INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN PROGRESSIVE EDUCATION & DEVELOPMENT

OPEN ACCESS JOURNAL

Vol 12, Issue 4, (2023) E-ISSN: 2226-6348

Hybrid Working Post COVID Pandemic: A Change in Organisation Governance and Its Impact on the Control Environment

Emmanuel Lumbwe[1], Asif Mahbub Karim[2] and Joseph Adaikalam[3]

[1]PhD Researcher, Binary University of Management & Entrepreneurship, Malaysia, [2]Professor & Dean, Binary Graduate School, Binary University of Management & Entrepreneurship, [3]Founder and Executive Chairman, Binary University of Management & Entrepreneurship, Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARPED/v12-i4/19708 DOI:10.6007/IJARPED/v12-i4/19708

Published Online: 30 November 2023

Abstract

The post COVID-19 return to normal way of life has brought in new challenges in the way organisations restructure their workspace and the governance that supports day-to-day operations. During the pandemic new strategies were deployed by most organisations across the world for the purpose of business continuity. Remote work, in particular working from home, was adopted by most organisations using different work platforms that included virtual (electronic) workspaces and meeting rooms (e.g., Zoom and Microsoft Teams). Staff remotely accessed electronic systems that included financial management systems. This brought a lot of stress on businesses in relation to their information technology infrastructure and increased related costs.

With the subsiding of COVID and the return to normalcy, a lot of organisations and staff are suggesting that organizations allow a hybrid work environment. This is the practice of alternating between working from home and working in the office. Hybrid working environments may create several control issues, including cyber security / cyber fraud risks which may lead to operational risks and financial risks.

The purpose of this paper is to review the impact of this change in operating style on organisational governance and how it has impacted the control environment in various organizations across the world. It also seeks to provide insight on the impact flexible internal controls has on work for both companies and employees.

Keywords: Business Continuity, Cyber Security, Fraud Risks, Operational Risks Management, Financial Risk, Organisation Governance, Control Environment.

Introduction

The COVID-19 pandemic compulsory made the world to close and progressed most companies' employees across the global to work remotely from home (Hossain et al., 2020). This led to the deployments of Technology for business continuity amid the pandemic. With the world slowly opening, The Centers for Disease Control and Prevention (CDC) issued new

guidance which indicates that COVID-19 continues to circulate globally, however, with so many tools available for reducing Its severity, that there is significantly less risk of severe illness, hospitalization and death compared to earlier in the pandemic. The guidance acknowledges that the pandemic is not over, but the tools available help the world move to a point where COVID-19 no longer severely disrupts our daily lives (Massetti, 2022).
With this, most organisations are using blended hybrid working to avoid having employees in the same space though the threat of contraction has reduced as guided by (CDC, 2022). Different work platforms that included virtual (electronic) workspaces and meeting rooms (e.g., Zoom and Microsoft Teams). Staff remotely access electronic systems that included financial management systems. This has brought a lot of stress on businesses in relation to their information technology infrastructure, internal controls pivoting and increased related costs.

Literature Review

Hybrid working is a flexible form of working that allows employees to split their time between working in the office and working remotely, usually from home. Hybrid working offers significant benefits for both the employer and the employee. The significant change in the usual way of managing an organisation influences the Organisation behaviour and ultimately on its performance.

Brooks (2009) defines Organisational behaviour (OB) as the study of human behaviour in organisational contexts, with a focus on individual and group processes and actions. Hence, it involves an exploration of organisational and managerial processes in the dynamic context of the organisation and is primarily concerned with the human implications of such activity.

Business Continuity (BCP)

According to Hopkin (2018) defines Business continuity has the way an organization prepares for future incidents that could jeopardize its existence. The range of incidents that should be covered will include everything from local events like fires through to regional disruption such as earthquakes or national security incidents and extend to international events like terrorism and pandemics.
Pandemic contingency plans for an organization should aim to ensure continuity of essential operations during an extended period of high illness rates in the workforce, suppliers, and customers. It should ensure that employees are not exposed to a high risk of infection in their workplace and aim to resume operations rapidly and competitively as soon as the pandemic cycle is over. Critical business processes can be protected by allocating additional back-up personnel, diversifying activities across multiple locations, and maximizing home-based working. Additional investments in training more personnel to take over essential roles and improving IT capability (Al Qalhati et al., 2020). Plans should anticipate that suppliers, equipment providers and support companies will be unable to function for some time, and stockpiles of essential supplies should be established. Telecommunications infrastructure may be unable to cope with the greatly increased demand. During a pandemic, employees are likely to become infected from their families, their children, or contacts outside the workplace. Social contacts in the workplace then spread infection through the workforce. Lower-contact work environment practices that minimize the risk of infection spread include a well-informed workforce, fewer face-to-face meetings, rigorous hygiene, and frequent biological cleaning of common area surfaces. Ultimately it may be necessary to close offices

