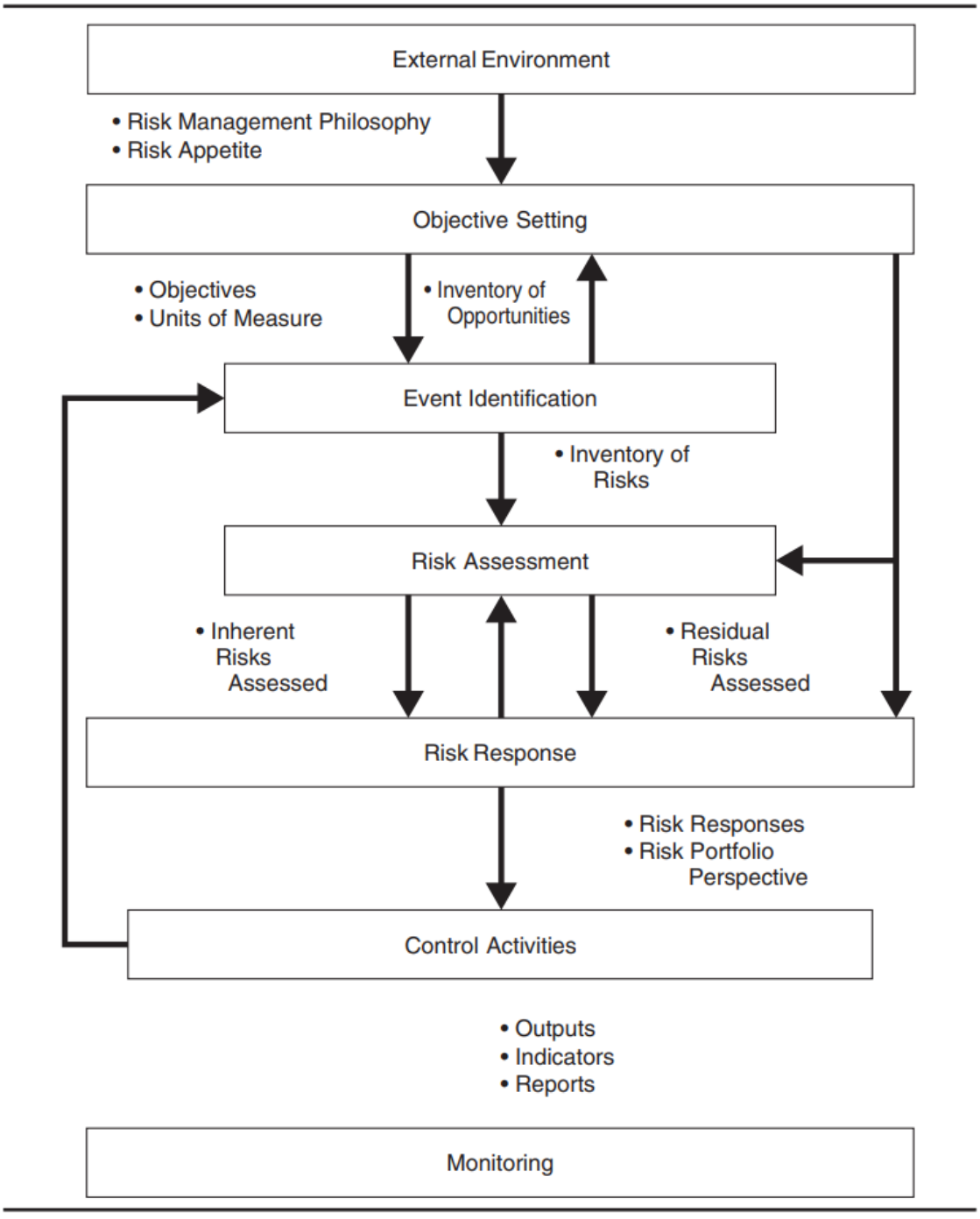

Figure 8. Information and Communication Flows Across ERM Components (Moeller,2007).

Monitoring

Monitoring determines the health of the system. Monitoring shows whether the installed components are continuing to work effectively (Moeller, 2007). Monitoring tools such as a dashboard can provide management with real-time updates to ensure proper functionality of controls. Controls should be monitored on a day-to-day basis, and trending data can provide vital information on the health and functionality of the internal systems. Automatic updates can send warnings when necessary. A network protocol analyzer such as Wire Shark can provide network administrators with a live capture analysis. Wire Shark can be used to capture network traffic; this information can be used to troubleshoot various network issues. Monitoring should include ongoing reviews of the overall ERM process (Moeller, 2007).

