Alexandria Journal
of Accounting Research

Third Issue, September, 2022, Vol. 6

Dr. Abdelmoneim Bahyeldin Metwally[1]
Accounting Department, Faculty of Commerce, Assiut University

Dr. Samir Ibrahim Abdelazim
College of Business Administration, Majmaah University, Saudi Arabia and Faculty of Commerce, Beni-Suef University

Dr. Mohammad Talaq Almarji
Senior Accounting Specialist
At Public Authority for Food and Nutrition - Kuwait

Internal Auditors' Role in Confronting Cyber and Fraud Risks Related to Outsourcing Insurance: an Exploratory Study

Abstract

This study investigates how the emergence of the coronavirus (COVID-19) pandemic has raised many concerns in insurers internal controls and fraud confrontation. Covid-19 required massive shift towards digital transformation in recent years, insurers are finding themselves relying on outsourcing as a way to cope with business model changes and requirements. This change augmented the risk of cyber-attacks and it is ultimately considered a high risk for insurers of any size because not only will it subject insurers to litigation concerning data breaches, but it will also cause massive harm to the insurer's reputation when an attack happens. Moreover, due to this digitalization fraud risk is harder to manage, as traditional internal controls are inefficient as the time spent in fraud investigation will delay the payment for hospitalised insurance claims, which would raise concerns about the insurer's reputation. To resolve this conundrum and manage reputational risk, most insurers seek trade-offs and negotiations with the insured. Data has been collected using archival research and semi-structured interviews with some chief risk officers (CROs), internal auditors and insurance practitioners. The authors explain how, following the COVID-19 pandemic, insurers are facing cyber and fraud risks that need specific planning and control by internal auditors as current internal controls fall short in front of these new risks. Therefore, the authors propose some potential policy solutions that would help internal auditors overcome both cyber and fraud risks. Through explaining the concurrent risks and proposing potential solutions in this emerging market, this paper provides some practical insights for internal auditing researchers, insurers and CROs who are seeking solutions to pandemic-related risks.

Keywords: Cyber risk, Fraud risk, Internal audit, Telework, Internal control, Covid-19.

E.mail: a.metwally@aun.edu.eg
E. mail: Samir.mohamed@commerce.bus.edu.eg
E. mail: Almarji@yahoo.com

دور المراجع الداخلي في مواجهة خطر الامن السيبراني وخطر الغش في الاستعانة بمصادر خارجية في عمليات التأمين: دراسة استطلاعية

ملخص البحث

تبحث هذه الدراسة في الكيفية التي أثار بها ظهور جائحة فيروس كورونا (COVID-19) العديد من المخاوف في الرقابة الداخلية لشركات التأمين ومواجهة الاحتيال. تطلب Covid-19 تحولا هائلا نحو التحول الرقمي في السنوات الأخيرة، وتجد شركات التأمين نفسها تعتمد على الاستعانة بمصادر خارجية كطريقة للتعامل مع تغييرات ومتطلبات نموذج الأعمال. زاد هذا التغيير من مخاطر الهجمات الإلكترونية ويعتبر في نهاية المطاف خطرا كبيرا على شركات التأمين من أي خطر اخر لأنه لن يعرض شركات التأمين للتقاضي بشأن انتهاكات البيانات فحسب، بل سيؤدي أيضا إلى إلحاق ضرر جسيم بسمعة شركة التأمين عند حدوث هجوم. علاوة على ذلك، بسبب هذا الرقمنة، من الصعب إدارة مخاطر الاحتيال، حيث أن الضوابط الداخلية التقليدية غير فعالة لأن الوقت الذي يقضيه في التحقيق في الاحتيال سيؤخر دفع مطالبات (تعويضات) التأمين في المستشفى، مما قد يثير مخاوف بشأن سمعة شركة التأمين. لحل هذه المعضلة وإدارة مخاطر السمعة، تسعى معظم شركات التأمين إلى المقايضات والمفاوضات مع المؤمن عليه. تم جمع البيانات باستخدام البحوث المكتبية والمقابلات شبه المهيكلة مع بعض كبار مسؤولي المخاطر (CRO) والمراجعين الداخليين وممارسي التأمين. توضح هذه الدراسة الاستطلاعية كيف تواجه شركات التأمين، في أعقاب جائحة COVID-19، مخاطر الإنترنت والاحتيال التي تحتاج إلى تخطيط ومراقبة محددة من قبل المراجعين الداخليين لأن الضوابط الداخلية الحالية تقف عاجزة أمام هذه المخاطر الجديدة. لذلك، يقترح المؤلفون بعض الحلول التي من شأنها أن تساعد المراجعين الداخليين في التغلب على كل من مخاطر الإنترنت والاحتيال. من خلال شرح المخاطر المتزامنة واقتراح الحلول المحتملة في هذه السوق الناشئة، تقدم هذه الورقة بعض الأفكار العملية للباحثين في المراجعة الداخلية وشركات التأمين وادارة الخطر الذين يبحثون عن حلول للمخاطر المتعلقة بالجوائح.

الكلمات المفتاحية: المخاطر السيبرانية،خطر الغش،المراجعة الداخلية،العمل عن بعد، الرقابة الداخلية، جائحة كورونا.

1. Introduction

The COVID-19 has diminished the economic activity of different business companies by consuming lots of money in their response to the massive emerging operational and technical risks following the pandemic (Metwally *et al.*, 2020; Naseeb *et al.*, 2021). Then, industries across the globe are facing significant challenges that they have never seen before. The insurance industry is not an exception. Insurers are currently having many new operational limitations and financial problems. Further, the availability of investments in the insurance sector is not like the situation before the COVID-19 pandemic. These new challenges and risks should be managed efficiently as they may affect insurers' continuation and future performance (Farooq *et al.*, 2021; Metwally *et al.*, 2021). Insurers are currently forced to grant premium payment extensions and policy renewal deadlines to the policyholders whose businesses ceased due to the pandemic. Moreover, governments require insurers to settle all claims during the pandemic. This is because with the accumulation of claims, the insurance market is likely to face tremendous losses, affecting the whole stock market (Naseeb *et al.*, 2021). These companies have to manage the increasing difficulties, risks, and uncertainties resulting from the pandemic to preserve their operational resilience and insureds' satisfaction and adapt to the 'new normal' after the end of the pandemic.