to prevent the spread of a virulent virus. Staff who recover from a case of pandemic influenza are unlikely to catch it again and are no longer infectious to others. Recovered and vaccinated staff can return to work. As the pandemic subsides, resuming operations rapidly and efficiently could become a competitive issue.

Cyber Security

According to CISCO (2022), it defines Cybersecurity as the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative (Mughairi et al., 2019).

Cybersecurity, also known as information security (IS), can be considered a subset of, or a complementary subject to, information technology (IT) risks and controls because of their interdependent operations yet often separate leadership. Cybersecurity controls include the policies, processes, tools, and personnel for ensuring an organization's information resources are adequately protected from many types of attacks, detecting when such attacks occur, and remediating deficiencies as effectively as possible expressed in one significant framework as the following five functions: Identify, Protect, Detect, Respond, and Recover. In the broadest sense, IT or IS teams may manage cybersecurity risks and controls, depending on the process under review and the organization's unique environment (KPMG, 2022). Cybersecurity operations refer to controls that generally prevent or detect cyberattacks and are typically managed by IS rather than IT personnel. Nevertheless, cybersecurity operations controls are often embedded within systems planning, building, and monitoring processes managed by the IT department (IMF, 2022).

Cybersecurity operations can be broadly categorized according to three high-level control objectives such as Security in design in Operation contributes to the IS leader or function to governance, risk management, and IT-managed control processes ensure adequate protection of data and resources. Prevention Technologies like encryption, email and network filters, and antivirus and data loss prevention software aim to thwart attempts to misuse or disrupt information resources or communications. Cybersecurity awareness training also helps employees understand their role in protecting the organization's resources and reduces the likelihood that they will fall victim to social engineering or other malicious tactics. Detection is another tools and processes such as cybersecurity monitoring which includes event log monitoring and forensic analysis of system outages or anomalies, vulnerability management, and penetration testing identify control weaknesses or the presence of entities or objects acting maliciously in the computing environment so that they can be addressed.

Stakeholders, primarily an organization's governing body and senior management, rely on independent, objective, and competent assurance services to verify whether cybersecurity operations controls are well-designed and effectively and efficiently implemented. The internal audit activity adds value to the organization when it provides such services in conformance with the Standards and with references to widely accepted control frameworks, particularly those expressly used by the organization's IT and IS (Theiia, 2022).

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber-attacks. COVID-19 disrupted businesses quickly and drove teams to remote working and serving customers through online interactions, this digital world has become more at risk. Organisations need to consider how to secure new remote working practices while ensuring critical business functions are operating without interruption, and how to keep the business protected from attackers exploiting the uncertainty of the situation.

According to (Deloitte, 2020) Information security during COVID 19 was and is still of paramount importance to effectively prevent fraud. Some basic measures should be considered, and these include amongst others, are Preventing the use of external storage media and in instances where this is unavoidable these should be encrypted using stringent passwords and kept under lock and key (ideally external storage media should be avoided),Prohibiting the use of personal email accounts to receive or distribute official company correspondence and data, Ensuring guidelines and protocols are in place for employee participation in video and audio conference calls to ensure privacy and confidentiality during lockdown periods. With the increased use of home Wi-Fi networks there should be focused communications regarding the use of password protected services and that specific security measures should be in place to prevent unauthorised access to home Wi-Fi networks. Further, printing of official company documentation take place at home there should be protocols in place regarding storage and subsequent secure and confidential destruction in line with each organisation's specific policies and guidelines. These unprecedented times will be hard on people, organisations, and governments. It is extremely difficult for organisations to navigate these unclear situations. However, it is important to keep an open eye for cybercrime and financial crime which can make the situation worse. Existing controls and procedures should at least remain intact, and when in doubt take a step back, think and consult.