Effective monitoring should include ongoing reporting. Reporting may include statistical trends and comparisons with prior periods. The enterprise should have a designated qualified reviewer to evaluate monitoring. An internal audit organization may be helpful to perform reviews (Moeller, 2007). Monitoring allows the enterprise to assess how well the enterprise risk management plan is functioning. Some monitoring tools according to the COSO ERM include:

- Process flow charting – Flow charts are used to document the ERM process. Flow charts can help in completing an ERM review. This requires looking at the documentation prepared for a process, determining if the process documentation is correct given current

conditions, and updating the process flowcharts as appropriate (Moeller, 2007). This can help determine if the identified risks are still valid and if they have been identified appropriately.

- Review of risk and control – An ERM process often results in a large volume of guidance materials, documented procedures, and report formats (Moeller, 2007). It is important to review and check for effectiveness and functionality of controls. The ERM team can perform these reviews periodically.
- Benchmarking – is the process of looking at the ERM functions in other enterprises to assess their operations and to develop an approach based on the best practices of others (Moeller, 2007). The information about how other enterprises have solved similar problems can provide insight and be valuable.
- Questionnaires – can be used to gather anonymous information from both employees and customers. This can be a great tool to gather specific information.

Strategic Objectives

Every organization should have a strategic vision (Moeller, 2007). Strategic objectives help to guide the COSO ERM process. Strategic objectives should be communicated across all levels of the enterprise. Strategic risks are related to all components on the COSO ERM cube. Strategic-level risks are key

factors in assessing the effectiveness of the enterprises risk management plan (Moeller, 2007).

Operations-Level Risks

Operational risks are considered as a broad risk category that has a high exposure level. Operational risks can impact any area of organization operations (Moeller, 2007). An enterprise should document operational risks along with risk likelihood estimates. An enterprise may choose to analyze high level operational risks and have an immediate stakeholder to describe its risks. A survey with follow-up questions can be addressed to the individual stakeholders to develop a set of operational risks across the enterprise. Surveys can help gather valuable information regarding operational level risks (Moeller, 2007).

Reporting Risks

Accurate reporting is critical for an enterprise's success. Inaccurate corporate financial reporting can cause a host of problems for the enterprise and even cause it to go out of business (Moeller, 2007). An enterprise may face risks related to inaccurate reporting on each business unit level of the enterprise. Strong internal controls, policies, ethics, and values should all be considered to reduce the risk of these reporting errors. Inaccurate financial reporting is a major concern throughout all levels of the enterprise (Moeller, 2007).

Compliance

Enterprises face a wide range of regulatory rules. If regulatory rules are neglected, the enterprise may be subjected to violations and fines. Compliance risks relate to violations of laws, regulations, and internal policies (SCCE, 2020). Such compliance violations could result in financial liability, penalties, or other negative effects (SCCE, 2020). A regulatory risk report can help determine the status of regulatory risks as well as communicate these risks to board members and managers. The goal is to keep the enterprise within compliance with all relevant laws and regulations.

ERM Entity and Unit-Level Risks

The right side of the COSO ERM cube represents risks across all organizational levels (Moeller, 2007). This side of the COSO ERM cube shows that risks should be considered throughout all levels of the organization. Management is responsible for defining its organizational-level risks in detail (Moeller, 2007). Depending on the size of the enterprise, risk responsibility should be divided among various stakeholders (Moeller, 2007). These risks can be managed by a designated ERM team.

Business Unit Level Risks

Risks may occur at all levels of an enterprise. Whether it be an organizational risk that affects many departments or a much smaller risk that

affects a specific task. Risks must be considered in every unit and should be controlled all the way down to the smallest unit (Moeller, 2007). A push-down process can be used to outline risk concerns. Management can issue surveys by passing them down to each unit of the enterprise. This exercise can help identify significant risks throughout all levels of the enterprise.

CHAPTER FOUR

CASE STUDY REVIEW: ANALYSIS AND FINDINGS

To answer the research questions in this project a real-life example was studied. This case study illustrates a successful implementation of enterprise risk management (ERM) at a Moroccan financial institution. The ERM process was based on the COSO ERM framework. For privacy reasons, the company will be referred to as “Financial Institution” (Finst). The “Finst” board of directors first deployed COSO ERM in the Portfolio Management Department as a pilot project. The Portfolio Management Department (PMD) faced several different risks including market risks, credit risks, liquidity risks, operational risks, and strategic risks.

The case study applied the COSO ERM framework to complete risk management objectives. A top-down approach was utilized to align the objectives with the enterprise’s mission statement and core values. The enterprise was able to manage both strategic and organizational risks by using the COSO ERM framework. The financial institution “Finst” also chose to transfer investment funds to reduce financial risks. By implementing controls and utilizing the COSO ERM tools it was able to successfully manage risks and improve internal operations.