The COVID-19 pandemic has presented increased pressures from international rating agencies and international reinsurers upon insurers to embed Enterprise Risk Management (ERM), which necessitates the adoption of solvency II capital adequacy requirements (Metwally and Diab, 2021). Within the present context where several risks have emerged following the COVID-19 pandemic, it is expected that the risk management department and internal auditors would play a key role in setting the company strategy and promoting the financial institutions' financial and operational resilience (Naseeb *et al.*, 2021). This is important to stabilize the financial position of the insurance companies.

To cope with the current challenges, these companies need to think of new risk management measures. In this regard, Uganda, for example, sought to market a new product, "COVID-19 Group Life Extension Insurance Cover" (Atlas, 2020b), to motivate insurers to pursue new policies to avoid this situation. Also, Amazon offered COVID-19 health coverage for its retailers in India over COVID-19 hospitalization, treatment, ambulatory assistance, and intensive care expenses (Atlas, 2020a, 2020b).

The recent financial crisis of 2008/2009 has made ERM an emerging research endeavour (Butaru *et al.*, 2016; Crovini *et al.*, 2021; El Baz and Ruel, 2021; Hopper and Bui, 2016; Pagach and Kosmala, 2020; Tallaki and Bracci, 2021; Wiengarten *et al.*, 2016). The rise of ERM has inspired more studies to examine its conceptualization and interactions with organizational apparatuses and how that led to new modes of controls (Bhimani, 2009; Huber and Scheytt, 2013; Soin and Collier, 2013; Tekathen and Dechow, 2013; Vinnari and Skaebaek, 2014). However, most of these studies focus on the risk-based management practices in both west and least-developed countries (LDCs) (see Metwally and Diab, 2021).

Our analysis revealed that with the recent over-reliance on technology to deliver services, insurers have consistently found themselves with the need to have a new business model that incorporates teleworking/working from home. New client acquisition, underwriting, policy issuances and claims filing can now all be done over the world wide web with minimal or no physical interaction at all. The COVID-19 pandemic has also accelerated this trend with the need for teleworking/working from home (Metwally *et al.*, 2021), and thus resulting into a magnified exposure to cyber risks. Now, cyber risks are one of the top risks on the risk management radar for financial institutions.

To ensure that the new business model of teleworking/working from home is effective or successful, financial institutions are consistently relying on

outsourcing to save costs and buy readily available skills or services. Insurance companies have also followed this trend specially to cope with the increasing magnitude of changes required on the company to achieve results and the resultant reduction in the requirement for a "physical office" to provide insurance solutions. Thus, outsourcing presented a ready-made solution to cope with such changes. The benefits of outsourcing have long been studied and observed and the derived conclusion is that outsourcing is beneficial, and it almost always outweighs its cost.

Yet, as insurers outsource business tasks to these vendors, they are not outsourcing their risk. In the event a data breach occurs that compromises your data within a third party's system, your company is still responsible for everything that comes with a data breach, including compliance with regulating bodies, potential lawsuits, and related costs (Burke, 2020). In addition, the loss of use of the systems or platforms because of cyber-attacks can further magnify the Insurer's cost in returning to business as normal.

It is also more concerning for Insurers as they are viewed as the least ready industry when it comes to dealing with technology in comparison to their famous counterparts – banks. Banks were getting pummelled by cyber-attacks and needed to move quickly to protect their reputations, customers and bottom lines. However, attackers are moving on to find weaker targets and this is bringing insurance companies into the firing line. KPMG's recent global CEO outlook survey, in which more than half of the insurance CEOs surveyed (43%) said that their organization is fully prepared for a cyber event (KPMG, 2017).

Accounting literature in LDCs offers rich insights into how neo-liberal control practices are implicated in socio-political ramifications (Alawattage and Wickramasinghe, 2009; Hopper *et al.*, 2009; Metwally and Diab, 2021; Wickramasinghe and Hopper, 2005). However, we know little about the dynamics influencing the risk management and internal auditing professions in

emerging markets such as the Egyptian market. Additionally, little attention in the literature has been paid to studying risk managers' and internal auditors' roles and practices during the recent pandemic (i.e., the COVID-19 pandemic). Given the absence of comprehensive attempts to address RM everyday practices as a 'situated practice' in the pandemic time, this study examines how the emergence of COVID-19 has implications for both risk managers and internal auditors in an emerging market.

2. The Role of Governments and Regulators

The public is currently placing a significant responsibility on their governments and insurance regulators to regulate the whole COVID-19 impacts on their lives, especially in terms of health-related costs. In this respect, governments are expected to manage the full information dissemination cycle, advice on safety procedures, implement the required laws to mandate social distancing and manage COVID-19 infections till recovery. Regarding insurance regulators, they are expected to advise on coverage, underwriting, pricing, claims and any other issues that are potential areas of conflict.

There is a general belief among the public that when the government is not providing coverage, medical insurers should shoulder it. Thus, insurers should control the situation and consider the pricing of COVID-19 risks into their insurance coverage. As a starting point to manage the ensuing pricing, fraud, reputational and cyber risks, insurers need to look for new measures to be implemented by the government and regulators to preserve the provision of medical insurance, as stated in Table 1.