Further, Walton (2022) indicates that as Covid-19 restrictions ease and offices reopen, many businesses are showing a preference towards maintaining some degree of flexible working. Commonly referred to as 'hybrid working', the new model sees a return to the office, but with the option of remote working where it suits both employees and managers. While this arrangement promises many benefits, such as increased employee wellbeing, improved productivity and better collaboration, businesses should be careful to factor in cyber security risks when laying out a hybrid working policy.

Board of directors should critically analyse the new models of working, by Assess the risks, and plan around them, focus in on identity management, formalise your hybrid cyber security culture as people and businesses have become increasingly reliant on video chatting since the coronavirus pandemic began, for example Zoom bombing incidents were reported to be on the Increase. A disruption specific to the teleconferencing app Zoom, which has recently surged in popularity, this vulnerability has been exploited by hackers, with disturbing results. For instance, uninvited strangers crashed a Zoom meeting on cyberattacks.

When the presenter started covering coronavirus disinformation posted to Reddit, Facebook, and Twitter, a Zoom bomber scribbled all over the screen, forcing the meeting to end early. Zoom hacking issues like this are happening all over the world,

from over-the-Internet meetings to sensitive high-level government gatherings (Fortune, 2022).

Fraud Risks

The Certified Fraud Examiners and Thornton (2021) completed a survey with anti-fraud professionals around the globe regarding the current and expected effects of COVID-19 on the fraud landscape and (51%) indicated that their organization has uncovered more fraud than usual since the onset of the pandemic, with one-fifth indicating a significant increase in the amount of fraud detected. In contrast, only 14% of respondents' organizations have uncovered less fraud during this time. The study indicates an expected increases in all types of fraud risks; more than half of respondents expected to see increases in every category except one (financial statement fraud). Cyber fraud (e.g., business email compromise, hacking, ransomware, and malware) and social engineering (e.g., phishing, brandjacking, and baiting) are the categories most expected to increase, with more than 80% of respondents anticipating growth in these two risk areas.

Other risks projected to see large increases include identity crime (e.g., identity theft, synthetic identity schemes, and account takeovers), unemployment fraud, and payment fraud (e.g., credit card fraud and fraudulent mobile payments). In contrast, the three categories with the lowest percentage of respondents expecting an increase are the three primary categories of internal or occupational fraud: employee embezzlement (54%), bribery and corruption (52%), and financial statement fraud (47%).

Weitz (2022) in a joint research report by the Internal Audit Foundation and Kroll, Fraud and the pandemic Internal Audit stepping up to the challenge, indicates that there is a change in the landscape in fraud risk management during the pandemic. With a shift in the nature of fraud to an uptick in frauds involving social media and cyberattacks, with people taking advantage of the pandemic to scam members of the public and employees of their organizations.

For example, people selling the "cure" for the virus, and others preying on the fear that was so prevalent at the beginning of the pandemic to exploit human vulnerabilities in control frameworks. Fraudsters took advantage of the pandemic to utilize technology in a more coordinated way to target companies and individuals, and phishing, cyberattacks, and social engineering increased in sophistication with new techniques exposing organizations to increased risk.

Remote working environment presented additional challenges that can lead to more fraud — particularly the inability to have any visibility over staff members or consultants, which resulted in the opportunity to misrepresent working hours without any real oversight. The difficulties of effectively managing people in a fragmented remote environment were also seen to directly impact culture, which some participants cite as key in terms of fraud prevention. Remote working was further cited to dilution or weakening of the internal control framework resulting from a change in working environment due to layoffs, furlough, and the lack of a consistent team. This has presented issues to reassess the procedures and processes. The survey noted an increase in forged documents presenting additional risk, both from a "fake CEO"3 fraud perspective and relating to third-party contracts being faked which allowed funds to be extracted from the business.

There was an acknowledgment from certain participants that fraud risks were not created as a direct result of the pandemic but had either been accelerated and had evolved because of the opportunities presented by the pandemic, or in some cases had revealed themselves through a change of focus and through management being forced to consider things from a different angle.

Data obtained from the LinkedIn poll and through the polling questions during the focus groups was consistent with the points in the discussion cyber/phishing fraud was the most prevalent increase across the board, with 54% of respondents stating that they noticed an increase in these kinds of instances.