The COSO ERM framework helps SMEs to identify both internal and external threats including cybersecurity risks. By methodically identifying threats,

developing a risk appetite, assessing, and monitoring the environment. Small and medium size enterprises can effectively manage risks. The COSO ERM framework emphasizes information and communication flow, this is a key element that helps SMEs to develop a well devised risk management plan. Frameworks developed for large corporations often require employees to have specialized knowledge and skills, making them an inadequate choice for SMEs. The COSO ERM takes several steps to cultivate a strong internal foundation, this is a fundamental step for SMEs to develop an enterprise risk management awareness.

Table 4. PMD Risks (Benabbou, 2013)

Ref	Risk	Category	Effects	Causes	Means to treat risks	Impact	Likelihood
1	Inappropriate Timing	Operational	Loss of investment opportunity	Delay in decision making or in taking to account an information	Facilitating communication and rapid decision making when faced with important market information in the specified interval risk tolerance.	3	4
2	Inappropriate reaction to rumors	Operational	Underestimate or overestimate an investment opportunity	Unreliable sources information and using incorrect information	Authenticate information and their sources before making a trading decision Create a watch unit for collecting and communicating relevant information	3	4
3	The lack of information or the overflow of information	Operational	Asset managers concurrently execute the same transaction at different price ranges	Lack of coordination between asset mangers and information is not communicated instantly to all asset managers	Centralize all data in a single database and instantly share the portfolio situation with all asset managers within the same interface	3	2
4	Cash does not cover a transaction	Operational	Overdue in payment of transactions	Operation missed, portfolio and cash situations are not updated	Apply procedures and plan cash flow	3	2
5	Exceed accepted tolerance risks	Operational	Exceed regulatory or strategic thresholds	Incorrect or missing data Files are not updated	Apply procedures and centralize all data in a single database	5	2
37	Non compliance with legal and regulatory requirements	Strategic / operational	Sanctions	Absence of control and non application of procedures	Implementation of an integrated portfolio management software with automatic control system	7	1
38	Computer system Failures	Strategic / operational	Momentary suspension of operation Loss of data Loss of investment opportunity	Absence of backup and recovery systems	Implementation of portfolio management software	7	5
39	Inability to respond appropriately to market uncertainty	Strategic / operational	Loss of investment opportunity Loss of portfolio performance	Lack of training or information	Organize training and frequent meetings to explain market uncertainty Create a watch unit for collecting and communicating relevant information	6	6
40	Inadequate Business Activity Plan (BPA)	Strategic / operational	Interruption of activity in the case of a disaster	BPA not updated	Keep in line with BPA update frequency	7	1

The goal of the COSO ERM framework is to identify, assess, and monitor risks and opportunities (Benabbou, 2013). Several risk workshops were conducted to prepare the internal environment. Workshops are a risk identification tool that can be used to discuss potential risk factors. These risks can come from both internal and external events. The result from these workshops would be action plans to correct the potential risks (Moeller, 2007). The workshops promote collaboration and strengthen communication from the PMD stakeholders. Workshops can help various stakeholders develop an ERM dialogue and develop a better understanding of risks.

To launch the ERM project “Finst” first established goals that aligned with the enterprise’s mission statement and strategic objectives. Next a project team was created to conduct the COSO ERM objectives. The project team was responsible for identifying risks, prioritizing responses, monitoring, and ensuring compliance with rules and regulations. Meetings ensured comprehension of the internal environment and they helped to strengthen communication and collaboration between various stakeholders. The project team consisted of:

- The Chief of the Portfolio Management Department.
- The Risk Manager – who is the project chief (Benabbou, 2013).
- A Fixed Income Securities manager (Benabbou, 2013).
- Equities Manager – who was the internal controller of the middle office (Benabbou, 2013).
- Internal Controller of the middle office (Benabbou, 2013).

An initial meeting, held by the risk manager aimed to explain the COSO ERM objectives to the project stakeholders. Steps and guidelines were created, a code of conduct was followed, and strategic objectives to manage risks were determined. PMD employees were then advised by board members on how to deal with uncertainty. The project was scheduled to be completed within six months.

Establish Objectives and Internal Environment

The analysis of an internal environment helps to establish the enterprises risk culture (Benabbou, 2013). Project stakeholders must first understand risk and the enterprises unique objectives before they can begin to identify risks. The PMD department aligned ethical values, objectives, and a code of conduct with the mission of the enterprise. After assessing the internal environment and understanding the organization's unique objectives, the next step was to define risk tolerance. This involves measuring the acceptable level of variation according to the organization's objectives and risk appetite. The risk appetite was then identified by choosing to either accept, avoid, reduce, or transfer the risk.