Table 1: **Example of governmental measures to preserve the provision of insurance**

Area	Example of measures
Product design, coverage and pricing	• Review products that may be impacted by COVID-19 to ensure they continue to meet customers' needs • Relax pricing requirements to improve the affordability of specific insurance products • Adjust insurance coverage due to movement restrictions e.g., accept claims arising from telemedicine services, simplify hospitalization claims processing • Provide accident, health, pension, medical and other insurance services on favorable terms to staff on the frontline of Covid-19 prevention and control • Reduce the cost-sharing of medical insurance
Underwriting and product distribution	• Require or allow more extensive use of technology and remote authentication to replace face-to-face underwriting processes • Require insurers to be flexible in providing or extending insurance coverage without complete paper documentation.
Policy servicing	• Allow deferral of premium payment or revised premium payment schedule without lapsing insurance policies of financially distressed individuals and businesses • Avoid triggering of policy cancellation, non-renewal of policies or denial of claims due to movement restrictions • Require insurers to clarify policy exclusions for pandemic

	events such as Covid-19 • Extend period within which insurers need to respond to complaints or queries by policyholders
Claims processing	• Adjust operational processes to accommodate virtual interaction with policyholders including simplifying or exempting requirements for paper-based claims submission • Expedite processing of valid insurance claims arising from Covid-19, including waiving waiting periods or providing flexibility in accepting proof of claims • Extend claims notification period by policyholders

Source: Yong (2020)

3. The Response of the Insurance Industry Worldwide

Claims activity across different insurance sectors makes it clear that companies of all sizes are experiencing substantial losses due to the unprecedented disruption of normal business operations (Banham, 2020). Given the ensuing rise in losses across different business lines, the insurance industry's response was to increase pricing. Globally, according to the Marsh Global Insurance Market Index, commercial insurance pricing increased by an average of 14% during the first quarter of 2020. This is the largest observed increase in the index since its inception in 2012 (Marsh, 2020). As regarding medical insurance, the position remains uncertain due to the lack of governmental enforcement on insurers to pay for medical expenses, as governments still bear the responsibility of spending on testing and treatment.

From risk management and internal control perspectives, the COVID-19 risk is not tolerated as part of a company's risk appetite. COVID-19 expenses will not be covered or even considered by insurers unless there is government

intervention. There have been rising pressures on governments to compel insurers to re-evaluate their positions. This pressure is more evident in other business lines, such as business interruption and travel insurance. Until governments formally announce that they will only cover a part of the incurred medical expenses or no expenses at all, medical insurers have no reason or motivation to change their current position concerning pricing. In this regard, the CEO of MarketScout Richard Kerr stated that "[l]ower exposure base and the possibility of governmental intervention in coverage application will have a dramatic impact on the pricing for the rest of the year" (Wilkinson, 2020). There might be an expected shift in governments' position when a vaccine is available, especially if the vaccine is costly.

4. Research Methodology

This study draws upon the qualitative research methodology to conduct an interpretive case study (Yin, 2013). Deploying this methodology is suitable for our research endeavour as it offers a better understanding of the context and how practitioners interpret their everyday contexts (See Burchell *et al.*, 1980). This is important in the current study that places a greater emphasis on the perceptions and explanations of the participants themselves (i.e., Chief Risk Officers (CROs), internal auditors and other risk officers) (Hopper and Powell, 1985). This helps us make sense of human actions or the meanings attached to people's issues in their daily context, hence the underlying social phenomena (Lukka, 2007; Vaivio, 2008). Following Yin's protocol for single studies, we defined our scope to be the Egyptian insurance sectors' internal auditor and risk officers in line with this methodology. Further, we deployed a data collection triangulation strategy to grasp the dynamics influencing the role of the internal auditors and risk managers and officers. The use of multiple methods is beneficial to get an in-depth understanding of the phenomenon in question. It provides a more robust substantiation of constructs and helps secure valid and reliable conclusions (Bryman, 2016). In particular, data are mainly collected using semi-structured

interviews, documentary analysis and Internet-based sources. The current study deploys a single case study approach.

Data collection was done in two phases: April-May 2021 (pilot study) and July-December 2021 (Main data collection phase) by telephone and skype conversations. The second phase data confirmed the initial data gathered previously. Interviews were tape-recorded whenever possible and were then transcribed. The time of the interview ranged from 1 hour to 2 hours depending on work circumstances and the time available of each interviewee. At the end of each interview, the authors were given interviewee(s) contact details so that s/he might be recalled later in the data analysis phase to understand any vague matters and follow-up any new events in their departments. We have conducted 23 interviews in the two stages of data collection. We conducted five interviews with CROs and internal auditors in three international companies and two local companies in the pilot phase. At that stage, the authors were curious to know about the impact of the COVID-19 pandemic on risk mapping, risk matrices, risk identification tools, stress testing, risk management, cyber risks, outsourcing process and corrective actions. The pilot study data were beneficial. It concentrated more on what we want in the main study (second round interviews), and our interviews were semi-structured (Bryman, 2016; Yin, 2013).

In the primary data collection phase, we conducted the remaining 18 semi-structured interviews (with 2 CROs, 12 internal auditors, two risk officers, and two accountants). Those people are from different companies to grasp the holistic idea of how risk officers and internal auditors see the impact of the COVID-19 pandemic and how they reacted to its uncertainties. We concentrated on participants whose practical experiences ranging from four to 25 years. The academic background of those participants was variant ranging from accountancy, management to actuarial statistics and risk management. The interview questions covered issues related to background information;

perception of risk management actions implemented by the organization before and after the COVID-19 pandemic; the role of external institutions, organizations, or governmental bodies in implementing risk management tools or measures during the pandemic; cyber risks, outsourcing process, fraud detection, fraud deterrence in this exceptional situation and the current legal requirements fulfilled by the organization.

The first author was granted the access to attend (Virtually through zoom and Microsoft teams) some of the risk management team meetings in three different companies and audit committee meeting in two companies. This allowed us to benefit from viewing various documents, ranging from Memos, booklets, risk maps, stress testing, issued policies, and letters sent to the governmental authorities and the western reinsurers (related to ERM) to local newspapers. Moreover, we reviewed the available Internet resources and literature about the impacts of the COVID-19 pandemic on the risk management profession, and internal auditing in the insurance sector. This included Marsh & McLennan Companies' pandemic reports, Deloitte, E&Y reports relating to risk management, and all the academic papers found concerning the pandemic impacts on insurance (e.g. Actuaries, 2020; Crovini *et al.*, 2021; El Baz and Ruel, 2021; Farooq *et al.*, 2021; Harris *et al.*, 2021; Ker, 2020; Kurt, 2021; Marsh, 2020; Metwally *et al.*, 2020; Naseeb *et al.*, 2021; Pagach and Kosmala, 2020; Richter and Wilson, 2020). This provided a rich source of information on the insurance sector and enhanced our understanding of enterprise RM systems.