The second most prevalent area was misappropriation of assets, with 12% of poll respondents saying that they experienced an increase in frauds relating to asset misappropriation. The pandemic could have a long-term positive impact on both fraud risk management and the value of internal audit through driving strategic change in the governance structures and encouraging more investment in fraud risk management to respond to the changing environment

Operational Risks Management

Operational Risk Management (ORM) is defined as the possibility of losses resulting from external events or failures; deficiency; or inadequacy of internal processes, people, or systems, including the legal risk associated with inadequacy or deficiency in contracts. The COVID 19 pandemic strained most organisations Operations Risk Management as normal operations were disrupted and businesses needed to adopt agile and robust processes for their procurement, supply chain, people management and security strengths and weaknesses.

Lambin and Maes (2021) of Price Waterhouse argues that organisations had to act as fast as possible to ensure business continuity. Because of their preparedness and flexibility, some dealt with the crisis better and even saw it as an opportunity for transformation and the creation of innovative products or services. Since then, operations, digitalisation, cybersecurity, risk management.

The Operations Risk Management was further noted by Weitz (2022) in the pandemic who identified another theme that was recognised as a challenge relating to visibility over the supply chain to ensure the quality and quantity of the supply of key goods. This was particularly highlighted in the medical supply industry, as supplies were in such high demand that new solutions had to be sought to meet the demand, which presented opportunity not only for excessive profiteering but also for exploiting the high demand and required quick turnaround to subject an organization to fraud. In some cases, this was compounded by a challenge in identifying fraudulent transactions due to fluctuating prices in supply chains, which meant that traditional analytical techniques were ineffective. The challenges faced by a reduction in visibility through the supply chain presented a further risk of third-party fraud and an increased risk of employee misappropriation of assets due to weaker physical controls over inventory and supply chain challenges that left the organization open to potential exploitation.

Lambin and Maes (2021) further suggests that Its time organisations reflect on what made them survive, work on innovation, fail on some aspects or shut down certain units or even entirely. These experiences should be capitalised and enhanced because the sustainability, resilience, and flexibility criteria you will embed in your strategy as of now are greatly influenced by the COVID-19 crisis. Organisations should ask the following questions, what

were the positive aspects of the crisis? What were the main issues encountered when taking action to face the pandemic? In case of limited possibility to act, what were the causes? Based on the previous answer, what should be the areas of improvement? What should be changed in the future, so the business's ORM strategy upgrades and strengthens?

Financial Risk

According to a 2020 Deloitte study, Managing and responding in times of crisis, Companies across various industries are experiencing increased operational and financial pressure due to the COVID-19 pandemic. These pressures create a heightened level of financial risks such as Significant reduction in trading, Loss in revenue, Loss in profits, Loss in market demand, Going concern and Liquidation and total collapse. These financial risks may lead to increased motivation or justification to commit fraud, through manipulation of financial results, misrepresentation of facts, misappropriation of assets and other fraud schemes (Jamadar et al., 2022).

While cyberattacks in high-income countries tend to make headlines, less attention is paid to the growing number of attacks on softer targets in low- and lower-middle-income countries. In October 2020 hack of Uganda's largest mobile money networks, MTN and Airtel, for example, resulted in a major four-day disruption of service transactions. The global financial system has become more vulnerable as innovation, competition, and the pandemic further fuel the digital revolution. Although many threat actors are focused on making money, the number of purely disruptive and destructive attacks has been increasing; furthermore, those who learn how to steal also learn about the financial system's networks and operations (Maurer and Nelson, 2022).

Organisation Governance

Eklund (2021) in his research the COVID-19 lessons learned for business and governance, indicates that the most immediate concern for the board of directors (BOD) should be the health and well-being of the employees and they should realize that employees are the human capital, not an expense. That is, the employees are the intellectual asset of the company. To create trust, executives needed to demonstrate leadership, fairness, transparency, and open, honest, and timely communication to all stakeholders (Jamadar et al., 2021). Further that the BOD should see this crisis as an opportunity to acknowledge the vulnerabilities of their organization and act for a change. Post-COVID-19, we are in a moment of change to more resilient, sustainable, and fairer companies. To do so, BOD should take a holistic approach and change their focus from 'shareholderism' to 'stakeholderism', develop sustainable value chains and partnerships, restructure their corporate governance mechanism for sustainability, learn to manage new upcoming risk and opportunities, have a succession plan for the critical employees, such as CEO and directors, and develop circular and sustainable strategies (Hossain et al., 2022).