Risk Identification and Assessment

After defining the internal environment and setting strategic objectives, the enterprise can then identify internal and external risks and opportunities

(Benabbou, 2013). An initial brainstorming workshop was conducted to identify operational risks based on impact and likelihood. Brainstorming workshops allow collaboration and communication from board members, managers, and lower-level employees. This collaboration can help to identify risks and answer questions that ERM team may have. “Finst” then used two more tools to identify other potential risks. This included building PMD functional diagrams and sharing ideas through face-to-face discussions. The diagrams help to describe the PMD functions and show hierarchical perspectives.

PMD functional diagrams helped to identify many operational risks. Several risks were also identified by interviewing the risk owners. Risk owners often have important insight for the ERM team. They can provide specialized knowledge, insight, and a better understanding of assets. This knowledge can be shared through face-to-face discussions and or surveys. Risk identification is a continuous process that should be updated periodically. The COSO ERM process requires day-to-day monitoring and review to test control effectiveness. This is a continuous process that should be repeated throughout the project development life cycle.

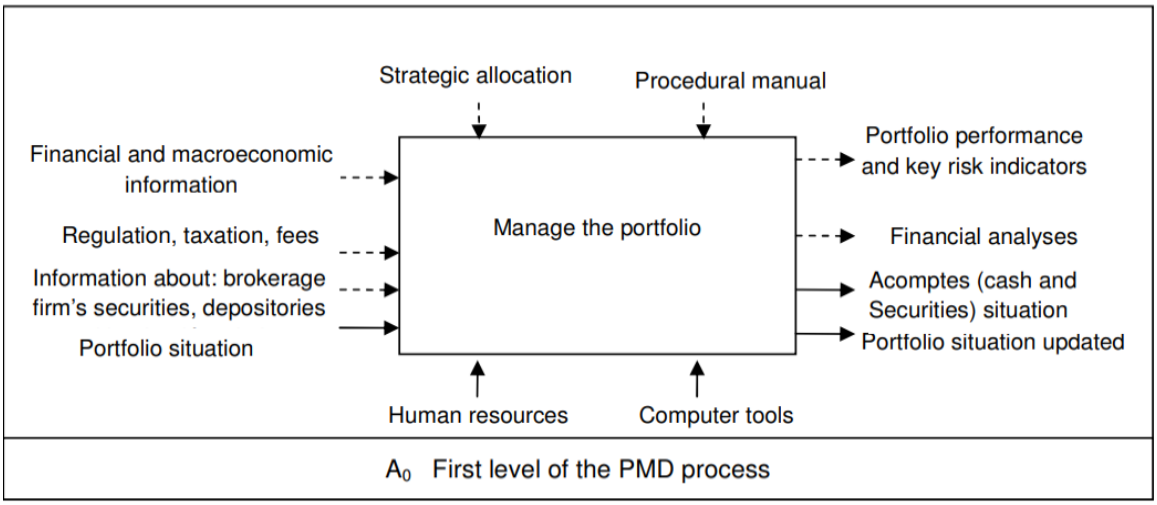

Figure 9. First Level of The PMD Process (Benabbou, 2013).

Each identified risk was assessed based on the likelihood and impact of the enterprise's objectives (Benabbou, 2013). "Finst" used a qualitative approach to identify strategic and operational risks. The project team created ordinal measurement scales to represent risks and establish the most imminent dangers to the enterprise. The ordinal levels were based on severity, the most fatal impact level was rated at a seven while low-impact events were considered a two on the ordinal scale. Seven levels were identified to rate impact ranging from fatal to insightful.

Table 5. Likelihood and Impact Measurement Scales (Benabbou, 2013).

Level	Kelihood	Level	Impact
7	Once a week	7 : Fatal	Events call into question the achievement of several or all key institution objectives
6	Once a fortnight	6 : Major	Events call into question the achievement of several or all key departmental objectives but without affecting all institution objectives
5	Once a month	5 : Critical	Events call into question the achievement more then one department objectives but without affecting all institution objectives
4	Once a quarter	4 : High	Events call into question one departmental objective or the performance of a service in the department
3	Once a year	3 : Moderate	Events partially call into question service process or performance
2	Between 1 and 5	2 : LOW	Near neutral events across the service
1	> 5 years	1 : Insignifiant	Near neutral events across desks of the service

To measure impact of risks on the Portfolio Management Department's objectives, the enterprise used a participative focus group (Benabbou, 2013). The ERM project team identified several risks (due to confidentiality, only a portion of the identified risk are shared). Most of the overall risks identified were operational risks, and several of these risks were associated with the misunderstanding of existing controls (Benabbou, 2013).