Data analysis was conducted manually to maintain interviewees' words and phrases close to their cultural contexts and background, as electronic analysis programs fall short in this regard (Bryman, 2016). This abductive reasoning is essential to increase the validity of the reached themes and results (Lukka, 2007; Metwally, 2016; Mohamed and Metwally, 2019; Vaivio, 2008). Thus, the process of data analysis was based on extensive reading and re-reading of the interview notes and transcripts, which helped the researchers get a better 'feel'

for the data. The initially identified themes were broad categories developed from the theoretical framework, research questions, and data from several interviews (Metwally, 2016; Wickramasinghe, 2011). Then, the transcript parts relating to each identified theme were read again to identify the principal themes that share common ideas. The researchers started process during the early stages of interviews, so that the researchers can ask the interviewees about the identified ambiguities in the transcribed data.

5. Insurance Outsourced Services

If outsourcing is successful, Insurers can capitalize on their other existing capabilities and deliver a comprehensive service package to client. Insurers can specifically save time and focus on other immediate issues. For Insurance companies that strive to keep everything in-house typically end up developing a series of vertically integrated silos that result in extensive duplication and redundancy across businesses and markets the need for the enterprise risk management (ERM) (Metwally and Diab, 2021). ERM is currently a requirement by many rating institutions to fulfil both the rating and solvency II requirements (Metwally *et al.*, 2019). This tends to apply for both small and larger insurance companies (Finextra, 2020).

ERM provides a holistic view on the risks an Insurer is exposed to and since the vertical silos model is not economically feasible anymore, risk managers are moving towards integrating ERM as part of the evolved Insurance business models. To holistically identify the threat of cyber risk, risk managers must evaluate and obtain answers by asking such questions:

- Should said function be outsourced? Cost vs. benefit analysis
- Is this a core function? This includes:
  - Acquisition – the process of acquiring clients through meetings or through an in-person or online quotations system.

- Underwriting – the risk assessment and evaluation of an application form for acceptance or rejection.
- Policy issuance – the creation of an insurance policy and handing it over to the client.
- Policy management – the after-policy issuance stage which involves frequent communication and interaction with the client to either keep the client updated on their policy status or if the client elects to make adjustments to the policy.
- Claims – the formal request for compensation from the Insurer
- Claims Subrogation – a large sub-part of the claims function that involves collecting recoveries from third parties for losses caused to the Insurer's clients.

- Is this a non-core function? Such as human resources, legal services, Marketing and communications, Customer interaction, Finance, and IT
- Should we outsource the entire function (labelled as business process outsourcing- BPO) or an activity within the function only? For example, the recruitment process of HR or entire HR operations, Claims decisions on Insurance policies or the entire claims function.

All of the above will contribute to the magnitude of cyber risks facing the Insurer and Risk managers and internal auditors must carefully devise their strategies around this different way of working.

6. Cyber Risks in Insurance

According to the International Association of Insurance Supervisors (IAIS), cyber risk means: "Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be

caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information – be it related to individuals, companies, or governments" (IAIS, 2018).

The concerns surrounding cyber risk in an Insurer directly are already a significant risk, and so for an Insurer that also uses outsourcing there is an added dimension of the cost of the cyber risk due to engaging with the outsourcing provider. The European Insurance and Occupational Pensions Authority estimated an impact of around EUR 16 million on the balance sheet considering only ransomware attacks as part of cyber risk, whilst it can go up to 38 million when including both violation of IT system and breach of an outsourcing providers' information system – more than double the amount (EIPOA, 2019).

The case of Anthem Insurance company's data breaches also served as an invaluable lesson and as a strong example of the cost of cyber risk when they suffered a data security breach in January 2015. Around 78.8 million customers were affected, and Anthem had to pay out $2.5 million to engage expert consultants; $115 million for the implementation of security improvements; $31 million to provide initial notification to the public and affected individuals; and $112 million to provide credit protection to breach-impacted consumers (ADOI, 2016).

The mode of delivery of the outsourced service will determine how cyber risk is generated or how exposed is the Insurer to the cyber risk attack. Since the outsourced service or final deliverable is provided over the web, through the Cloud or online data storage application online, then cyber risk is generated here over the web. For example, it could be simply that the Insurer is using Microsoft 365 as the tool for email communication. One simple hack and this will cause numerous data and privacy breaches. The risk is even greater if the entire business function such as the claims process is initiated and completed over the

web by the outsourcing provider. Any access to such claims data can reveal vast amounts of information about the Insurer and the client.

Additionally, Insurers need to understand the disruption in service that can occur ex post (after the cyber-attack) and the alternative solutions to reduce the business interruption time. The dependency on the outsourcing provider will determine the severity of the interruption. The greater the risk, the stronger the attack and then longer time will be required to return back to usual business.

7. How Insurers Identify Risk Factors

The selection of the "right" outsourcing provider will determine the level of exposure to cyber risk. There are various risk factors that should be assessed and evaluated appropriately when choosing the outsourcing provider and those include:

1. Expertise
2. Previous assignments,
3. Cost
4. Approach to carrying out processes
5. Delivery mode of service
6. Personnel
7. Project management (integration) – in terms of how the outsourcing provider's business model integrates with that of the Insurer with minimal service disruption to clients
8. Previous incidents – information regarding magnitude of attack and the probable cost is of vital importance
9. Cyber risk attacks management (ex-ante)
10. Post attack management (ex-post)

The Insurer's experience in dealing with and the selection of outsourcing providers will have a larger advantage or a heads up in dealing with cyber risk in comparison to non-experienced or small Insurers.

8. The Impact of Fraud Risk

COVID-19 pandemic has become a catalyst for fraud in insurance, representing an additional risk to deal with when we come to risk management and internal auditing and control. Fraud problems can appear in fake medical testing kits, treatments or vaccinations, or fake travel insurance claims or any other forms relating to moving to teleworking. For example, in April 2020, Verisk showed a 14 percent increase in claims linked to providers with suspicious billing practices (Hulett, 2020). Authorities are now wary of potential scams. The same applies to insurers, so they are dedicating sections in their official communications or website to educate the public on this issue. In this regard, the FBI has issued a warning on its webpage, advising customers to check if they are billed for medical services that they did not receive and to check the accuracy of the date of such services (Pandemic, 2020). The present fraud schemes are complicating the situation for insurers, which increases the cost of the insurance. This can have implications for their policies: they must consider including this new risk in their pricing.