Control Environment

Deloitte (2020) the increase in remote work and other things will bring about major changes in processes and interfaces. This has repercussions for process risks, the suitability of established controls, and ultimately the general effectiveness of the Internal Controls.
In the Covid 19 and Fraud Risk: Managing and responding in times of crisis paper, they advise that reliable Internal Controls during the COVID crisis may include, Revaluation of the scoping

and the process risks, e.g., for non-routine processes (issue of hardware, remote work cybersecurity),Design and implementation of suitable remote controls, Modification of responsibilities (deputization rules, etc.),Introduction of an alternative form of evidencing performance of remote controls, Flexible implementation of key controls taking the deadlines of the external auditor into account ,Dialog with shared service centres; if necessary, development of contingency plans for outsourced processes, and Early and continuous coordination with the external auditor.

Companies with well-developed control automation will have to cope with different challenges than organizations with mostly manual controls (Alshams et al., 2019). Remote monitoring and reporting Even with the monitoring and reporting of the Internal Controls, a response is necessary whenever short-term changes in the processes and controls occur. Examples include, Increased performance of control tests remotely, Additional risk-based sampling (e.g., focus on the crisis period starting February 2020; IT risks; accounting judgment, management review, cash payment controls),Increased monitoring of alternative control activities, Establishment of a process for prompt elimination of weak points arising with increasing frequency and identification of any damage incurred, Adaptation of the Internal Controls (ad hoc) reporting for key stakeholders, and Increased dialog with external stakeholders and the external auditor (Alshamsi et al., 2019; Nur-Al-Ahad et al., 2022).

Methodology

The study presented in this paper is an exploratory one, based on secondary sources of information. The secondary sources include published books, journals, periodicals, reports, and newspaper. Secondary research is a common approach to a systematic investigation in which the researcher depends solely on existing data during the research process. This research design involves organizing, collating, and analysing these data samples for valid research conclusions. Secondary research is also known as desk research since it involves synthesizing existing data that can be sourced from the internet, peer-reviewed journals, textbooks, government archives, and libraries. What the secondary researcher does is to study already established patterns in previous research and apply this information to the specific research context. This methodology often relies on data provided by primary research, and therefore some research combines both methods of investigation. In this sense, the researcher begins by evaluating and identifying gaps in existing knowledge before adopting primary research to gather new information that will serve his or her research. As already highlighted, secondary research involves data assimilation from different sources, that is, using available research materials instead of creating a new pool of data using primary research methods. Common secondary research methods include data collection through the internet, libraries, archives, schools and organizational reports.

Online Data - Online data is data that is gathered via the internet. In recent times, this method has become popular because the internet provides a large pool of both free and paid research resources that can be easily accessed with the click of a button. While this method simplifies the data gathering process, the researcher must take care to depend solely on authentic sites when collecting information. In some way, the internet is a virtual aggregation for all other sources of secondary research data. Data from Government and Non-government Archives - You can also gather useful research materials from government and non-government archives and these archives usually contain verifiable information that provides useful insights on varying research contexts. In many cases, you would need to pay a sum to gain access to these

data. The challenge, however, is that such data is not always readily available due to several factors. For instance, some of these materials are described as classified information as such, it would be difficult for researchers to have access to them.

Data from Libraries - Research materials can also be accessed through public and private libraries. Think of a library as an information storehouse that contains an aggregation of important information that can serve as valid data in different research contexts. Typically, researchers donate several copies of dissertations to public and private libraries: especially in cases of academic research. Also, business directories, newsletters, annual reports, and other similar documents that can serve as research data, are gathered, and stored in libraries, in both soft and hard copies. Data from Institutions of Learning - Educational facilities like schools, faculties, and colleges are also a great source of secondary data, especially in academic research. This is because a lot of research is carried out in educational institutions more than in other sectors. It is relatively easier to obtain research data from educational institutions because these institutions are committed to solving problems and expanding the body of knowledge.

One can easily request research materials from educational facilities for the purpose of a literature review. Secondary research methods can also be categorized into qualitative and quantitative data collection methods. Quantitative data gathering methods include online questionnaires and surveys, reports about trends plus statistics about different areas of a business or industry. Qualitative research methods include relying on previous interviews and data gathered through focus groups which helps an organization to understand the needs of its customers and plan to fulfill these needs. It also helps businesses to measure the level of employee satisfaction with organizational policies.

Mora (2022) Advantages of Secondary Research Secondary data can be faster and cheaper to obtain, depending on the sources you use. It helps to Answer certain research questions and test some hypotheses, formulate an appropriate research design (e.g., identify key variables). Interpret data from primary research as it can provide some insights into general trends in an industry or product category and understand the competitive landscape.

Limitations of Secondary Research -The usefulness of secondary research tends to be limited often for two main reasons; Lack of relevance Secondary research rarely provides all the answers you need. The objectives and methodology used to collect the secondary data may not be appropriate for the problem at hand. Lack of Accuracy Secondary data may be incomplete and lack accuracy depending on the research design exploratory, descriptive, causal, primary vs. repackaged secondary data, the analytical plan, etc., Sampling design and sources target audiences, recruitment methods, Data collection method qualitative and quantitative techniques Analysis point of view focus and omissions, Reporting stages preliminary, final, peer-reviewed, Rate of change in the studied topic slowly vs. rapidly evolving phenomenon, e.g., adoption of specific technologies and Lack of agreement between data sources.

Analysis of Findings

From the literature reviewed, we note that business continuity planning is key for organisations to consider going forward and identification of critical Operational processes must be documented and tested. This we suggest should be an agenda item of every board meeting going forward.

Our inference for this review is that Hybrid work is heavily reliant on the availability of a strong and reliable Information Technology infrastructure of the organization that intend to deploy

this work model. But with it comes extra cost to organisations that include the Hardware and software and Security that go with a well-defined network that allows cloud or remote connectivity. Cyber Security is very paramount in the securing and advancement of implementing of the model as any attack on the companies' systems may result in huge losses that may go beyond the impact COVID19.Employee awareness training in Cyber risks is one area the needs to be adopted by organisations when transitioning to Hybrid work has, they need to understand their role in the prevention, detection, and monitoring. Most employees will have access to unsecure Wi-Fi networks either personal or in cafés to connect to company this will strain the organisation IT Infrastructure.

The Pandemic has unquestionably redefined the nature and scale of fraud risk with new scheme been carried out that is targeted at the vulnerabilities COVID presented. As study indicates fraud increased in business email compromise, hacking, ransomware, and malware and social engineering such as phishing, brandjacking, and baiting. As we move to Hybrid work literature suggests that a large increase in identity crime including identity theft, synthetic identity schemes, and account takeovers, unemployment fraud, and payment fraud, credit card fraud and fraudulent mobile payments as the case of Uganda.

Remote work is also noted to challenge visibility and oversight on staff members and consultants who may misrepresents work hours. Further, if not managed well the staff attrition faced during COVID period weakened the control environment which may require organisations to relook at the current controls, process, and procedures to align them to the new prevailing condition that will support remote connectivity by employees. Third party contracts will need to be monitored as there is a likehood of these been used to defraud organisation with identity theft projected to be on the increase.

Organisations need to reorganise operations and adopt agile and robust processes for their procurement, supply chain, people management and security strengths and weaknesses as noted in literature, monitor turnaround times for supply chain issues as this was highly affected during the pandemic. With the shift to hybrid work this is one area that need to be strengthened to avoid fraudulent transactions by both employees and third-party providers.

At the helm of this change from work from the office to hybrid is the governance that has oversight over financial risks and creating a favorable control environment. Boards (BoD) should evaluate the benefits and risks that come with the change to the hybrid work model. Investments must be put in the change management process that should complete risk assessments that speak to the new future of work and adopt what fits in the organization as the change over is not a one shoe fits all. Though not emphasized as part of this study, employee welfare, mental health and safety must be looked at and safe guarded as the implementation of the work model is completed.

Conclusion

We give our conclusions in this section based on the steps mentioned above it's evident that Hybrid Work is not going anywhere soon, and organisations must embrace this model of working as the new future of work as analysed by different scholars and researcher pre and post COVID 19 pandemics. In doing so there must be specific and deliberate focus on leadership, culture, and purpose. Further, organisation structures and roles must be defined

including ways of working to avoid disruption to work because of adoption of a hybrid work model. Furthermore, our findings demonstrate that their room to do more studies on this subject's matter for any developments in the post COVID-19 to have a lasting effect on risk management.

References

Al Qalhati, N., Karim, A. M., Al Mughairi, B., Al Hilali, K., & Hossain, M. I. (2020). Technology and HR Practices in Educational Sector in Sharqiya Governate of Oman. *International Journal of Academic Research in Business and Social Sciences*. 10(10), 435-443.

