Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol: 55 Issue: 05:2022
DOI 10.17605/OSF.IO/XTE9B

AN OPERATIONAL RISK MANAGEMENT FOR EFFECTIVE POLICE OPERATION AND MANAGEMENT

N. K. ALBLOOSHI,
Institute of Technology Management and Entrepreneurship,
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian
Tunggal, Melaka, Malaysia
Abu Dhabi Police General Command - Criminal Security Sector - Al Ain Police Directorate - Deputy Director for Police Stations Affairs - Falaj Hazaa Police Station

S. AKMAL*
Faculty of Mechanical and Manufacturing Engineering Technolgy, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian
Tunggal, Melaka, Malaysia. *(Corresponding Author)

ABSTRACT

Due to their position in the Middle East, which are oil-producing nations, civil war, and political unrest, the police face various rates of crime in the United Arab Emirates (UAE). Much effort has been made to decrease police exposure in the UAE to operational risks. Policies have developed up-to-date work facilities and security technologies, which are supported by the government. However, police in the UAE face dilemma regarding operational risk involves poor management of service delivery, lack of sufficient equipment, and insufficient response to problems and oversight functions. This study provides an overview of the methods and potential future directions for risk management and reduction in the UAE's police operations. The study aims to examine the effects of governance, leadership, information technology, risk perception, and compliance with the organisational risk management of the UAE police in Dubai. Data were collected from Dubai Police Sector employees, which collected 435 questionnaires representing 5236 Dubai Police Force total population, and obtained 412 valid questionnaires. After confirming the validity and reliability of the latent variables with confirmatory and exploratory factor analyses, structural equation modelling Analysis of Moment Structures (Smart PLS) was used to test the hypothesis in Structural Equation Modelling (SEM). This study has shown that different operational risk factors significantly affect difference performance outcomes. Results revealed that the compliance, governance and risk awareness showed significant positive relationships with effective operational risk management, while leadership, information technology were rejected. On the other hands, compliance, Governance and Information Technology showed significant relationship with mediating of training, while leadership and risk awareness found not important. The results would also provide a basis for enhancing policing functions in the UAE in an exceedingly dynamic and fast-changing environment through an objective understanding of operational risk management paradigms. Future research could employ a mixed method (quantitative and qualitative) approach to address any problem of knowledge.

Keywords: UAE, governance, leadership, information technology, risk perception, compliance, organisational risk management,

1. Introduction

The police are a significant and a civil law enforcement agency in the world that is important to the safety of a nation. In the United Arab Emirates (UAE), the Police force faces various crimes due to the country's position in the Middle East, bordered by oil-producing nations, civil war, and political instability. The UAE's economic development, political stability, and business environment have attracted an influx of people and international capital and people of different nationalities. However, owing to its location and open-minded business regulations and trade' affiliations with other Gulf countries, east Africa, and Southeast Asia, and its expanding trade with Balkan states, the UAE has the potential to be a major channel for money laundering (citation), trafficking (citation), fraud (citation), and all sorts of crimes. Additionally, its closeness to Afghanistan, which makes it an opium hub, further exposes the country to greater organised crime and terrorism (citation). This situation exposes its security agencies to a hazardous encounter involving illicit criminal activities. This gives rise to police risk exposure and liabilities, which is a serious concern to the government, public and the police officers on duty from the crimes due to these shady activities (citation).

The criminal are attracted to the UAE due to the generous business atmosphere as a suitable place to perpetrate illegal activities. Furthermore, the UAE has an unconventional maritime infrastructure, which comprises nearly 15 seaports that help facilitate trade on the local, regional and international level (citation). There are also wide-ranging international air networks that are within the UAE, with roughly 66 airlines offering passenger and cargo services between Dubai, America, China, Europe, India and more than a hundred international destinations (citation). These are some of the legal entry routes and there are many illegal borders crossing the illegal migrant, which have made their way into the country. The ports further put the job of security and law enforcement outfits to a riskier undertaking that require risk management practices to mitigate and control the situation and order to build confidence in the police sector and the citizens.

Therefore, the objective of this paper intends to examine the effects of governance, leadership, information technology, risk perception, and compliance with the organisational risk management of the UAE police in Dubai.

2. Literature Review

Risk is characterised as the possibility and severity of an accident or failure due to exposure to various hazards, including human injury and resource loss. Risk management is characterised as the process of recognising and managing risks that the company is inevitably exposed to in an effort to achieve its corporate goals (CIMA Official Terminology, 2005). For an organisation, threats are future incidents that may impact the achievement of the goals of the organisation. Risk management is about recognising and representing risks and making positive plans to minimise them by understanding the essence of such incidents. Fraud is a major danger that not only affects the corporation in terms of financial health, but also its image and credibility.

Operational Risk Management (ORM) is a decision-making instrument that systematically recognises risks and advantages and defines the appropriate course of action for any given situation (Koehler, 2018). ORM is designed to minimise the risks involved in preventing mishaps, maintaining properties and protecting health and welfare. Operational risk management provides a logical and structured means of defining and managing risk. Operational risk management however is not a complicated process, but it requires individuals to continuously endorse and enforce the basic concepts of it. Consequently, operational risk management provides a valuable method for individuals and organisations to improve productivity and minimise injuries. In any possible environment or situation, the ORM method is open to and accessible by all. It guarantees that in the crucial decisions that decide progress or failure in operations and activities, all workers will have a voice. ORM will still boost efficiency if implemented properly.

All police daily activities involve risk and require decisions that include risk assessment and risk management. Operational Risk Management (ORM) is simply a formalized way of thinking about these things. ORM is a simple six-step process; these steps are- Identify Mission Tasks- Identify Hazards- Assess Risks - Identify Options - Evaluate Risk vs. Gain and Monitor Situation which identifies operational hazards and takes reasonable measures to reduce risk to personnel, equipment and the mission.

2.1 Operational Risk management in UAE police Sector

The field of operational risks management in the UAE police force lacks adequate research (Alosani and Al-Dhaafri 2020). This study primarily focuses on Dubai and assesses how national and international legislation, law enforcement is struggling with risk management issues in the police service. The study is on preventing and reducing operational risks in Dubai, which is crucial to the nation's security and the city's position in the UAE and as a global trade hub, which means that the current study is practical and academically relevant.

The police are also seen as risk knowledge specialists who organise various information structures to respond to the risk management of their own external groups while gathering data from multiple extrinsic sources to respond to their investigative requirements. Although there are numerous risk monitoring and information-transfer projects from individuals and groups to the police, such as community policing, documentation of domestic abuse and self-protection services, this data exchange is impeded by the right to privacy (Alqutbah, 2017).

Risks are more multifaceted in the public sector than in the private sector (Schillemans, & Busuioc). This is because risk-taking outcomes can entail serious concerns for individuals (Alqutbah, 2017), although the additional reach of public scrutiny suggests less margins for failure (Tilly, 2014). The literature has established a number of risks affecting the police sector, including organisational, reputational, financial, regulatory, litigation and efficiency.