There are two types of pandemic-related fraud: internal and external fraud. Employees from inside the company perpetrate internal fraud. In contrast, external fraud emanates from regular customers outside the company (Jans *et al.*, 2009). Fraud risk mitigation and management should include both preventive and detective tools. Fraud risk can be deterred by applying an effective internal control system that, for example, separates the duties, ensures proper authorizations, enforces penalties, and makes the required reviews before any transaction is approved.

One challenge related to fraud risk in insurance is the requirement to meet the payment of insureds' claims efficiently and quickly when an insured's

catastrophe happens. The quickness of the payment is crucial, especially in certain types of insurance such as medical insurance, where people's lives are at stake (Csiszar and Heidrich, 2006). Having said this, the thorough review of fraud suspicion will take time and may cause a death of a patient in the hospital if the payment –which also might not be fraudulent – is delayed. This will result in clients' complaints against the insurance company (Derrig, 2002). If such action is recurrent, the company's reputation will be negatively affected, especially in small and connected communities. Thus, this fraud risk can cause reputational risk (Power *et al.*, 2009). To resolve this conundrum, most insurers seek trade-offs and negotiations with insureds. They mostly pay the negotiated claims to close the case under investigation, which is crucial to save their reputation in this local market.

Hence, fraud risk is more apparent in the Covid-19 situation. This represents another uncertainty (blind spot) for insurers, their internal auditors, and risk managers (Jovanović *et al.*, 2020). This situation is further impacted by the emerging changes such as the 'working from home' situation, and the present massive digital transformation in all the transactions that contributed to the ineffectiveness of the presently used traditional internal controls. In other words, conventional internal control tools over claim reviews and payments are insufficient, and sometimes are impractical, to face the massive digital transformation in the claim and payment cycle. This raises questions about the effectiveness of the technical and financial review of the claim files, the role of internal auditors in this new normal, and what sort of management control tools should be innovated to cope with this change. These questions and more are currently posed in the market, while most insurance and reinsurance companies are presently applying conventional techniques such as the management by exception model (Merchant and Otley, 2006). With the 'management by

exception' model, only red flags (Big claims) are thoroughly reviewed, while medium and small claims are processed with less rigid measures and reviews. This raises doubt about: what would happen if the situation changed and the Egyptian government, for example, made the payment of medical costs compulsory on insurance companies; and how insurers' capital adequacy and profits will be affected if this issue continued for some time.

9. Recommended Policy Solutions

It is now apparent that pricing risk represent an immediate risk that needs a quick intervention, especially after the historically-used risk models fall short in calculating the proper prices that contain proper conservative calculations of the impact of COVID-19. Many negotiations and trade-offs are made regarding claims payments and the expected accompanying frauds. Having said this, we see that insurers' responses to such risks could be enhanced through some proposed solutions. Firstly, insurers should establish a crisis management task force that directly reports to senior management. An insurer's task force should involve members from the risk management, underwriting, claims, and sales teams. This task force should focus on risk and response assessment, monitoring analysis and reporting, and crisis operation management and communication, as explained below in the following paragraphs (EY, 2020).

Insurers should identify risks and trends or best practices in risk management responses towards COVID-19 starting with pricing, cyber and fraud risks. Here, the task force should highlight the emerging issues in current business processes and propose solutions and new business models for overcoming them. Further, the task force should look at various measures to increase the insurer's resilience, especially with the resurgence of the coming waves of COVID-19. Testing current business continuity plans to measure resilience is vital. This can be done by activating short term emergency response (to limit the negative impact on the

health of employees or the public); crisis management (to ensure that key stakeholders retain confidence in the ongoing viability of the company); and business recovery (enabling the most important, value-generating parts of the company to recover, as quickly as possible).

Besides, it is crucial to monitor the evolution of the virus and the current risk management practices implemented, and analyze their effectiveness, starting with travel insurance as countries open their borders and resume flights again. On the pricing risk front, once the task force recommended a course of action, close monitoring of the new coverage and prices' impact is required. For fraud risks, most insurers are considering a move to online solutions. Because this is unfamiliar territory for most insurers in Egypt, the task force will need to consult with technology experts to ensure a similar or better delivery of services and avoid cyber fraud. Also, crisis operation management is needed through: testing of incidence response plans; revising key risks' impacts on working capital and liquidity; revising governance structure to maintain a strategic approach to crisis management; and identifying the minimum viable business models, critical controls, core processes, key customers, products and suppliers, etc. Further, communication with senior management and an organization's stakeholders is necessary to improve transparency and readiness in handling a crisis. This can be done through internal circulars to keep employees informed of the organization's stance on policy issuance.

Secondly, a supply chain analysis is necessary to identify the areas in which an insurer is likely to be hit due to pricing and fraud risks. Such an analysis will enable insurers to reduce exposure to such risks and answer questions like:

- How will your operational processes be impacted?
- How will the demand in the industry respond?
- Will customers continue to buy policies? Or pay for modified policies?

- How will the disruption in the supply chain affect you?

In return, insurers can design a risk management strategy and model to respond to these questions under a COVID-19 scenario. One of the popular implemented strategies is the Prevention, Preparedness, Response, and Recovery (PPRR) Strategy. If an insurer is operating largely on the digital front, then a cyber supply chain analysis is required, especially for cyber fraud risk. The problem with this recommendation under the COVID-19 scenario is that various assumptions can be incorporated into the model as this is an unprecedented situation for the entire industry. This may render the analysis probably inaccurate.

Thirdly, a comprehensive exercise will be required to update the insurer's risk management policy to cover COVID-19 pricing and fraud risks. Once these risks are clearly identified along with the subsequent impact on the business, insurers must update the risk management policy and cascade it to all relevant stakeholders. Here, they need to consider areas such as: categorizing the risks (under a pandemic scenario or otherwise); studying the current risk appetite framework; doing interconnectivity analysis-to other business risks; identifying key risk indicators and lines of defense; and reporting on the key applied controls.