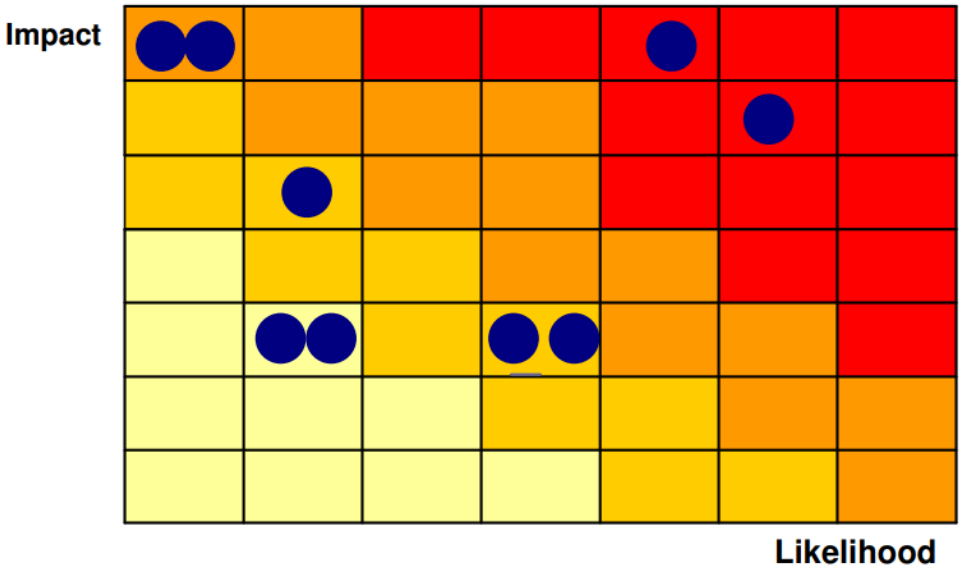

Figure 10. Risk Map (Benabbou, 2013).

Once net risks had been assessed, a risk map was then produced to help the enterprise decide on the acceptable range of risk appetite. The risk map measures risk events based on likelihood and impact. Four risk response strategies were created: critical, high, medium, and low. The remediation and monitoring requirements depend on risk exposure levels (Benabbou, 2013). Risks with the highest likelihood and impact level should be prioritized first as these are the most imminent dangers for the enterprise.

Risk Treatment and Control

Depending on the severity of each risk, an appropriate risk response strategy was chosen (Benabbou, 2013). The goal of risk response strategy is to reduce risks to acceptable levels within the enterprises risk appetite. The risk

owner (asset manager) is responsible for deciding on the appropriate strategic treatment after management signs off on the plan. The Portfolio Management Department had financial risks that were managed by the risk owner under the appropriate risk tolerance. The risk reduction strategies that “Finst” used were to measure likelihood, impact levels, and then apply corrective measures.

To reduce the critical risk of the failure of computer systems the likelihood and impact estimates were calculated then “Finst” used a Portfolio Management Software to remediate the risk (Benabbou, 2013). To reduce the fatal and rare risk of inadequate Business Activity Plan (BAP) the Portfolio Management Department decided to update the plan annually to reduce the inactivity time in case of a catastrophic event (Benabbou, 2013).

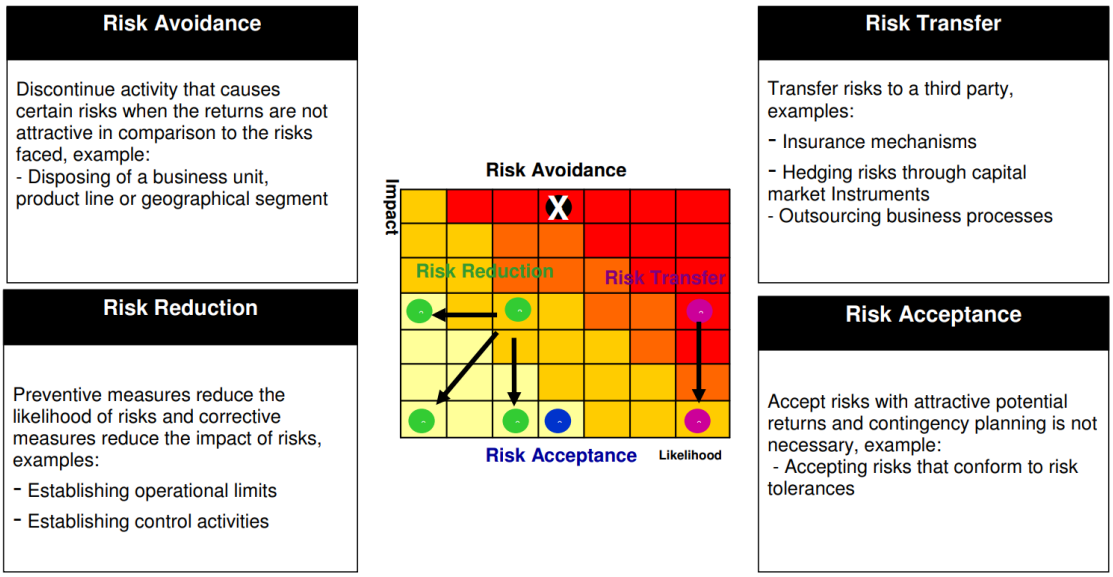

Figure 11. Risk Response Strategies (Benabbou, 2013).