The possible vulnerabilities or threats to such operating systems are the underlying concepts, beliefs, expectations, values and behaviours of employees, all of which contribute to the composition of the risk culture of an organisation. Safa, & Futcher, (2016) has indicated that for effective organisational risk management, the 'human aspect is important. It is the most vulnerable component of any strategy or attempt to reduce an organization's risk potential. Audit studies, periodicals and conferences have stressed this (Oakman, & Kinsman, 2018). Risk management methods that are expressed as policies and procedures can only be effective within a suitable culture of risk. Most of the concept of threats does not consider the basic requirements of the police department, which is where the latest analysis will be carried out in order to understand the police force's organisational risk management.

A strategic review of the mechanism, processes, role, structure, risk and operational effectiveness is being developed by the UAE Police. The situation is promising that such an approach is being taken at such a stage. At the federal level, a common strategy ensures that national collaboration is instituted on a national basis (Abrams, 2019). The need for such a framework is a sign that change has not been a high priority for an integrated federal approach to policing. The risk of not encouraging and speeding up a concerted federal response is too high in the face of the threats posed by money laundering, terrorist funding, and other crimes in a fast-growing economy like the UAE (Quamar, 2018). Subject to privacy and ethical concerns, the implementation of a national identification card containing personal information, including photographic and fingerprint details, is a welcome and significant step towards embracing a national approach to policing.

The police department must be reminded vigilantly of their obligations. They need to have such traits, such as learning and improving on their errors by broadening their information horizons (Al-Darmaki, 2015). Such skills have been acknowledged as important to the management of police affairs, allowing their officers to work more effectively in responding to threats that jeopardise the national interests. Perhaps the most significant of all that is required is the inclusion of training for the men of the UAE police force. This is expected to ultimately extend their numerous technical specialist abilities, impacting organisational risk management (Al Darmaki, 2015).

Similarly, having the requisite and up-to-date facilities, technology, leadership and governance is also very important, which, without a doubt, boost their performance. In addition, the requisite competencies include most importantly, risk management and the ability to consider the magnitude of the risk to which the local public will be open if not handled in a timely manner. Police officers must also fully identify and recognise risks that have the potential of risking and injuring people.

The absence of organisational risk conceptualization inhibits the ability of police departments to assess and improve the efficiency of individuals, teams and organisations to a degree sufficient to address mission-critical goals. It is this issue, which forms the focus of this research. This research develops a conceptual framework for assessing the effects of governance, leadership, information technology, risk awareness, and enforcement on the operational risk management of the UAE police in Dubai.

1. **Theoretical background and hypothesis development**

A theoretical framework is the synthesis of existing theories, empirical research and related concepts used to build a foundation for a new theory or concept (Rocco and Plakhotnik, 2009). Choice can be made from among existing theories that have been tested by earlier researchers in the same field. The foundation for knowledge construction for a research study is regarded literally and metaphorically as a theoretical framework (Grant and Osanloo, 2014). They further maintained that a framework provides the basis for the literature review, methods and analysis. Thus a theoretical framework is about the thinking, understanding and how a researcher plans to study concepts of a topic in relation to a theory(s). In this section therefore, the management theories that explain organizational performance in relation to all the postulated variables are reviewed.

Risk Management's and Decision Theory's Common Ground this theory used as an indication of priority. New Institutional Economists Theory the theory links security with specific assets purchase, which implies that risk management, can be important in contracts which bind two sides without allowing diversification, such as large financing contract or close cooperation within a supply chain. Agency Theory implies that defined hedging policies can have an important influence on police sector value. The stakeholder theory helps to address the importance of customer trust and financial distress costs to companies

The Organizational Learning Theory has been used in this study to carried out the effects of risk management on the performance. Employees can apply their acquired knowledge of risk management to change their behaviour towards risk. The constraints theory has been used in this study because its consider as very much applicable in the implementation of the risk management process as it is a methodology for detecting the limiting factors (constraints) that stand in the way of achieving management decision support in the firm.

Stakeholder Theory: The stakeholder theory focuses explicitly on the equilibrium of stakeholder interests as the main determinant of corporate policy and that it is a most promising contribution to risk management is the extension of implicit contracts theory from employment to other contracts

Resource-based view (RBV) theory from the management decision support perspective, it emphasizes harnessing internal resources as a key element in achieving a sustained improved performance (Fork-Yew et al., 2014). Equally, the COSO ERM framework, governance structure, standards and process, according to Ping and Muthuveloo (2015), are used to integrate, improve and facilitate a wider intra and inter-organization knowledge management with RBV. The theory will help risk management contribute to organizational performance. The RBV theory corresponds to risk management determinants in higher education. The core capabilities explain competitive success based on their competencies (Hunt and Madhavaram, 2019)

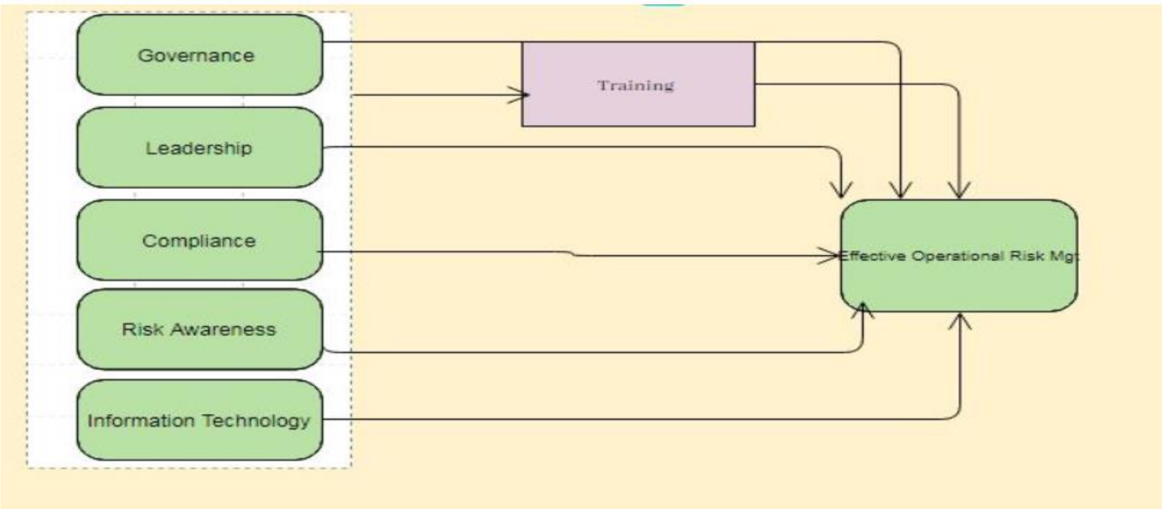

Figure 1. Conceptual Framework

1.1 The relationship between Governance and Effective Operational Risk Management

Organizational governance, decision-making and behaviour are increasingly being driven by risk and risk management practices (Kaarbøe et al. 2017). Risk is commonly defined as the function of the probability of consequence multiplied by its relative magnitude (Zscheischler et al., 2018). In the last few decades, the scope of risk management in organizations has widened considerably through advances in the technical ability to estimate probabilities and impacts (Carlsson-Wall & Tran 2019), the codification of risk-based decision making and management processes (Crovini & Ossola, 2020) and the identification of the organizational processes involved in risk management (Hopkin et al. 2018).