Again, the readiness of an insurer's response to such risks is vital in these unprecedented circumstances. The sooner the policy is updated, the faster an insurer can recover.

Fourthly, to mitigate against cyber risks, Insurers should establish lines of defence in all stages of the relationship with the outsourcing provider.

1. Contract management

Prior to the selection of the outsourcing provider, all risk factors mentioned above should be weighted and evaluated carefully and any issues are identified

upfront. Surveys and studies from the International Association of Contract and Commercial Management have found that outsourcing customers can lose up to 9.2% of the value of contracts due to inefficient contract management (Horsfeldt, 2020). It can also lead to unnecessary legal costs and disputes.

Additionally, it is vital to negotiate minimal database access as part of the contract as some Insurers provide full access to their database where it is not needed.

2. Regular audits

Post contract inception audits from independent third-party who have the relevant core competencies especially if own Insurer's does not possess such capability will enable Insurers to identify any issues and gaps in managing cyber risk and implementing the recommendations to bridge such gaps.

Auditors will have to focus heavily on the channels used to deliver the outsourced service since this is where cyber attackers will target first. In a study done by Glasgow Caledonian University, the four most secured channels were identified and they are (Ikerionwu and Edgar, 2019):

- Email through dedicated server
- Remote access to client's server
- Dashboard on the cloud
- Teleconference

Auditors experienced in cyber risks will provide the best recommendations on this as selecting the best delivery model is determinate in controlling the risk exposure.

3. Cyber-attack simulations run through

Conducting penetration testing to identify weak spots in the end to end process between Insurer and outsourcing provider and it will help assess both parties readiness in the event of such attacks. Various consultants provide

comprehensive solutions on the same and can be engaged easily to conduct such tests. Simulations cover various types of attacks such as reconnaissance, denial of service, phishing, malware and ransomware testing, espionage detection & Containment. Engaging experts can also provide an experienced point of view of attacks on the outsourcing providers' systems for the Insurer to consider.

Banks, insurers, asset managers and suchlike should also ensure that they have effective alert systems in place so that they know as and when possible cyber breaches are occurring, including log aggregators that are able to work with big data and sophisticated analytics. Such devices can help to minimise threatening probes.

4. Business continuation tests to build resilience

Risk managers usually design BCP (business continuity plans) on an overall enterprise risk level. However, Insurers will also need to participate and run business continuation tests with their outsourcing providers to ensure preparedness against any cyber-attack as part of their ongoing monitoring process. In doing so, Insurers not only ensure preparedness but also build resilience which is now becoming the required trait especially post COVID-19. Resilient organizations maintain robust production capacity that can both flex to meet changes in demand as well as remain stable in the face of operational disruption, all without sacrificing quality. They also fortify both their supply chains and delivery mechanisms to maintain operational capacity and the provision of goods and services to customers, even under stress of all forms ranging from failures of individual suppliers or distributors to natural catastrophes to geopolitical events.

10. Conclusion

In this exploratory study, we concentrated on pricing, cyber, and fraud risks relating to the emergence of the COVID-19 pandemic. Our main concern was the impacts on the Egyptian insurance sector. We clarified how the COVID-19

pandemic has brought about disruptions across different industries worldwide, and in Egypt as well. In response to this pandemic, governments around the world have developed specific measures to preserve the insurance industry from COVID-19 risks. However, this can only work in the short term, while the world is gearing for a third and fourth probable wave of the coronavirus. Hence, the situation remains unclear for medical insurers, with the pricing risk looming over. When more data becomes available, it will unravel whether they are ready for managing the emerging threats.

Additionally, we clarified that there is increased fraud and cyber risks due to the emergence of COVID-19 related challenges. We argued that the fraud risk in insurance is more complex to manage, as people's lives are at stake especially in health insurance, and the time is a crucial factor in saving their lives. The presently used internal cont1rol systems have many deficiencies in coping with emerging risks. Applying authorization, separations of duties, and traditionally used control measures cannot help internal auditors and risk managers (who are currently working from home) to face the present control deficiencies and the related fraud risk. Moreover, fraud risk is mostly connected to a delay of payment to hospitalized insureds, which can eventually result in reputational risk. This might force insurers to forgo the critical action of making the required in-depth analysis and investigations to discover the expected fraud, not to sacrifice their reputation or to minimize the expected reputational risk. Most insurers in Egypt resolve this dilemma by paying the claim and closing the case under investigation.

Lastly, risk managers and internal auditors will have to formulate a clear strategy for approaching the subject of cyber and fraud risks. This will require further research looking perhaps at how the entire world responds to that issue. For travel insurance, risk managers must move faster since borders are re-opening to revive the travel industry. Relatedly, many companies are currently introducing COVID-19 travel coverage. Likewise, chances for fraud will

increase since there are numerous COVID testing scams. Therefore, with the emergence of new vaccines, it is likely that fake vaccine scam efforts will be heightened. Overall, a vaccine will present managers with another subset of risks to tackle as part of dealing with the pandemic.

These risks require quick practical solutions as many chief risk officers and internal auditors in Egypt and worldwide expect that this pandemic's impacts will continue for two more years or so. Having said this, we recommended some actions that represent potential recommended policy solutions to deal with both pricing, cyber, and fraud risks in this changing blurred uncertain situation. As previously clarified in detail, these suggestions are related to establishing a crisis management task force; conducting a supply chain analysis to strengthen defenses; formulating different scenario analyses of the impact of incorporating the COVID-19 cost within prices and resultant profitability (pricing risk); and finally, updating the risk management policy with a required thorough revision once the vaccine is ready for use.

References

Actuaries, A. A. o. (2020), "Drivers of 2021 health insurance premium changes: the effects of COVID-19", available at: https://www.actuary.org/node/13629#_ftn15 (accessed 3/2/2022).

ADOI. (2016), "Regulatory Settlement agreement", available at: https://www.commerce.alaska.gov/web/Portals/11/Pub/Companies/Exams/MCE16-09.pdf?ver=2016-12-12-083253-927 (accessed).