Risk Monitoring and Reporting

Enterprise risk management is a continuous process that requires constant monitoring. To address this, “Finst” created a risk management service to monitor remediation strategies, risks, and potential changes in exposure (Benabbou, 2013). The risk register was then updated, and a dashboard was set up to report results (Benabbou, 2013). The dashboard was set up to monitor the performance according to the guidance set by board members.

Case Study: Final Note

The COSO ERM framework helped the enterprise to deal with uncertainty and it allowed decision-makers to achieve the enterprise’s objectives (Benabbou, 2013). This case study demonstrates the importance of risk management implementation in SMEs. It illustrates how the ERM implementation process contributes to increasing operational risk awareness and understanding strategic objectives from the board members down to individual employees (Benabbou, 2013). The case study shows how “Finst” successfully made strategic decisions and increased operational efficiency. By implementing controls and completing objectives, the enterprise was able to reduce the likelihood and impact of risk occurrence. Implementation of COSO ERM had many benefits:

- Execution of strategic objectives.
- Reduced impact and likelihood of computer system risks.

- Used risk management service to monitor controls and system health.
- Allowed for the review of control process to reduce the likelihood of strategic, financial, and operational risks (Benabbou, 2013).
- Allowed for the transfer of investment funds to reduce financial risks.
- Update the business activity plan (BAP) to reduce response time in case of catastrophic events.

Table 6. Summary of Case Study and Research Questions

Question 1: What are risk identification strategies which do not overstrain SMEs limited resources?	Question 2: How may risk analysis be performed effectively in SMEs?	Question 3: How does the SMEs risk management system change over time?	Question 4: What are risk analysis techniques that are effective for SMEs with limited resources?
Use brainstorming workshops to identify risks. Use face-to-face discussions to share ideas and provide feedback. Use a qualitative top-down approach with stakeholders to identify organizational and strategic risks. Use functional diagrams and interview with risk owners to understand and identify risks.	Consider risks in every activity from the organizational level to business unit. Hold meetings with PMD stakeholders to gain insight. Understand the organizations risk culture and objectives. Conduct a risk risk assessment. Board members and management involvement throughout the ERM process. Understand and define organizational objectives. Define risk tolerance, develop risk response, and control activities.	Once ERM was successful in PMD it was expanded throughout the enterprise. Continuous monitoring, assessment, and updating is critical throughout the enterprise life cycle. Routine maintenance is required, and the risk register should be updated periodically. Threats and risks are always changing and evolving, so they must be revisited. Controls should be checked for effectiveness and risks should be reevaluated.	Define risk tolerance by specifying risk appetite. Measure financial risk tolerance based on a benchmark. Use PMD Risk Map to calculate likelihood and impact. Update PMD risk table to show current risks. Use likelihood to measure the impact of risks. Use portfolio management software to monitor and receive feedback.

CHAPTER FIVE:

DISCUSSION, RECOMMENDATIONS, LIMITATIONS OF PROJECT, CONCLUSION, AND AREAS OF FURTHER STUDY

Discussion

The research questions were: 1. What are risk identification strategies which do not overstain SMEs' limited resources? 2. How may risk analysis be performed effectively in SMEs? 3. How does the SME risk management system change over time? 4. What are the most effective risk analysis techniques and strategies for SMEs with limited resources?

The case study identified unique challenges that SMEs faced and provided recommendations. The results were: 1. Use brainstorming workshops to identify risks. Use face-to-face discussions to share ideas and provide feedback. Use a qualitative top-down approach with stakeholders to identify organizational and strategic risks. Use functional diagrams and interviews with risk owners to understand and identify risks. 2. Consider risks in every activity from organizational level to business unit. Hold meetings with stakeholders to gain insight. Understand the enterprise's risk culture and objectives. Conduct a risk assessment. Board members and management involvement throughout the enterprise risk management process. Understand and define organizational objectives. Define risk tolerance, develop a risk response, and control activities.

3. Once enterprise risk management was successful in the Project Management Department, it was expanded throughout the enterprise.