Operational risk is characterized as the risk of failure arising from internal processes, people and structures, external events or reputational risk that are ineffective or failing. Breakdowns of internal controls and corporate governance include the most severe forms of organizational risk. Company of the 21st century runs under technology clouds, these clouds will rain for survival and business development is properly handled or disaster will occur, which can kill business if risk management fails. Apart from many aspects, corporate governance provides the high-level structure for IT governance. Corporate governance provides a mechanism for the creation of long-term trust between business and its stakeholders. This trust is established by rationalizing and documenting a company's risks, reducing top management liability by carefully articulating the decision-making process, maintaining the accuracy of financial results, and finally providing a degree of trust that is required for an organization to operate properly.

The lack of conceptualisation of operational risk undermines UAE police organisations' ability to measure and raise performance for individuals, teams and organisations to a level necessary to address mission-critical objectives. This problem forms the focus of this study. This study's critical review of the literature develops a conceptual framework for determining the effects of governance, leadership, information technology, risk awareness, and compliance on operational risk management of the UAE police in Dubai. Therefore:
Hypothesis H1: Governance is positively related to effective operational risk management

1.2 The relationship between Leadership and Effective Operational Risk Management

In the past literature it is highlighted that an organization desires an effective leadership to produce long-term results for business sustainability (Macke, & Genari, 2019). Yilmaz, & Flouris (2017) stated that leadership has a basic role in shaping and controlling an organization by securing a sense of direction, vision, mission, business strategy and tactics for all associates. Although there is strong recognition of the need to encourage effective leadership at the highest level in any organization, the changing nature of work has necessitated a focus on building leadership capabilities across organizational-wide approach. In other words, the managers must be equipped with necessary competencies, knowledge, skills, support, focus and talent. Fiaz, & Saqib, (2017) stated good leaders good leaders must have the following four key dimensions: (1) the ability to drive the organization's goal alignment, business strategy and priorities; (2) the development of the organizational culture within operational needs and parameter setting; (3) the maintenance of good practices to accommodate conducive working environment; and (4) the encouragement of high performance and world class standard in the work execution.

Strong leadership leading to a high commitment in managing risk is needed to ensure continuous executive support for the implementation of integrated ERM (Uhl-Bien, M., & Arena, 2018). The champion is responsible for addressing integrated risk management and supporting executives to meet in both the short term and long terms corporate objectives. Previous studies have indicated that risk management adoption relies heavily on the institutional ownership of leadership (Bena, & Pires, 2017).

However, the police department must be reminded vigilantly of their obligations. They need to have such traits, such as learning and improving on their errors by broadening their information horizons (Al-Darmaki, 2015). Such skills have been acknowledged as important to the management of police affairs, allowing their officers to work more effectively in responding to threats that jeopardise the national interests. Perhaps the most significant of all that is required is the inclusion of training for the men of the UAE police force. This is expected to ultimately extend their numerous technical specialist abilities, impacting organisational risk management (Al Darmaki, 2015). Therefore:

Hypothesis H2: Leadership is positively related to effective operational risk management

1.2 The Relationship between Compliance and Effective Operational Risk Management

The risk compliance portal on the NEC intranet (for Japan) and DASHBOARD Global (for subsidiaries outside Japan) are dedicated to sharing and disseminating information on the latest compliance issues within the NEC Group. The company issues the fortnightly Compliance News email magazine, which provides timely topics in accordance with the business environment. Every year, it also updates the NEC Group Code of Conduct Case Sheet, which currently presents more than 160 case studies. These materials are used for a wide range of purposes, such as for distribution to new employees and use as educational materials during promotion of managers.

In this study, our focus is on institutions' role in encouraging citizens to believe that it is morally just to obey the law (Zietsma & Toubiana, 2018). Legal legitimacy is the public belief that laws are personally binding and the corresponding moral obligation to abide by the law. When people believe that rules are binding in their 'existential, present lives' (Hertogh, (2018) they feel a duty to obey the rules put in place by authorities, regardless of the morality of a given act (Farmaki, & Kaniadakis, 2019). Granting authorities such as the police and courts legitimacy cedes to authorities the right to define what constitutes proper behaviour. Holding the system of rules to be legitimate overrides specific questions concerning the morality of particular rules.

In the UAE, the outsourcing of policing operations to the private security sector is significantly embedded as a key policy objective driven by a wider commitment to deliver efficient public services and restructure government ministries (Alqutbah, 2017). This strategic shift in service delivery is resulting in a heightened momentum for UAE police authorities towards greater outsourcing which thus far is evidenced by the outsourcing of fire services by Abu Dhabi police, and the licensing of private sector involvement in non-core services (Alqutbah, 2017). Moreover, the UAE has extensively recruited former foreign police to act in diverse roles such as advisors to government ministries, providing ad hoc training and consultancy services, and community policing services (Ellinson and Sinclair, 2013). As a result, there is a growing imperative to ensure that outsourced contracts deliver services effectively and efficiently and maintain high standards across a range of critical areas. Therefore:

Hypothesis H3: Compliance is positively related to effective operational risk management

1.2 The Relationship between Risk Awareness and Effective Operational Risk Management

Risk awareness is the 6th component of this model representing a crosscutting and comprehensive dimension underpinning other dimensions. Understanding of risk awareness and the impact of model dimensions is understood to require some form of measurement in order to identify priorities, discrepancies, and conditions, which promote risk awareness. It has been noted that monitoring and evaluation is essential to refining approaches and methods and understanding the effectiveness or shortcomings of different factors on risk awareness (Delponte, & Schenone, 2017).

The central premise is that risk awareness levels in each of these areas critically impact on the effectiveness of functions and the overall organisational success. These five dimensions (governance, compliance, enterprise, IT GRC, risk Management) represent five major areas of IT management, which have become increasingly dependent on new awareness of risk. These dimensions present a holistic frame of reference for exploring risk awareness. While there is a significant overlap between the general governance, risk management compliance dimensions and specific governance within IT GRC, both have relevance. While IT GRC focuses on IT specific related governance risk, an understanding of risk awareness issues within broader compliance, governance and risk contributes to holistic strategic exploration of risk awareness. Risk awareness within the MERIT model represents the central connecting underpinning dimension impacting on the effectiveness of the five other dimensions. Since awareness is a human quality, this element focuses on measuring the effect of the previous elements on managers and staff level of awareness of risk. Therefore;

Hypothesis H4: Risk awareness is positively related to effective operational risk management

1.3 The Relationship between Information Technology and Effective Operational Risk Management

Information technology is associated with significant financial risks emphasising the importance of addressing risk within IT systems. Tsay, & Mahoney, (2018) considered how managers make decisions to outsource IT systems and contends that managers should consider why they should not insource. He identified eleven risks associated with IT outsourcing including possibility of weak management in the Seller Company, inexperienced staff, business uncertainty and hidden costs. One particular risk, 'endemic uncertainty', concerns IT operations and development as 'inherently uncertain'. "Users are not sure of their needs, new technology is risky, business requirements change, and implementation is full of surprises. This provides an insight into the problematic manner of managing IT systems risk in the context of inherent uncertainty. Wangen, & Snekkenes, et.al, (2018) further report that: "the results also show that organisations still have room for improvement to create idyllic ISRA processes" Information Systems Risk Assessment (ISRA). They identified eight risk factors, with financial loss (93%) and risk to infrastructure (81%) accounting for the highest focus. Firm theoretical basis for IT systems risk management strategies involves deterrence, prevention, detection and recovery (DuHadway, & Hazen, 2019).