Alshams, Y. A. A. B, Hock, O. Y., Karim, A. M, Hossain, M. I. (2019). Developing a Framework on Performance and Challenges of Strategic Management Information System: A Case study on Ministry of Interior, UAE. *International Journal of Academic Research in Business and Social Sciences*, 9(5), 633 – 646.

Alshamsi, H. S. A. A., Karim, A. M., Hossain, M. I. (2019) Effectiveness of Public Sector Financial Audit on Police Department of Abu Dhabi, UAE: Proposition of a Conceptual Framework. *International Journal of Academic Research in Business and Social Sciences*, 9(5), 647–659.

Brooks, I. (2009). *Organisational behaviour: individuals, groups and organisation*. Pearson Education.

CDC. (2022). CDC streamlines COVID-19 guidance to help the public better protect themselves and understand their risk https://www.cdc.gov/media/releases/2022/p0811-covid-guidance.html Accessed on 24 August, 2022

CISCO. (2022). COVID-19: Remote Access to Operational Technology Environments Covid-19: longer-term impact on internal audit – focus on canada Cybersecurity. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~types-of-threats Accessed on 24 August, 2022

Deloitte. (2020). https://www2.deloitte.com/content/dam/Deloitte/au/Documents/audit/deloitte-au-audit-covid-19-control-environment-considerations-report.pdf Accessed on 25/08/22

Deloitte. (2020). https://www2.deloitte.com/content/dam/Deloitte/de/Documents/about-deloitte/COVID-19-Effects-on-the-internal-control-system-fact-sheet.pdf Accessed on 25/08/22

Deloitte. (2020). https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/The_Fraud_Triangle_Final.pdfAccessed on 24 August, 2022

Eklund, M. A. (2021). The COVID-19 lessons learned for business and governance. *SN Business & Economics*, *1*(1), 25.

Fortune. (2022). https://fortune.com/2020/04/02/zoom-bombing-what-is-meeting-hacked-how-to-prevent-vulnerability-is-zoom-safe-video-chats/ 04/09/2022

Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

Hossain, M. I., Polas, M. R. H., Rahman, M. M., Islam, T., & Jamadar, Y. (2020). An Exploration of COVID-19 Pandemic and its Consequences on FMCG Industry in Bangladesh. *Journal of Management Info*, 7(3), 145-155. https://doi.org/10.31580/jmi.v7i3.1484

Hossain, M. I., San, O. T., Ling, S. M., Said, R. M. & Teh. B. H. (2022). Nexus of Stakeholder Integration, Environmental Investment, Green Technology Adoption and Environmental

Sustainability Practices: Evidence from Bangladesh Textile SMEs. *Journal of Social Sciences and Humanities*. 30 (1), 253 – 281.

IMF. (2022). https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm 04/09/2022

Jamadar, Y., Ong, T. S., Kamarudin, F., & Abdullah, A. A. (2022). Future firm performance, corporate governance, information asymmetry and insider trading–a systematic literature review using PRISMA. *International Journal of Sustainable Economy*, 14(3), 309-329.

Jamadar, Y., San, O. T., Abdullah, A. A.. and Kamarudin, F. (2021). Earnings and discretionary accruals. *Managerial and Decision Economics*. Doi: https://doi.org/10.1002/mde.3391

KPMG. (2022). https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/maintaining-controls-in-a-covid-19-environment.pdf Accessed on 25/08/22

Mughairi, B. M. A., Hajri, H. A., Karim, A. M., Hossain, M. I. (2019). An Innovative Cyber Security based Approach for National Infrastructure Resiliency for Sultanate of Oman. International Journal of Academic Research in Business and Social Sciences, 9(3) 1180–1195.

Nur-Al-Ahad, M., Jamadar, Y., Latiff, A. R. A., Tabash, M. I., & Zaman, A. (2022). Effect of Islamic and Conventional Bonds on Firm's Performance: Evidence from Malaysia. In *2022 International Conference on Sustainable Islamic Business and Finance (SIBF)* (pp. 108-116). IEEE.

Theiia. (2022). COVID-19: Control environment considerations. https://www.theiia.org/globalassets/site/affiliates/canada/documents/covid-19-longer-term-impact-on-ia.pdf Accessed on 25/08/22