Continuous monitoring, assessment, and updating is critical throughout the enterprise life cycle. Routine maintenance is required, and the risk register should be updated on a schedule. Threats and risks are always changing and evolving so they must be revisited. Controls should be checked for effectiveness and risks should be reevaluated. 4. Define risk tolerance by specifying risk appetite. Measure financial risk tolerance based on the benchmark. Use a Risk Map to calculate likelihood and impact. Update the risk table to show current risks. Use portfolio management software to monitor and receive feedback.

Enterprise risk management can directly influence the performance and execution of strategic objectives by helping SMEs deal with uncertainty. This project demonstrates why business owners should use it. The case study showed many benefits to using enterprise risk management, including increased operational risk awareness, a better understanding of strategic objectives, increased efficiency, improved collaboration, and cultural development. Although the benefits to enterprise risk management are apparent, SMEs still face challenges in adopting this approach. Stakeholders are more engaged in managing risk and frameworks and tools are becoming more readily available. These are important trends for SMEs.

The project's objectives are to explore risk management trends and challenges that SMEs currently face and to provide recommendations to business owners, executives, and security professionals in the form of methods and tools to limit threats and minimize the attack surface. Research and

investigation of the case study has helped to achieve the projects objectives. To address issues of inadequate resources, lack of expertise, and understanding the recommendation is to utilize the COSO ERM framework. This also addresses the lack of information because the COSO ERM framework is a free tool that can help structure internal operations. To address the lack of time, adequate planning and allocation of a risk response team should be utilized to ensure that risk management is prioritized throughout the enterprise life cycle. To address the lack of training, an enterprise may choose to develop a culture that embraces learning and facilitates periodic training protocols. Board members and managers must lead by example and actively communicate best practices, update policies, and encourage collaboration among stakeholders. Periodic workshops and meetings are also encouraged to help reinforce proper training protocols.

Recommendations

To utilize a pilot study. Enterprise risk management may be intimidating to business owners and managers due to the complexity of the framework. By first implementing a pilot study, the business owner can deploy enterprise risk management on a smaller scale. Stakeholders can learn the fundamentals of enterprise risk management. By mastering some of the key COSO ERM components before launching ERM across the whole organization. This will save time and money and allow the business to learn as they go.

Embrace change – Business owners must be proactive and dedicate time and effort into managing risk. Threats are constantly evolving, and business owners must adapt to the current landscape. They can do this by prioritizing efforts to secure critical business functions. Reactive security protocols are no longer effective. A proactive and systematic approach allows the enterprise to analyze risk in a consistent manner across the entire enterprise.

Limitations of the Project

There was a shortage of relevant case studies on SMEs applying risk management. Most of the articles are geared towards larger organizations which limited the scope of this project.

Conclusion

Enterprise risk management involves more than just managing risks. It requires careful planning and execution of key objectives based on several risk components across all levels of the organization. The appropriate plan depends on the enterprise and sector. By understanding the benefits of enterprise risk management, the enterprise can develop a top-down strategy that transforms the internal environment by promoting governance and culture. This allows the enterprise to reinforce key behaviors, develop risk identification strategies, and establish responsibility and authority. By developing a strong internal foundation, the enterprise can effectively begin to identify various risks, perform a risk

assessment, develop risk response techniques, monitor, test, and document changes. By using these strategies SMEs can effectively limit threats, manage risks, and reduce the likelihood and impact of unforeseeable events.

Areas of Further Study

The use of artificial intelligence and machine learning to predict risks. The use of alternative frameworks such as the NIST Risk Management Framework (RMF), the ISO 31000, or the COBIT ERM Framework.

REFERENCES

Basset, G., Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2022). 2022 Data breach investigations report. Verizon. Retrieved September 15, 2022, from https://www.verizon.com/business/resources/Ta0f/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Benabbou, L. (2013). Enterprise risk management: A case study of a Moroccan financial institution. Retrieved September 15, 2022, from http://www.ah2st.ma/fse/docpaper/44-22.pdf

Bensaada, I., & Taghezout, N. (June 2019). An enterprise risk management system for smes: innovative design paradigm and risk representation model. *Small Enterprise Research*. Volume 26, Issue 2, 179-206.

Blank, R. & Gallagher, P. (2012). Guide for conducting risk assessments NIST special publication 800-30 revision 1. Retrieved September 12, 2022, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Brustbauer, J. (July 2014). Enterprise risk management in smes: towards a structural model. *Sage Journals*. Volume 34, Issue 1, 70-85.

Chakabva, O., Tengeh, R., & Dubihlela, J. (May, 2021). Factors inhibiting effective risk management in emerging market smes. *Journals of Risk and Financial Management,* Volume 14*,* Issue 6*,* 231.