The need for information system risk awareness is critical given the increasing range and number of risks to which information systems are exposed on a daily basis. The problem is pervasive with over 90% of US companies for example experiencing some type of cyberattack and the global cost has been conservatively estimated at approximately $388 billion (Hampton 2014). The nature of the threats to information systems are diverse, dynamic and evolving and include attacks such as denial of service, phishing, data breaches, and deployment of malware, malicious code and botnets. These attacks are frequently designed to support the execution of cyber-crimes involving wrongdoing such as theft, fraud and extortion of organisations (Jain and Kalyanam, 2012)

In the context of widespread use of IT by organisations, IT risk management needs to be understood from both the perspective of the computer hardware, software and, crucially, from the perspective of the people who use IT and information systems (IS). The risk exposure of the computer hardware and IT systems can be measured using metrics specifically developed to assess threats to computers and software IT systems. These include metrics used in other domains such as volatility, compliance, terror and or systemic risk (Haber, 2012). But the risk exposure of the people who use the IT systems and IS is subjective. Research on the subjective aspects of IT risk management is lacking however, this is an important gap as people are the central feature and potential weakness of any business process-oriented IT system.

Organizations need to consider IT as an important factor in the face of increasing competition, higher performance levels, globalization, and liberalization. IT plays a key role in achieving an organization's objectives. IT relates to all aspects of the business processes, including access to a shared infrastructure consisting of knowledge, human assets, core competencies, resource allocation, performance management, project tasking and communication support (Antoni, & Akbar, 2019). Therefore:

Hypothesis H5: Information technology is positively related to effective operational risk management

1.4 Training Mediate the Relationship between critical components of management and operations on the effective operational risk management

Training is a critical part of training effectiveness and also give effect to learn an assessment of knowledge acquired, skills improved, or attitudes changed and design of a training for improvement is the main focus (Alvelos, Ferreira & Bates, 2015). The design stage of training play an important role in the outcomes and affect the employees and organizational performance. Training design with reference to employees explain that the content of the training should be similar with the actual job and the skills needs of the employees required improving the performance.

According to Alvelos et al. (2015) training material should have reasonable content with the work of the training material, and said to be relevant. According to the theory of expanded identical elements trainers should move around to protect the environment to ensure consistent training to safeguard of near transfer by the trainees (Thorndike & Woodworth, 1901). Awais Bhatti et al., (2013) specified a training should train trainees on the particular knowledge, skills, and abilities (KSAs) that have been identified in the task analysis prior to the training process. The second factor that trainers and professionals must confirm that there are no objectives are included in the training program, which are irrelevant to the job of individuals participating in trainin.

One hand, content relevance of training had been researched, and shown that content relevance is related to training transfer by an individual (Zumrah & Boyle, 2015). Yamnill and McLean’s (2002) conducted research on Thai managers and found that content relevance was a key factor in predicting trainee awareness of training transfer. On the other hand, Nafukho, & Cherrstrom, (2017) found that Training Mediate operations on the effective operational risk management. As a final point, there must be a close relationship between work tasks and training content, underpinning the necessity of an analysis to identify suitable training content. Therefore:

Hypothesis H6: Training mediated the relationship between governance and effective operational risk management.

Hypothesis H7: Training mediated the relationship between leadership and effective operational risk management.

Hypothesis H8: Training mediated the relationship between compliance and effective operational risk management.

Hypothesis H9: Training mediated the relationship between risk-awareness and effective operational risk management.

Hypothesis H10: Training mediated the relationship between information technology and effective operational risk management.

2. Methodology

2.1 Measurement instrument and sample

A research instrument is the way by which data are collected from respondents, and include questionnaire, observation and document analysis (Rahi, 2017). The particular instrument depends on the type of data, scope and objectives of the study, timeframe, resources and accuracy needed. In this study, a descriptive survey, a questionnaire was adopted to collect data for both independent and dependent variables from primary sources. Table 1 shows the questionnaires development in this study. The present study used purposive survey methodology and focusing on the organizational level as the unit of measure.

Five-point likert scale was used to measure the construct of proposed model, starting from “very disagreeable” (1) to very agree (5). The survey questionnaire has seven major parts. First, governance responses to operational risk had 8 items adapted from the risk related management support literature (Hearld & Alexander, 2014; Roundy & Brockman, 2018; Pechlaner & Bieger, 2014; Press & Arnould, 2014; Chung et al., 2012; Pompian, 2012). Second, leadership responses to operational risk had 7 items adapted from the risk related organizational management (Senge & Kania, 2015; Miller & Lyons, 2016; Allen et al., 2016; Meder & Wegner, 2015). Third, compliance to operational risk had 6 items adapted from the risk related IT management support literature (Agha et al., 2018; Boyce, 2017; Miller, 2018; English & Hammond, 2014). Fourth, risk awareness had 7 items adapted from risk related risk management support (Giannakis & Papadopoulos, 2016; Kavlock & Thomas, 2018; Mangla & Barua, 2015; Ho & Talluri, 2015; Hopkin, 2018; Trkman & McCormack, 2016). Fifth, information technology responses to operational risk had 5 items adapted from the risk related IT management support literature (Garrison & Kim, 2015: Mian & Spoor,2019; Abualoush & Al-Badi, 2018; Shatto & Erwin, 2016; Kwoczek & Nejdl, 2014). Sixth, training to operational risk had 8 items adapted from the risk related job motivation literature (Taylor & Marmon, 2017; De Leon & Cohen, 2014; Coleman & Hemsworth, 2014; Korte et al., 2015; Morsy et al., 2016). Seventh, effective operational risk management had 10 items adapted from risk related risk management support (Ponte & Sturgeon, 2014; Qiu & Trapnell, 2017; Choi & Yue, 2016; Kanger et al,, 2019; Zheng & Yang, 2019: Zheng et al., 2019; Pritchard, 2014).

Table 1: Questionnaires Development

Factors and Items	References
Governance responses	
We have a clear IT vision, mission, or strategy	(Hearld & Alexander, 2014; Roundy & Brockman, 2018; Pechlaner & Bieger, 2014; Press & Arnould, 2014; Chung et al., 2012; Pompian, 2012)
Our technology ecosystem is inflexible or complex	
We have adequate leadership support for IT governance	
We have a culture of shared governance, transparency, and communication.	
We have committed participation from stakeholders	

We make investment decisions wisely.	
We are able to set priorities.	
We provide community representation in IT decision making.	
Leadership responses	
Members need to be supervised closely or they are not likely to do their work.	(Senge & Kania, 2015; Miller & Lyons, 2016; Allen et al., 2016; Meder & Wegner, 2015)
In complex situations, leaders should let members work out problem on their own.	
Members want to be a part of the decision-making process	
Providing guidance without pressure is the key to be being a good leader.	
As a rule, members must be given rewards or punishments in order to motivate them to achieve organizational objectives.	
Leadership requires staying out of the way members as they do their work.	
Most members want frequent and supportive communication with their leaders.	
Compliance	
We have a process in place for reviewing and updating our IT compliance practices.	(Agha et al., 2018; Boyce, 2017; Miller, 2018; English & Hammond, 2014)
We have adequate staff hours devoted to IT compliance.	
We have enough qualified staff devoted IT compliance.	
We have an adequate budget devoted to IT compliance.	
The regulatory environment is too complex.	
We have a formal IT compliance program in place	
Risk-Awareness	
We have a formal procedure for identifying risks	(Giannakis & Papadopoulos, 2016; Kavlock & Thomas, 2018; Mangla & Barua, 2015; Ho & Talluri, 2015; Hopkin, 2018; Trkman & McCormack, 2016).
IT effectively participates in institutional risk assessment	
We implement policies and controls in response to risk analysis.	
We have a process in place for reviewing and updating our risk management practices	
We effectively communicate about risks with all relevant parties.	
Institutional leadership is adequately involved in risk management	
We have an adequate budget devoted to risk management	
Information technology responses	
Integration of our work processes in operations.	(Garrison & Kim, 2015: Mian & Spoor,2019;
Installations for monitoring of operations and people	

Ease of communication between field staff and management	Abualoush & Al-Badi, 2018; Shatto & Erwin, 2016; Kwoczek & Nejdl, 2014
Generation of immediate feedback	
Speeding information spread of potential events	
Training	
Training Program is sufficiently demanding.	(Taylor & Marmon, 2017; De Leon & Cohen, 2014; Coleman & Hemsworth, 2014; Korte et al., 2015; Morsy et al., 2016).
Our organization conducting periodic tests and reviews.	
Training Enhance knowledge, skills, attitude and job.	
Training increases the quality of work.	
Training leads to high employee morale.	
Giving opportunities to socialize with one another during the programme.	
Developing and adjusting long term training goals as necessary.	
The training is very beneficial to my work	
Effective Operational Risk Management	
Embedding more robust Operational Risk practices in taking key decision-making across the organization's value chain	(Ponte & Sturgeon, 2014; Qiu & Trapnell, 2017; Choi & Yue, 2016; Kanger et al,, 2019; Zheng & Yang, 2019: Zheng et al., 2019; Pritchard, 2014)
Embedding more robust measurement process	
Improving the implementation of risk tolerances for Operational Risk	
Embedding more robust risk monitoring process	
Embedding robust risk identification and assessment processes	
Implementing a more robust internal control system	
Defining clearer roles and responsibilities for Operational Risk management capabilities	
Strengthening the tone at the top.	
Adopting a broader scope for the management of Operational Risk	
Embedding more robust business resiliency and continuity processes	

A total number of 600 questionnaires were distributed to different position of employee at police department across Dubai using Google form. A total of 435 questionnaires representing 72.5 percent of the total questionnaires administered were retrieved from this number. Out of this number, 23 questionnaires were either partially filled or invalidated as a result of wrongful filling. This, therefore, resulted in a total number of 412 valid questionnaires that were used for analyses. This is considered a significant sample appropriate to give meaningful responses.

3. Findings

5.1 Respondent characteristics and sample profile

Table 2 shows the socio-demographic characteristics of the respondents in this research. The gender distribution indicated that about 57.3 percent were males, while the remaining 42.7 were females.

The respondents' educational background showed that above half (54.9 percent) had a master degree education, 35 percent holds bachelor degree education, 7.3 percent have diploma education.

The respondents' working experience inclination showed that 65.3 percent have working experience with the organization for 1 to 5 years. The respondents have 17.7 percentage shows 6 to 10 years of working experience, while 16 percent have 11 to 15 years of working experience.

Table 2. Demographic Characteristics of Respondents

		Frequency	Percent
Gender	Male	236	57.3
	Female	176	42.7
	Total	412	100
Academic Qualification	Diploma	30	7.3
	Bachelor Degree	144	35.0
	Master’s	226	54.9
Working Experience	1-5	269	65.3
	6-10	73	17.7
	11-15	66	16.0

5.2 Validity and reliability analysis

The research assessment model presented in this paper was validated using the PLS-SEM approach. Explain why you select PLS-SEM approach. The essence of validating the model using this approach was to empirically gauge its performance with existing criteria that underpin the validation of measurement and structural models.

The measurement model only involved constructs with reflective indicators. Validity and reliability tests were conducted to assess the quality of the measurement model. The results are presented in Table 3. Confirmatory factor analysis showed that factor loadings overcame the critical value of 0.7 (Hair et al., 2014). Moreover, most loadings meet the recommended 0.7 thresholds except for four items. The lowest loading is ranging from 0.429 to 0.673. The researcher retained those items on the recommendations of Hair et al., (2014) if the AVE is achieved then lowest items can be retained. In comparison, the highest loading is 0.886, which is associated with the Compliance construct. This shows that the indicators of each construct were positively correlated with their respective construct, thus indicative of convergent validity (see Table 3). Similarly, the reported AVEs showed that all values meet the minimum threshold of 0.5 (Hair et al., 2014). Therefore, the requirement for convergent validity was achieved.

The results in Table 3 show that all these statistics met the recommended values; that is, Cronbach's alpha >0.7, Dillon-Goldstein's rho >0.7, first eigenvalue >1 and second eigenvalue <1 (Chin, 1998; Sanchez, 2013). Summarizing, the results of the above analysis suggested a good psychometric quality of the measurement model.

Table 3. Convergent Validity Analysis and AVE Values

	Compliance	EORM	Governance	Information Technology	Leadership	Risk Awareness	Cronbach alpha	Composite reliability	AVE value
Compliance									
C1	0.819						0.907	0.928	0.683
C2	0.816								
C3	0.812								
C4	0.886								
C5	0.807								
C6	0.815								
Effective Operational Risk Management									
EORM1		0.803					0.828	0.877	0.551
EORM2		0.810							
EORM3		0.707							
EORM4		0.804							
EORM5		0.821							
EORM7		0.429							
Governance									
GO2			0.724				0.903	0.910	0.631
GO3			0.786						
GO4			0.724						
GO5			0.894						
GO6			0.884						
GO7			0.733						
Information technology									
IT1				0.765			0.794	0.847	0.584
IT2				0.634					
IT3				0.822					
IT4				0.820					
Leadership									
L1					0.811		0.877	0.882	0.562
L2					0.552				

	Compliance	EORM	Governance	Information Technology	Leadership	Risk Awareness	Cronbach alpha	Composite reliability	AVE value
L3					0.701				
L4					0.902				
L5					0.673				
L6					0.805				
Risk awareness									
RA1						0.790	0.897	0.920	0.659
RA2						0.856			
RA3						0.826			
RA4						0.882			
RA5						0.790			
RA6						0.719			

Table 4 shows the discriminant validity result using the the Heterotrait-Monotrait. The HTMT approach is regarded as the most conservative and the most appropriate criterion for assessing discriminant validity (Henseler *et al.,* 2014). The decision rule for establishing discriminant validity in the HTMT approach is for all inter-correlations between the construct of interest and the remaining constructs to be less than 0.85 (r < HTMT0.85) (Henseler *et al*., 2015; Kline, 2011). Table 5.16 shows the result of the HTMT ratio with respect to the constructs in the research model. All the reported values were less than the HTMT0.85 criterion, thus further proving the achievement of discriminant validity.

Table 4. Heterotrait-Monotrait

	Compliance	EORM	Governance	Information Technology	Leadership	Risk-Awareness
Compliance						
EORM	0.446					
Governance	0.226	0.132				
Information Technology	0.262	0.309	0.380			
Leadership	0.263	0.119	0.278	0.204		
Risk-Awareness	0.401	0.386	0.241	0.595	0.102	

5.3 Construct analysis

The predictive capabilities of structural models were assessed based on two criteria of coefficient of determination (R^2) and effect size f^2. It is the indication of the combined effects of all the exogenous latent constructs on the endogenous construct on the model (Hair *et al.* 2014). The result indicates that the entire five exogenous constructs in the structural model have a moderate effect on the endogenous latent construct (R2=.26). This shows that the combined effect of the exogenous latent constructs explains about 26 percent of the variance in the endogenous latent construct. This suggests that governance, compliance, information technology, leadership and risk-awareness collectively predict an individual's intentions to handle operational risk management effectively.

The *f* 2 measures the change in R2 occasioned to the omission of a specific exogenous construct in a model. It is used to assess the impact of individual exogenous construct on the R2 value of the endogenous construct (Hair, *et al.,* 2014). The effect size is measured according to Cohen's (1988) guidelines where *f* 2 values of .02, .15 and .35 are considered as small, medium and large effects respectively. From Table 4.17, the *f*2 values of the respective path relationships in the structural model are presented. The results indicate that compliance has an enormous impact on effective operational risk management with effect sizes of *f* 2=1.600. All other constructs have similarly large effects on the R-square. For governance, information technology leadership and risk-awareness have large effects the *f* 2 of 0.734, 0.792, 0.791 and 0.805 respectively shows values effects on the R-square value.

5.4 Test of hypotheses

In the previous section, it was shown that all the recommended criteria for measurement model validity were satisfied, thus accomplishing the first stage of the two-staged PLS-SEM evaluation process. In this section, the second stage of the process is presented. The structural model evaluation is a five-staged process that involves collinearity assessment, significance testing of the structural model relationships, R^2, *f* 2, and assessment of predictive relevance of the model (Hair *et al.*, 2014). Figure 2 shows the structural model indicating the t-values of the respective path coefficients and factor loadings.

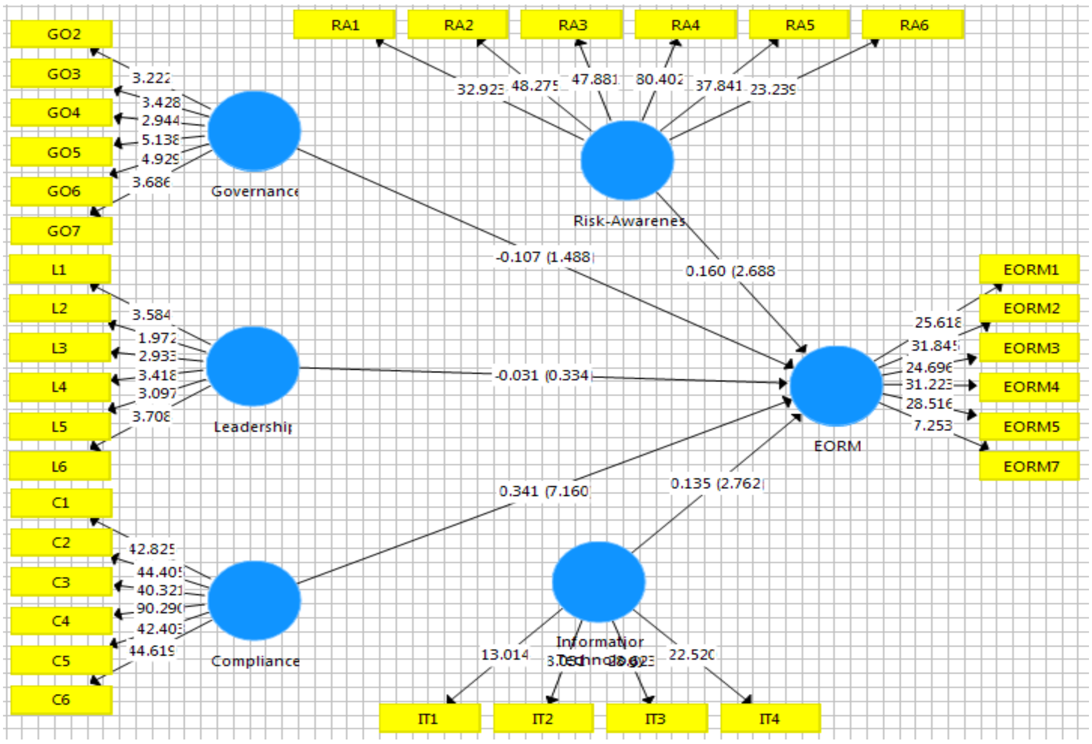

Figure 2: Structural Model

Table 6 shows the path coefficients (β) with their respective t-values, p-values and *f*2 values. As shown in the table, three paths show significant positive relationships, while two paths show a negative significant relationship. The highest positive significant path relationship was between Compliance and effective operational risk management (β=.341, t=7.160, p< .050). In contrast, the least positive significant path relationship was between risk-awareness and effective operational risk management (β=.160, t=2.688, p< .050), hypotheses H3 and H4 were supported. Similarly, information technology and effective operational risk management reported positive and significant relationship with path estimates of (β=.135, t=2.762, p<.05), hypothesis 5 was also supported. The result suggests that individual compliance to effective operational risk management is positively influenced by their sense of governance, their perception of the leadership of the organization, the perceived risk-awareness and their ability to handle the operational risk. On the other hand, the path relationship between governance and effective operational risk management shows a negatively significant path relationship (β=-.107, t=1.488, p**>**.05), so hypothesis 1 was not supported. There is also a negative relationship between Leadership and operational risk management with path model (β=-.031, t=0.334, p**>**.05); hence, hypothesis 2 was rejected (not supported. However, when the considered from the questions on the questionnaire, it is clear that the respondents rated highly on the governance and leadership scales that measured their perceived operational risk management, which implies that they considered themselves better up in terms of handling operational risk.

Table 6: Standardized path coefficient estimates of the final structural equation model

Hypothesis path	Beta	T Statistics (|O/STDEV|)	p-values	f2	R2	Remarks (supports or not?)
Compliance -> EORM	0.341	7.160	0.000	1.600	0.263	Support
Governance -> EORM	-0.107	1.488	0.137	0.734		Not Support
Information Technology -> EORM	0.135	2.762	0.006	0.792		Support
Leadership -> EORM	-0.031	0.334	0.739	0.791		Not Support
Risk-Awareness -> EORM	0.160	2.688	0.007	0.805		Support

To test the mediation effect, this study used Preacher and Hayes (2008. For this purpose, this study used a two-step approach. At the first step, all direct relationships were estimated in two ways, first direct relationship without a mediator and second indirect with mediators. At the second stage, all indirect effects have been calculated and their significance through bootstrapping was calculated.

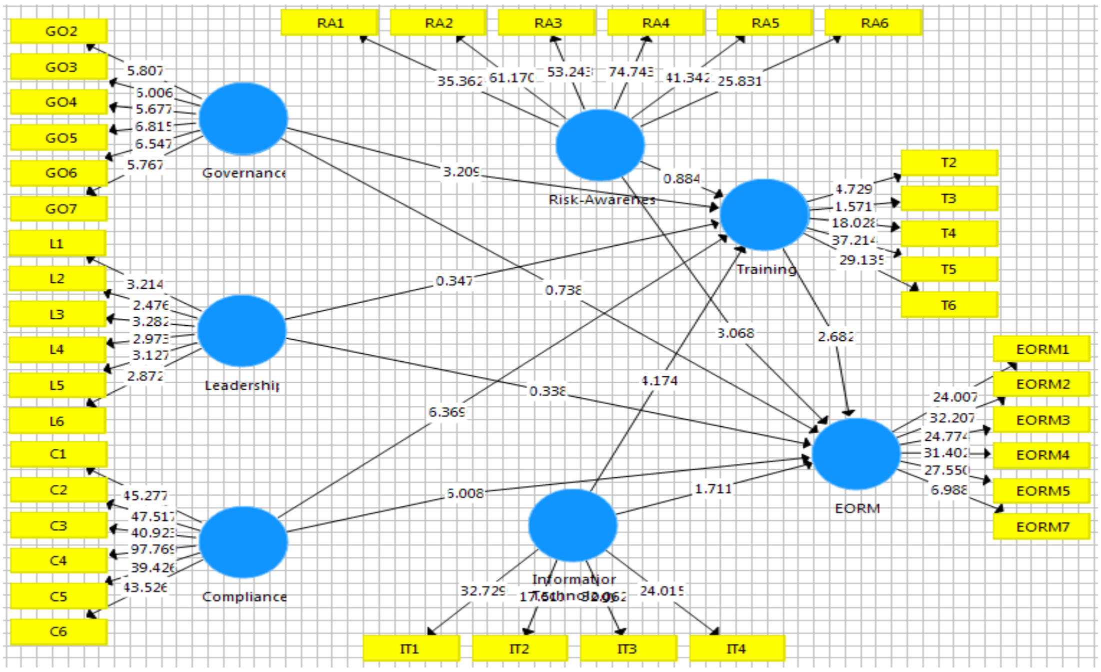

Figure 3: Mediation Measurement Model

Figure 3 shows the t-statistics value of the direct and indirect relationship between endogenous and exogenous constructs. Table 9 shows the path coefficients (Beta), t-statistics and p-value of the ORM constructs on EORM, through Training mediation.

Hypothesis H6 stated: Training mediated the relationship between governance and effective operational risk management.

The results indicated that the path coefficient of the indirect path for the Hypothesis *H7: Training not mediated the relationship between leadership and effective operational risk management* The Beta (Path coefficient) -0.025 value and t-statistics 0.338 shows the non-significance in the relationship. By examining the P-value 0.735, it shows the non-significance in the relationship. Therefore, from the T-value and P-value is below the recommended threshold, so the hypothesis H13 was not supported (Rejected).

Hypothesis H8: the results reveal that the Training mediated the relationship between compliance and effective operational risk management. The values Beta, 0.299, t-statistics 6.008 and P-value is 0.000. Hypothesis 8 was significant (supported). The results indicate that the employees aware of risk can minimize operational risk. This helps the organization to manage operational risk effectively

Hypothesis H9: training mediated the relationship between risk-awareness and effective operational risk management. The Beta value is 0.160, and t-value 3.068 and P-value 0.002, which is above the threshold of recommended statistics. Therefore, hypothesis 9 was supported (accepted). The results indicate that the employees aware of risk can minimize operational risk. This helps the organization to manage operational risk effectively

Furthermore, *Hypothesis H10: Training mediated the relationship between information technology and effective operational risk management.* The results of Beta, 0.089, T-statistics 1.711 and P-value is 0.088. The hypothesis results are below the recommended threshold. Hence, H10 was supported.

However, it was found out that three of the five indirect paths was not significant. This indicates that the existence of non-mediation effects of training on governance, leadership and information technology. This result represents that organizations focusing on governance and leadership does not succeed effectively in managing operational risk, though it may have impact employee performance.

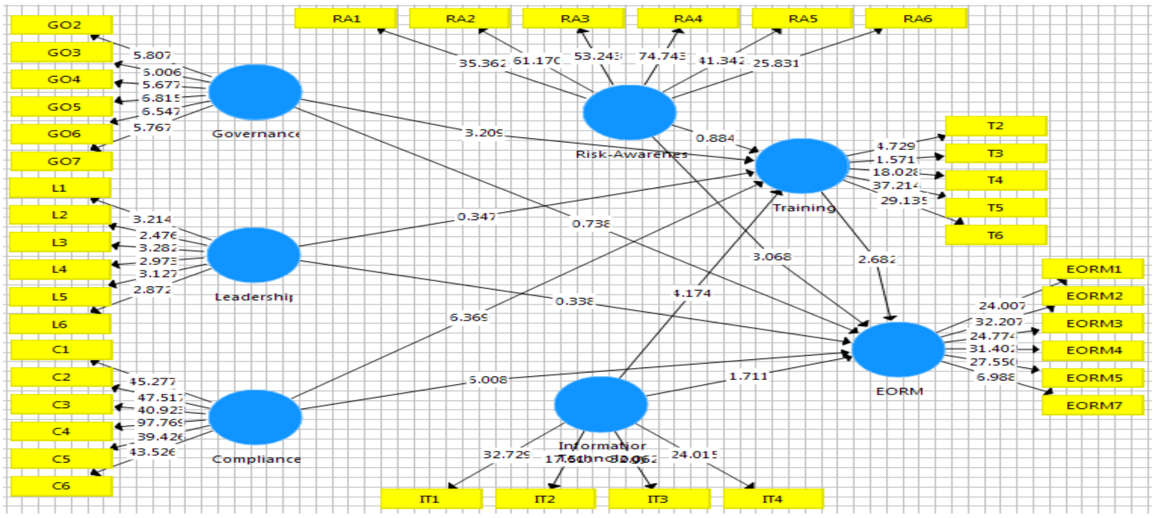

Figure4: Mediation Structural Model

Table 8: Results of mediating hypothesis

	Beta	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values	Decision
Compliance -> EORM	0.299	0.050	6.008	0.000	Supported
Compliance -> Training	0.322	0.051	6.369	0.000	Supported
Governance -> EORM	-0.043	0.059	0.738	0.461	Not-supported
Governance -> Training	-0.187	0.058	3.209	0.001	Supported
Information Technology -> EORM	0.089	0.052	1.711	0.088	Not-supported
Information Technology -> Training	0.233	0.056	4.174	0.000	Supported
Leadership -> EORM	-0.025	0.074	0.338	0.735	Not-supported
Leadership -> Training	0.025	0.073	0.347	0.729	Not-supported
Risk-Awareness -> EORM	0.160	0.052	3.068	0.002	Supported
Risk-Awareness -> Training	0.054	0.062	0.884	0.377	Not-supported
Training -> EORM	0.141	0.052	2.682	0.008	Supported

5.5 Discussion and implications

The outcomes of the study can be applied to practice. It is expected that the main outcome of the study will be used by the UAE Police Force to (a) help them better articulate their risk awareness policies, (b) provide relevant training to promote compliance (c) suggest kind of leadership and governance suitable for operational risk management and (d) use IT support to enable accurate risk identification, assessment, reporting, control and mitigation. This outcome can be generalised to cover Abu Dhabi and other neighbouring Gulf Nations Police authorities through specific and broader communication and engagement. The research will broaden the impact to benefit other Gulf Countries' Police Forces, who will be invited to share best practices.

Problems related to governance, leadership, compliance, information technology and risk awareness as they relate to risk management practice in the UAE police will be addressed. The study would be done in collaboration with the Force's risk management experts, which will further co-produce knowledge through its activities, outputs and usage.

The explicit benefit to the Force will be an awareness of the need to have a functional operational risk strategy. Force commanders and risk managers will profit by considering the findings to articulate their risk management strategy. The results would also provide a basis for enhancing policing functions in the UAE in an exceedingly dynamic and fast-changing environment through an objective understanding of operational risk management paradigms. Such a framework provides a theoretical foundation for implementing operational risk management culture, which maximises the knowledge and experience of the policing sector, contributing to appropriate responses.

6. Conclusion

The chapter presented and discussed the quantitative results of the research that began with an analysis of the questionnaire google form, preliminary data analysis, structural model evaluation, and moderation analysis. The findings revealed that individuals' willingness to follow the leadership does not have the autonomy to take steps to manage operational risk efficiently. The governance part shows that if the supervisors are not familiar with the leadership skills, the governance part will not affect the managing operational risk. The employee's willingness to update information technology may also affect managing operational risk. Similarly, the results identified that risk-awareness and compliance help the organization effectively manage operational risk in day to fay business handling.

References

- Abrams, J. (2019). The emergence of network governance in US National Forest Administration: Causal factors and propositions for future research. Forest Policy and Economics, 106, 101977.
- Alqutbah, A. S. M. (2017). Assessing police privatisation in the United Arab Emirates (Doctoral dissertation, Middlesex University).
- Alqutbah, A. S. M. (2017). Assessing police privatisation in the United Arab Emirates (Doctoral dissertation, Middlesex University).
- Alqutbah, A. S. M. (2017). Assessing police privatisation in the United Arab Emirates (Doctoral dissertation, Middlesex University).
- Antoni, D., & Akbar, M. (2019). E-supply chain management value concept for the palm oil industry. Jurnal Sistem Informasi, 15(2), 15-29.
- Bena, J., Ferreira, M. A., Matos, P., & Pires, P. (2017). Are foreign investors locusts? The long-term effects of foreign institutional ownership. Journal of Financial Economics, 126(1), 122-146.
- Carlsson-Wall, M., Kraus, K., Meidell, A., & Tran, P. (2019). Managing risk in the public sector–The interaction between vernacular and formal risk management systems. Financial Accountability & Management, 35(1), 3-19.

- Crovini, C., Santoro, G., & Ossola, G. (2020). Rethinking risk management in entrepreneurial SMEs: towards the integration with the decision-making process. Management Decision.
- Delponte, I., Pittaluga, I., & Schenone, C. (2017). Monitoring and evaluation of Sustainable Energy Action Plan: practice and perspective. Energy Policy, 100, 9-17.
- DuHadway, S., Carnovale, S., & Hazen, B. (2019). Understanding risk management for intentional supply chain disruptions: Risk detection, risk mitigation, and risk recovery. Annals of Operations Research, 283(1), 179-198.
- Farmaki, A., Stergiou, D., & Kaniadakis, A. (2019). Self-perceptions of Airbnb hosts' responsibility: a moral identity perspective. Journal of Sustainable Tourism, 1-21.
- Fiaz, M., Su, Q., & Saqib, A. (2017). Leadership styles and employees' motivation: Perspective from an emerging economy. The Journal of Developing Areas, 51(4), 143-156.
- Hertogh, M. (2018). Nobody's law: Legal consciousness and legal alienation in everyday life. Springer.
- Hopkin, P. (2018). Fundamentals of risk management: understanding, evaluating and implementing effective risk management. Kogan Page Publishers.
- Macke, J., & Genari, D. (2019). Systematic literature review on sustainable human resource management. Journal of cleaner production, 208, 806-815.
- Meidell, A., & Kaarbøe, K. (2017). How the enterprise risk management function influences decision-making in the organization–A field study of a large, global oil and gas company. The British Accounting Review, 49(1), 39-55.
- Nafukho, F. M., Alfred, M., Chakraborty, M., Johnson, M., & Cherrstrom, C. A. (2017). Predicting workplace transfer of learning. European Journal of training and Development.
- Oakman, J., Macdonald, W., Bartram, T., Keegel, T., & Kinsman, N. (2018). Workplace risk management practices to prevent musculoskeletal and mental health disorders: what are the gaps?. Safety science, 101, 220-230.
- Quamar, M. M. (2018). The changing nature of the Pakistan factor in India-Gulf relations: An Indian Perspective. Asian Affairs, 49(4), 625-644.
- Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. International Journal of Economics & Management Sciences, 6(2), 1-5.
- Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. Computer Fraud & Security, 2016(2), 15-18.
- Schillemans, T., & Busuioc, M. (2015). Predicting public sector accountability: From agency drift to forum drift. Journal of Public Administration Research and Theory, 25(1), 191-215.
- Tsay, A. A., Gray, J. V., Noh, I. J., & Mahoney, J. T. (2018). A review of production and operations management research on outsourcing in supply chains: Implications for the theory of the firm. Production and Operations Management, 27(7), 1177-1220.
- Uhl-Bien, M., & Arena, M. (2018). Leadership for organizational adaptability: A theoretical synthesis and integrative framework. The Leadership Quarterly, 29(1), 89-104.
- Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 17(6), 681-699.
- Yilmaz, A. K., & Flouris, T. (2017). Enterprise risk management in terms of organizational culture and its leadership and strategic management. In Corporate risk management for international business (pp. 65-112). Springer, Singapore.
- Zietsma, C., & Toubiana, M. (2018). The valuable, the constitutive, and the energetic: Exploring the impact and importance of studying emotions and institutions.
- Zscheischler, J., Westra, S., Van Den Hurk, B. J., Seneviratne, S. I., Ward, P. J., Pitman, A., ... & Zhang, X. (2018). Future climate risk from compound events. Nature Climate Change, 8(6), 469-477.