Alawattage, C. and Wickramasinghe, D. (2009), "Institutionalisation of control and accounting for bonded labour in colonial plantations: A historical analysis", Critical Perspectives on Accounting, Vol. 20 No. 6, pp. 701-715.

Atlas, M. (2020a), "Aviation insurance in turmoil", available at: https://www.atlas-mag.net/en/issue/turbulence-in-aviation-insurance (accessed 3/2/2022).

Atlas, M. (2020b), "Coronavirus: Kenyan insurers cover health costs", available at: https://www.atlas-mag.net/en/article/covid-19-prudential-uganda-and-goldstar-insurance-to-launch-new-product (accessed 3/2/2022).

Banham, R. (2020), "he impact of COVID-19 on Insurance Markets', Risk Management Magazine", available at: http://www.rmmagazine. com/2020/06/01/the-impact-of-covid-19-on-insurance-markets/ (accessed 2/2/2022).

Bhimani, A. (2009), "Risk management, corporate governance and management accounting: emerging interdependencies", Management Accounting Research, Vol. 20 No. 1, pp. 2-5.

Bryman, A. (2016), Social Research Methods, Oxford University Press, Oxford.

Burchell, S., Clubb, C., Hopwood, A., Hughes, J. and Nahapiet, J. (1980), "The roles of accounting in organizations and society", Accounting, Organizations and Society, Vol. 5 No. 1, pp. 5-27.

Burke, D. (2020), "You Can Outsource a Service, but Not Cyber Risk", available at: https://woodruffsawyer.com/cyber-liability/you-can-outsource-service-not-cyber-risk/ (accessed 2/2/2022).

Butaru, F., Chen, Q., Clark, B., Das, S., Lo, A. W. and Siddique, A. (2016), "Risk and risk management in the credit card industry", Journal of Banking & Finance, Vol. 72, pp. 218-239.

Crovini, C., Schaper, S. and Simoni, L. (2021), "Dynamic accountability and the role of risk reporting during a global pandemic", Accounting, Auditing & Accountability Journal, Vol. ahead-of-print No. ahead-of-print.

Csiszar, E. and Heidrich, G. W. (2006), "The Question of Reputational Risk: Perspectives From An Industry", The Geneva Papers on Risk and Insurance - Issues and Practice, Vol. 31 No. 3, pp. 382-394.

Derrig, R. A. (2002), "Insurance Fraud", Journal of Risk and Insurance, Vol. 69 No. 3, pp. 271-287.

EIPOA. (2019), "Cyber risk for insurers – challenges and opportunities", in. EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY, pp. 1-30.

El Baz, J. and Ruel, S. (2021), "Can supply chain risk management practices mitigate the disruption impacts on supply chains' resilience and robustness? Evidence from an empirical survey in a COVID-19 outbreak era", International Journal of Production Economics, Vol. 233, pp. 107972.

EY. (2020), "How to safeguard your business with COVID-19 risk management tactics", available at: https://www.ey.com/en_be/covid-19/how-to-safeguard-your-business-with-covid-19-risk-management-tactics (accessed 2/2/2022).

Farooq, U., Nasir, A., Bilal and Quddoos, M. U. (2021), "The impact of COVID-19 pandemic on abnormal returns of insurance firms: a cross-country evidence", Applied Economics, Vol. 53 No. 31, pp. 3658-3678.

Finextra. (2020), "Decoding Outsourcing Within the Insurance Industry", available at: https://www.finextra.com/blogposting/19279/decoding-outsourcing-within-the-insurance-industry (accessed 2/2/2022).

Harris, T. F., Yelowitz, A. and Courtemanche, C. (2021), "Did COVID-19 change life insurance offerings?", Journal of Risk and Insurance, Vol. In Press, pp. 1-31.

Hopper, T. and Bui, B. (2016), "Has management accounting research been critical?", Management Accounting Research, Vol. 31, pp. 10-30.

Hopper, T., Graham, C., Tsamenyi, M., Uddin, S. and Wickramasinghe, D. (2009), "Management accounting in less developed countries: what is known and needs knowing", Accounting, Auditing & Accountability Journal, Vol. 22 No. 3, pp. 469-514.

Hopper, T. and Powell, A. (1985), "Making sense of research into the organizational and social aspects of management accounting: A review of its underlying assumptions [1]", Journal of Management Studies, Vol. 22 No. 5, pp. 429-465.

Horsfeldt, O. (2020), "Contract management in outsourced enterprises", available at:https://uk.practicallaw.thomsonreuters.com/w-010-7943? Transition Type=Default&contextData=(sc.Default)&firstPage=true(accessed4/2/2022).

Huber, C. and Scheytt, T. (2013), "The dispositif of risk management: reconstructing risk management after the financial crisis", Management Accounting Research, Vol. 24 No. 2, pp. 88-99.

Hulett, J. (2020), "Insurance fraud detection in action: Identifying suspicious medical billing during the COVID-19 crisis", available at: https://www.verisk.com/insurance/visualize/insurance-fraud-detection-in-action-identifying-suspicious-medical-billing-during-the-covid-19-crisis/ (accessed 2/2/2022).

IAIS. (2018), "Draft Application Paper on Supervision of Insurer Cybersecurity'", in IAIS (Ed.). IAIS, pp. 1-59.

Ikerionwu, C. and Edgar, D. (2019), "Secured service delivery model for outsourced services in a business process outsourcing relationship", International Journal of Information Communication Sciences, Vol. 4 No. 1, pp. 7-17.

Jans, M., Lybaert, N. and Vanhoof, K. (2009), "A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR 2 Framework", International Journal of Digital Accounting Research, Vol. 9 No. 1, pp. 1-29.

Jovanović, A., Klimek, P., Renn, O., Schneider, R., Øien, K., Brown, J., DiGennaro, M., Liu, Y., Pfau, V. and Jelić, M. (2020), "Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards", Environment Systems Decisions, Vol. 40, pp. 252-286.

Ker, A. P. (2020), "Risk management in Canada's agricultural sector in light of COVID-19", Vol. 68 No. 2, pp. 251-258.

KPMG. (2017), "Closing the Gap: Cyber security and the Insurance sector", available at: https://assets.kpmg/content/dam/kpmg/ae/pdf/closing-the-gap.pdf (accessed 2/2/2022 2022).

Kurt, Y. (2021), "Diffusion of the Airport Health Accreditation Program in the COVID-19 period: An Assessment with Institutional Logic and Legitimacy Approach", Journal of Air Transport Management, Vol. 94, pp. 102078.

Lukka, K. (2007), "Management accounting change and stability: loosely coupled rules and routines in action", Management Accounting Research, Vol. 18 No. 1, pp. 76-101.

Marsh. (2020), "COVID-19: evolving insurance and risk management implications", available at: https://coronavirus. marsh.com/us/en/ insights/research-and-briefings/covid-19-evolving-insurance-risk-management-implications.html (accessed 3/2/2022).

Merchant, K. A. and Otley, D. T. (2006), "A Review of the Literature on Control and Accountability", in Chapman, C. S., Hopwood, A. G. and

Shields, M. D. (Eds.), Handbooks of Management Accounting Research. Elsevier, pp. 785-802.

Metwally, A., Ali, H., Diab, A. A. and Hussainey, K. (2019), "The hype of risk-based management control: a phronetic approach", Risk Governance and Control: Financial Markets & Institutions, Vol. 9 No. 2, pp. 18-33.

Metwally, A., Ali, S. and Mohamed, A. (2020), "Resilience and agility as indispensable conditions for sustaining viable supply chain during pandemics: the case of Bahrain", in 2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI). IEEE Explore, University of Bahrain, pp. 1-5.

Metwally, A. and Diab, A. (2021), "Risk-based management control resistance in a context of institutional complexity: evidence from an emerging economy", Journal of Accounting & Organizational Change, Vol. 17 No. 3, pp. 416-435.

Metwally, A., Diab, A. and Mohamed, M. (2021), "Telework operationalization through internal CSR, governmentality, and accountability during the Covid -19: evidence from a developing country", International Journal of Organizational Analysis, Vol. ahead-of-print No. ahead-of-print.

Metwally, A. M. (2016), "Making sense of a story: illustrations from a case study of enterprise risk management", NSBM Journal of Management, Vol. 2 No. 2, pp. 1-22.

Mohamed, M. K. and Metwally, A. B. M. (2019), "Qualitative/Quantitative Methodological Dilemma in Accounting Research: Whence and Whither?", الفكر المحاسبي, Vol. 23 No. 3, pp. 702-736.

Naseeb, H., Diab, A. and Metwally, A. (2021), "The impact of the COVID – 19 pandemic on medical and travel insurance pricing and fraud risks: an exploratory study", Journal of Risk Management in Financial Institutions, Vol. 14 No. 1, pp. 59-71.

Pagach, D. and Kosmala, M. (2020), "The Challenges and Opportunities for ERM Post-COVID-19: Agendas for Future Research", Journal of Risk and Financial Management, Vol. 13 No. 12, pp. 1-10.

Pandemic, F. W. o. E. H. C. F. S. R. t. C.-. (2020), "FBI Warns of Emerging Health Care Fraud Schemes Related to COVID-19 Pandemic", available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-emerging-health-care-fraud-schemes-related-to-covid-19-pandemic (accessed 2/2/2022).

Power, M., Scheytt, T., Soin, K. and Sahlin, K. (2009), "Reputational Risk as a Logic of Organizing in Late Modernity", Organization Studies, Vol. 30 No. 2-3, pp. 301-324.

Richter, A. and Wilson, T. C. (2020), "Covid-19: implications for insurer risk management and the insurability of pandemic risk", The Geneva Risk and Insurance Review, Vol. 45 No. 2, pp. 171-199.

Soin, K. and Collier, P. (2013), "Risk and risk management in management accounting and control", Management Accounting Research, Vol. 24 No. 2, pp. 82-87.

Tallaki, M. and Bracci, E. (2021), "Risk allocation, transfer and management in public–private partnership and private finance initiatives: a systematic literature review", International Journal of Public Sector Management, Vol. ahead-of-print No. ahead-of-print.

Tekathen, M. and Dechow, N. (2013), "Enterprise risk management and continuous re-alignment in the pursuit of accountability: A German case", Management Accounting Research, Vol. 24 No. 2, pp. 100-121.

Vaivio, J. (2008), "Qualitative management accounting research: rationale, pitfalls and potential", Qualitative Research in Accounting & Management, Vol. 5 No. 1, pp. 64-86.

Vinnari, E. and Skaebaek, P. (2014), "The uncertainties of risk management A field study on risk management internal audit practices in a finnish municipality", Accounting Auditing & Accountability Journal, Vol. 27 No. 3, pp. 489-526.

Wickramasinghe, D. (2011), "Ontological dependency on epistemology strategy: interpretive management accounting research revisited", in M.G., A.-

K. (Ed.), Review of Management Accounting Research. Palgrave Macmillan, London, pp. 543-566.

Wickramasinghe, D. and Hopper, T. (2005), "A cultural political economy of management accounting controls: a case study of a textile Mill in a traditional Sinhalese village", Critical Perspectives on Accounting, Vol. 16 No. 4, pp. 473-503.

Wiengarten, F., Humphreys, P., Gimenez, C. and McIvor, R. (2016), "Risk, risk management practices, and the success of supply chain integration", International Journal of Production Economics, Vol. 171, pp. 361-370.

Wilkinson, C. (2020), "Pricing impact of COVID-19 likely 'dramatic': MarketScout", available at: https://www. Businessinsurance .com/article/20200406/NEWS06/912333887/US-commercial-insurance-pricing-impact-of-COVID-19-likely-%E2%80%98dramatic%E2%80%99-MarketScout (accessed 4/2/2022).

Yin, R. (2013), Case Study Research: Design and Methods, Sage Publications, New York.

Yong, J. (2020), "Insurance regulatory measures in response to COVID-19', Financial Stability Institute", available at: https://www.bis.org/fsi/fsibriefs4.pdf (accessed 3/2/2022).