Ciampa, M. (2017). CompTIA Security+ Guide to Network Security Fundamentals. Retrieved October 15, 2022, from https://www.fpbooks.space/books/1496/1496-comptia-security-guide-to-network-security-fundamentals-(www.tawcer.com).pdf

Ciocoiu, C. N., Prioteasa, A. L., & Colesca, S. E. (June, 2020) Risk management implementation of Romanian smes: a fuzzy approach. *Amfiteatru Economic,* Volume 22, Issue 55*, 726-741.*

Crovini, C., Ossola, G., & Britzelmaier, B. (February, 2021) How to reconsider risk management in smes? An advanced reason and organized literature review. *European Management Journal*, Volume 39, 118-134.

Everson, M. E. A, Chelsey, D., Martens, F. J., Bagin, M., Katz, H., Sylvis, K. T., Perraglia, S.J, Zelnik, K. C., & Grimshaw, M. (2017). Enterprise risk management integrating with strategy and performance executive summary. Retrieved October 16, 2022, from https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Gregory, J. (2022). Only half of small businesses are prepared for cyberattacks. Security Intelligence. Retrieved September 12, 2022, from https://securityintelligence.com/news/only-half-small-businesses-prepared-cyberattacks/

Grondys, K., Slusarczyk, O, & Hussain, H. I. (April 2021). Risk assessment of the sme sector operations during the covid-19 pandemic. *Int J Environ Res Public Health.* Volume 18, Issue 8, 4183.

Gutierrez, S. (2022). Momentive study: Americans shrug at Russia cybersecurity risks. Momentive. Retrieved September 12, 2022, from https://www.momentive.ai/en/blog/momentive-study-russia-cybersecurity-risks/

Heidt, M., Gerlach, J. P., & Buxmann, P. (November 2019). Investigating the security divide between sme and large companies: how sme characteristics influence organizational its security investments. *Information Systems Frontiers.* Volume 21, 1285-1305.

Henschel, T., & Durst, S. (2014). Risk management in Scottish, Chinese, and German small and medium-sized enterprises: a country comparison. *International Council for Small Business.* 1-3.

Insurance Bureau of Canada (2022). Cyber savvy research. Retrieved September 20, 2022, from https://cybersavvycanada.ca/docs/Cyber-Savvy-Research.pdf

Johnson, R. (2019). 60 percent of small companies close within 6 months of being hacked. Cybercrime Magazine. Retrieved October 10, 2022, from https://cybersecurityventures.com/60-percent-of-smallcompanies-close-within-6-months-of-being-hacked/

Krüger, N. A. (January, 2021). The correlation between various demographic variables and risk management: The case of smes in the Sedibeng district. *Journal of Contemporary Management,* Volume 18, Issue 1.

Krüger, N. A., & Meyer, N. (June, 2021). The development of a small and medium-sized business risk management intervention tool. *Journal of Risk and Financial Management,* Volume 14, Issue 7, 310.

Kurpjuhn, T., (March, 2015). The sme security challenge. *Computer Fraud and Security.* Volume 2015, Issue 3, 5-7.

Lima, P. F. D. A, & Verbano, C. (March, 2019). Project risk management implementation in smes: a case study from Italy. *Journal of Technology Management & Innovation.* Volume 14, Issue 1, 0718-2724.

Martins, Y. S., Silva, C.E.S., & Gaudencio, J. H. D. (2021) From theory to practice: a risk management model for SMEs in the context of ISO 9001. *Production, 31,* e20210036.

Moeller, R. R. (2007). COSO Enterprise Risk Management Understanding the New Integrated ERM Framework. Retrieved October 20, 2022, from https://diblokdcma.files.wordpress.com/2009/10/coso-erm.pdf

Quader, F., & Janeja, V. P. (November, 2021). Insights into organizational security readiness: lessons learned from cyber-attack case studies. *Journal of Cybersecurity and Privacy*. Volume 1, Issue 4, 638-659.

Reed, C. (2022). 23 Small business cybersecurity statistics – 2022. Firewall Times. Retrieved October 12, 2022, from https://firewalltimes.com/small-businesscybersecuritystatistics/#:~:text=22%25%20of%20Small%20Business%20Owners,their%20spending%20levels%20the%20same

Joint Task Force (December, 2018). Risk management framework for information systems and organizations a system life cycle approach for security and privacy. NIST Special Publication 800-37 r.2. Retrieved September 21, 2022, from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Sba.gov. (2022). Sba announces inaugural small business cyber summit to take place during national cybersecurity month. SBA U.S. Small Business Administration.

Retrieved October 11, 2022, from https://www.sba.gov/article/2022/sep/21/sba-announces-inaugural-small-business-cyber-summit-take-place-during-national-cybersecurity-month#:~:text=According%20to%20a%20SBA%20survey,not%20know%20where%20to%20begin

Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA). (2020). Compliance risk management: applying the COSO framework. COSO. Retrieved October 20, 2022, from https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf