INTEGRATED ENTERPRISE RISK MANAGEMENT (IERM) FOR PENSION FUND ORGANISATIONS: FROM A TECHNOLOGY POINT OF VIEW

ABDUL RAHMAN AHMAD DAHLAN[1] ,NOOR NABIL MUHIDIN[2]

[12] *Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia.*

**Corresponding author: nabilmuhidin@gmail.com*

ABSTRACT: Any appraisal at this point must keep in mind that the epidemic is far from over and that the pandemic was economic and financial consequences has been considerably reduced due to the strong governmental efforts. Such event occurred in this digital era has shaped many financial institutions, including the pension funds, to take bold policy actions to overcome this issue in the future, as their role in protecting and managing people`s retirement savings is crucial and critical (Feher and Bidegain, 2020). A pension fund is also an institutional investor who invests substantial sums of money in public and private enterprises. The principal purpose of a pension fund is to ensure that there will be enough money to cover employees' pensions once they retire in the future. Proper Integrated Enterprise Risk Management (IERM) is needed to cater for ISO 31000: 2018 Risk Management Standard – Principles and Guidelines and ISO 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. This paper attempts to highlight the key IT-related risk factors and IERM in the context of a pension fund in this digitalization and post Covid-19 era; among others is the enhancement of performance of the investment system, digital readiness, technology-related processes, and system integrity.

KEY WORDS: *Integrated Enterprise Risk Management (IERM), pension funds, risk factors, post-COVID-19, digital era.*

1. INTRODUCTION

The current COVID-19 epidemic has already proved to be one of the worst crises in recent history, wreaking havoc on several sectors of the global economy. The financial industry is one of the most hit by the economic downturn brought on by the COVID-19 epidemic. Coupled with the new dangers posed by digital change, banking models and reputations are being put to the test (Feher and Bidegain, 2020). Banks, including the pension funds, are under an additional pressure to strengthen their technical skills as a result of the COVID-19 situation, which comes at a time when they are also more exposed to cyber assaults and consumer credit issues. These concerns and their consequences for the future are discussed by world financial leaders. The pension funds must look into the new risk factors and their mitigation post-COVID-19 to ensure that if history repeats itself, such a scenario can be properly measured and mitigated accordingly.

2. PROBLEM STATEMENT

Technology dependence might also introduce new dangers (OECD, 2017). Less educated and well-paid workers may be excluded from the technology advancement because they are unable or unwilling to interact with the new communication techniques. Non-regulated corporations from other industries may cherry-pick some components of pension provision, leaving conventional players with less profitable operations and exposing them to regulatory risk. Concerns about data privacy and security, and consumer protection problems pertaining to the acceptability of the services and goods supplied are also present.

The FinTech's effect is particularly seen in the financial advisory industry. Insurance businesses are also adopting the technology, despite the fact that its principal application is now in wealth management. In general, Robo-advice is less expensive and more accessible than "human" guidance. FinTech businesses can enhance the provision of financial advice to previously underserved communities according to the UK Government's Chief Scientific Adviser, owing to their "reduced cost structures, broader client reach, or superior capacity to monitor or evaluate risk."

3. METHODOLOGY

This article will evaluate several literature reviews which discuss matters related to risks of technological advances and enhancement that the pension funds may encounter. This is done by looking at the usage, implementation, and utilization of integrated risk management of ISO 31000:2018 Risk Management Standard – Principles and Guidelines and ISO27000:2018 Series Standards on information security management.

Additionally, a qualitative research which is based on interviews has also been conducted with three employees which are selected from the private and public pension funds to discuss in depth their thought on the technological risk associated with a pension fund. This is to capture the rationale of how an organization creates, delivers, and captures value via the Business Model Canvas (BMC) framework.

The BMC covers the four main areas of any venture: customers, offering, infrastructure, and financial viability. There are nine building blocks that describe and assess a business model: customer segments, value propositions, channels, customer relationships, revenue streams, key resources, key activities, key partnerships, and cost structure (Brillinger, Anne-Sophie, Christian, Bjorn Beate, 2020).

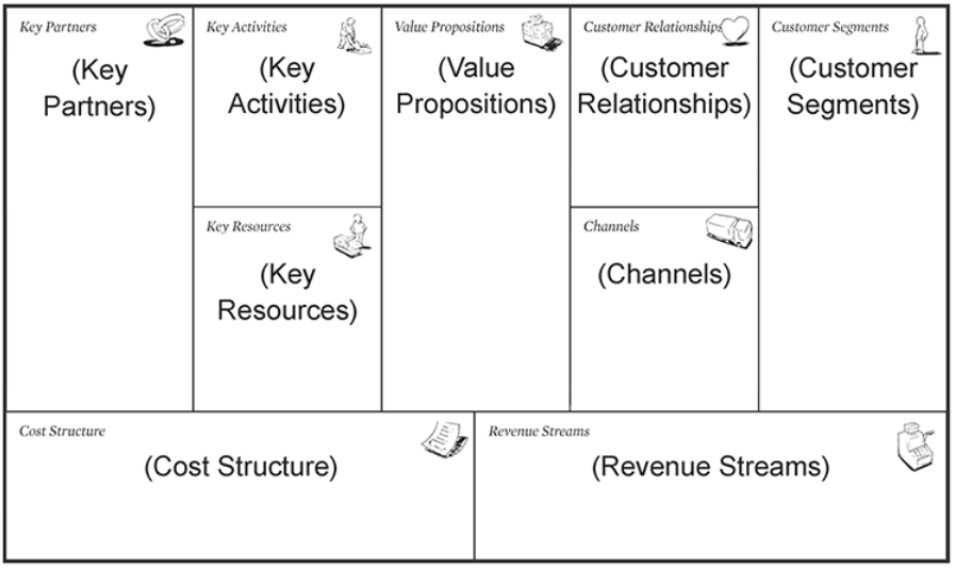

Fig. 1. Business Model Canvas nine elements

4. LITERATURE REVIEWS

The OECD Basic Principles of the Corporate Pension System (OECD 2004) (2.4) states: The approval guidelines address risk management issues and explain: "Risk management procedures contribute to sound corporate practices and help establish appropriate risk measurement and management systems. These procedures include conflicts of interest and operational risks, including those related to technical failures. It contains a mechanism to identify and resolve. In implementing the technological enhancement in a pension fund, the writer suggests that OECD Basic Principles requires pension fund to establish proper risk management including any technology and IT system in the fund. Another approach that is also used by organizations is ISO 31000. It is a standard that provides guidelines, principles, frameworks, and procedures for managing risk in an organization, regardless of the type and size of the organization. The ISO 27000 series is a special standard for information technology. The advantage of this ISO 27000 series is that it provides security that protects your data from theft and illegal use that can lead to threats. Moreover, this standard is not limited to specific areas such as finance and banking, but also to pension funds."

General risk management requirements of different financial sectors are similar. Therefore, it is not surprising that more detailed instructions from various international organizations and national supervisors on how these key requirements are met are equivalent. The risk management system can be divided into five major categories: Strategy Risk, Reputation Risk, Financial Risk, Operation Risk, and Technology Risk; and the guidance on implementing on each side is included in the recommendations above. (Baker McKenzie, 2020)

All types of financial services today are highly technology-dependent and require internal control to check the security of IT systems (PWC, 2020). IT security risks can be defined as security risks associated with potential threats to the confidentiality, integrity, availability, and accountability of IT of an institution. These IT security risks include data concentration, which can compromise the security of

information, and the use of complex applications, which can cause recurring problems. The risk of errors, fraud, negligence and accidental accidents (such as system crashes) must all be protected. Data integrity is just as important as risk mitigation factors such as false service payments.

Information system and technology management should include both general management and application management for pension funds. Common controls are for the computer systems (mainframes, clients/servers, end-user workstations cloud computing, AI, internet of things, mobile phones, etc.) to ensure that they continue to work properly. Common controls include internal backup and recovery procedures, software development and procurement guidelines, maintenance procedures (modification control), and physical/logical access security controls. Application control is a computerized step within a software application, and other manual steps that control the processing of the transaction and business activities such as edit checks and specific logical access controls specific to the business system. This is quite similar to any financial institution.

Existing pension providers can be at a disadvantage when using the new technology compared to new players because they are constrained by their existing IT infrastructure, which is expensive to change or replace (UNCTAD 2021). This will allow new entrants to enter several areas of retirement offerings at a lower cost, as already shown in the consultations (UNCTAD 2021). As an example of the potential cost of upgrading legacy systems, UBS, an investment banking company has started very much early to have invested $ 1.444 trillion in the reengineering process for its entire wealth management business to bring the Robo advice to the UK (Williams-Grut, O. 2016).

In the area of interaction with members, there are a number of potential risks. The pension funds could aggravate financial exclusion for those who do not engage with digital communications; conversely, there is some concern that consumers will place too much trust in technological solutions and so the fall-out from any problems with the pension fund will be particularly damaging (OECD, 2017). One example of this is crowdfunding, where small investors might take more risks than traditional investment products.

Privacy and security risks are heightened by the introduction of technologies that rely on the collection, storage, and analysis of large amounts of data to provide enhanced services (Brous, Janssen, Herder. 2020). If the pension funds were to use cloud-based IT services, it can keep the data out of the reach of regulators. Advances in technology may increase consulting and outsourcing to professional providers such as advanced analytics companies. These companies may not be within the scope of the pension regulators, but the failure of these companies can have a negative result in confidence in private pension funds (Department for Works and Pensions, 2021).

The regulators also need to ensure that the benefits of technology are actually passed on to retirees and beneficiaries. Philippon argues that the financial services industry has maintained improved IT efficiency and that the role of regulators is to ensure the outbreak of turmoil (Philippon, 2017). The regulatory framework needs to accommodate such disruption and ensure that the same rules are applicable for both public and private pension funds.

For the pension funds, whether private or public, it is paramount to recognize or understand the key success factors of an organization in relation to the customer segment they serve: 1) understand the key-value propositions for each customer segment; and 2) understand the key resources, activities and partners needed to deliver the value proposition and benefits to the various customer segments, sources of income and cost structure. This can be done by using the Business Model Canvas (BMC) as one of the best tools available. The BMC helps organizations to visualize and shape their key factors using the nine blocks and innovate their business models. The BMC also helps to identify different mechanisms in an organization (Y Ching H. & Fauvel, C., 2013). In addition, its capabilities help you to understand and identify the key organization assets and find solutions to mitigate all types of risks, now and in the future.

In addition, the pension funds were also affected by the Fourth Industrial Revolution (IR 4.0) (Radojko, L. 2019). IR 4.0 is a technological advancement that was adopted in the Tertiary Industrial Revolution. New technological advances come in the form of artificial intelligence, robotics, the Internet of Things, and many more. The financial institutions include the pension sector that does not wonder about the use of technology and can be vulnerable to the same threats as other sectors (PWC 2020).

5. ANALYSIS AND DISCUSSION

This paper intends to discuss matters related to IERM in technology for the pension funds during this digitalization era. Based on the literature reviews and interviews conducted, there are several important findings derived from this study.

All interviewees unanimously agreed that the risk factors must be based on the business plan of the institution. The common elements of the risk factors of the pension fund would be the availability and viability of an investment system. Especially during the COVID 19 lockdown, most of the processes related to an investment, including the system, are conducted remotely at home. This is an important element that any pension fund should consider in its risk control.

Crucial controls such as providing training to technical staff on the latest technology and maintaining the electronic document management system are necessary so that the confidentiality, integrity and availability (CIA) triad can be fulfilled by the staff and members at home.

As systems tend to experience glitches or fleeting errors or worst-case scenarios that cause serious harm to the system such as power failure and temporary loss of service or data loss, a self-assessment or a constant review by the strategic and architect system team must be done. Another part that the pension funds should look into is putting in place the business continuity and disaster recovery plans, which may now put this preparation to the test. For all the schemes, it will be the time to think about their processes and obligations and take practical and reasonable steps to reduce the risk of disruption to payments and other services to members and to ensure that the schemes continue to run to the best of their ability (Lavell, 2004). From a security point of view, scenarios such as malware attacks and cyber terrorism can potentially occur if a proper security firewall is not installed and exercised. Such risk control seems to be satisfactory as it will act as a detective measure rather than a preventive or corrective. If such a problem can

be detected earlier, a proper arrangement regarding the system enhancement can be done effectively. This is in line with ISO 27001:2018, where the specific standard provides requirements for an information security management system. It covers much range of matters such as financial information, intellectual property, employee details, or information entrusted by third parties.

Apart from focusing on the process and the system, one should also consider human resources as a risk control in relation to the performance of the investment system. As some system is not fully automated yet, human intervention may allow a certain level of error. If such error is fundamental or significant, it is important that the pension funds review the staff's competencies in keeping up with the relevant technology developments and if necessary send the staff for training. The pension funds should also organize programs to increase awareness of risk management. As highlighted by Bank Negara Malaysia in the Risk Management in Technology (RMiT), another element that is important is the designation of Chief Information Security Officer or similar, who is responsible for the technology risk management function of a financial institution in Malaysia. Based on the interview conducted, one pension fund in particular, placed the function of technology risk under the purview of the Risk Management Department. To a certain extent, the function is independent of other functions and reports directly to the Chief Executive Officer. Any risk assessment, beginning from Identification, Analysis & Evaluation, Treatment, to Monitoring & Report, is conducted without interference from any department or personnel (Risk Management in Technology, Central Bank of Malaysia, 2020).

Another important risk control that any pension fund should consider is for the staff's understanding on the importance of a risk culture. This can only be achieved if the staff understood the vision and mission of the pension fund, which is to serve customers for better retirement days. Having such control not only manages the staff's behaviors (integrity and honesty) in performing a certain task, but it will impact the overall attitude and their attitude towards IT and technology security matters. To overcome this, many factors should be considered, such as having a proper recording of departmental policies and procedures, reviewing and updating the department`s risk profile, allocating risk scorecard to owners, and monitoring it efficiently. Based on the interview, the concept of shared accountability and ownership is important to an effective implementation. However in order to be accountable, employees must be equipped with the required methods, tools and skills. Sufficient training is imperative to an effective risk management. The study also highlighted the importance of a risk champion. This is where dedicated individual's visibility identifies risks and acts as mentors to others. To make this happens, specific resources such as time, resources and training must be provided. This demonstrates commitment and support (Cormican, 2014).

Moreover, the Business Model Canvas (BMC) can be illustrated as a guide, as it is a visual chart consisting of nine blocks which are Key Partners, Key Activities, Key Resources, Value Proposition, Customer Relations, Channels, Customer Segment, Cost Structure, and Revenue Stream. The intention of BMC is for the pension funds to understand and identify what type of risks they are facing. Effectively, this will help the pension funds to develop proper and integrated risk management strategies.

Table 1: Proposed Integrated Enterprise Risk Management (IERM) using the Business Model Canvas Framework for Pension Funds.

<table>
<tr><th>Key Partners</th><th>Key Activities</th><th>Value Proposition</th><th>Customer Relation</th><th>Customer Segments</th></tr>
<tr><td rowspan="4">• For pension funds to deliver excellent services to its members.
• Consultant/ vendor to provide reliant advice and assistance to pension funds in matters related to IT and technology.</td><td>•Technology related processes are well preserved and practiced.
• Manual operations and guidelines are put in place for IT-related matters.
• IT and technology risk is being properly supervised and updated.</td><td rowspan="3">•Mission and vision of the pension fund are embedded with IT/digital capabilities.
•Human capital development is properly monitored in relation to security matters.</td><td>•Maintain and improve members and pension fund relationships through the advancement of technology.
•Visibility of the pension funds` initiative and improvement via new technology development</td><td rowspan="3">• Members are aware of the new enhancement of the pension fund`s digital services.
•Enhance customer digital experience.</td></tr>
<tr><td>Key Resources</td><td>Channels</td></tr>
<tr><td>•Pension funds have sufficient resources to support the digital move.
•Staffs are capable of at least sufficient digital knowledge.</td><td>• Sufficient digital platforms such as social media for marketing.
• Corporate affairs department to play its role for advertisement.</td></tr>
<tr><td colspan="3">Cost Structure</td><td colspan="2">Revenue Stream</td></tr>
<tr><td colspan="3">• Key Activities and Key Resources.</td><td colspan="2">•Appropriate allocation of funding by the Board of the pension funds.
•Steady revenue from the investment made by the funds.
•Continuous contribution by members.</td></tr>
</table>

Value Proposition (VP): In order for a pension fund to achieve its VP of having digital and technology as part of the vision and mission, the management should consider having a proper and sufficient IT or technology-related training for its staff. Minimum standard of accessibility of the internet should be made to its members, as the members require stable internet connectivity and a minimum standard of access to the sites in order to have a better IT and technology experience.

Customer Segments (CS): The group of people that matters here are the members of the pension fund. The customer service department should play a role in collecting ideas related to IT and technology to improve the pension fund capabilities to serve the members better. Together with the technology department, they should come out with a program that can remove the need for members going to counters. Security IT should also play a role in ensuring that the members' right and privacy is well protected whilst using the program.

Channels (CH): As highlighted in the literature review, technology is an important component for the financial institution including the pension funds. Any new initiative made by the pension fund should be advertised via social media such as Facebook, Instagram and Twitter. Research has shown that the effect of social media advertising has a great impact, as most members have access to social media (Sreejesh, Paul, Strong, Pius, 2020).

Customers Relations (CR): Apart from the social media, the pension funds should establish better relationships to understand their members better. The introduction of certain phone applications for the members can allow them to communicate better with the pension funds rather than relying on the traditional hotline phone calls. Feedback can be given in real-time and by leveraging on the better technology enhancement and security protocols, user experience is heightened.

Revenue Stream (RS): Similar to any financial institution, the budget spending is allocated at the end of each year for the utilization in the next year. The main source of the pension fund is from the members' contributions and the revenue from investments. Before any allocation can be given, justification for the utilization is important as the approval must be stand guided with proper justifications. Related departments must put forward concrete business cases especially for the implementation or enhancement of technological-related processes and procedures.

Key Partners (KP): The main key partners are the Ministry of Finance (MOF), the employers and the members. It is the relationship that the pension fund has with other businesses, authorities and others that help the business model works. MOF should be the main supporter of any technological enhancement. Government should provide any tax exemption or a research grant in matters related to technology.

Key Activities (KA): The fundamental mitigation for key activities is to have the proper manual operations and guidelines to be put in place for IT-related matters. In line with ISO 9001:2015, the standard highlights to provide an effective framework for any organization that would like to consistently provide products and services that meet their customers' requirements; and to continually improve on their products, processes, and system to enhance satisfaction.

Key Resources (KR): Human capital, and the availability and viability of digital infrastructure are the main factors for KR. In any enhancement, including technology, human capital plays an important role as it would benefit the rate of participation and reduce the time necessary for the introduction of a new technology. Sufficient up-to-date technology facilities with proper protection by firewall/ antivirus are paramount too.

Cost Structure (CS): The high cost incurred is usually in terms of infrastructure, including the overall security protection from hardware and software. Another aspect that one should ponder is the cost associated with maintaining it. To mitigate this risk, the annual budget should take into account such costs.

It is important that the BMC would coordinate across the sub-disciplines of technology risk management. The relationship between cybersecurity and disaster recovery, vendor and third-party management, and project and change management to mention a few, even though interdependent in many ways, often are not formally connected. It is important to the risk associated across the sub-disciplines of technology risk management to avoid inadvertent gaps in risk management or redundant overprotection (Bevan, Ganguly, Kaminski & Rezek, 2016). Table 2 below shows the effective technology risk management that covers certain sub-disciplines as an example.

Table 2: Effective IT-risk management covers relevant sub-disciplines.

No.	Technology risk sub-disciplines	Key risks for pension fund
1.	Information and cybersecurity	Fraudulent transactions, blackmail and leakage of confidential pension fund members and internal data.
2.	Resilience and disaster recovery	Interruptions of IT investment services led to economical loss toward the investment portfolio of the pension fund.
3.	Project and change management	Changes that led to incomplete projects within the timeline and not at a desirable quality.
4.	Data quality and compliance	Missing data will lead to legal issues or transaction-settlement issues.

Some of the banks separate their enterprise risk management from the technology risk management. This will hinder the capabilities of banks to prioritize the risks associated with technology. The lack of a common risk-management technology platform used by both enterprise risk and technology risk teams is one of the contributing factors of why those elements are not integrated. When enterprise risk management technology risk groups are combined, advantages may arise. Fast making decisions is possible to the degree necessary to meet the requirements of the business as it integrates enterprise and technology risk management. Resilience and disaster recovery as well as vendor and third-party management are two areas where enterprise and technology risk management integration can be particularly beneficial. Technology risk managers should define a risk appetite that represents the business effect of interruptions in order to prevent the interruption of essential services. Most banks will discover that a near-perfect technology resilience is necessary for a modest portion of their business processes (Bevan, Ganguly, Kaminski & Rezek, 2016).

Based on the interview conducted, one respondent explained that a particular pension fund has its risk assessment in the midst of being consolidated in one system, namely the IERM. The current system only acts as a depository where the risk assessment is being done outside of the system. The liaison officer from each department will be updating the risk rating together with justification before it is reviewed and accepted by the risk department.

6. SUMMARY AND CONCLUSION

The way the pensions are set up, managed, and delivered to consumers is changing with the use and the application of technology. Such application of technology increases access to a wider range of member-based retirement investments and makes communication with retirement savers more effective. In addition, the pension funds increase the operational efficiency of the system through risk management applications, and automate the investment process, and facilitate compliance with regulatory requirements.

The private or public pension funds must adopt relevant security posture assessments to further strengthen the technology of an institution and the digital risk measures by identifying what their security status is, what do they need further and what they need to do to improve or maintain their current security status or maturity level. The security posture assessment helps the pension funds define the security status as it guides security strategies, determines security projects, and impacts security spending based on ISO 31000:2018. It is also essential for building a long-term security strategy that protects the institution. Information security is implemented by systems, policies and procedures in compliance with ISO/IEC 27001:2018 Information Security Management System (ISMS). Therefore, the security posture assessment provides a thorough understanding of information security, follows by technical knowledge and skillsets.

The key themes that emerged are centered on awareness, policies, processes, management, culture and benefits. The findings show that there is a need for an integrated approach to enterprise risk management. It seems that IERM practices are not widely employed in industry and many organizations do not consider the consequence of risks. However many interviewees responded that their pension organization does not have a formal structured process in place to enable this.

In conclusion, every pension fund should have its Integrated Enterprise Risk Management (IERM) in line with its business plan. This paper demonstrated IERM using the Business Model Canvas framework to ensure that the key risk factors are identified and the controls are in place. COVID-19 has shown that we need to anticipate the worst-case scenario in every event. Especially in this digital era, technological-related risks such as information security incidents, cyber-attacks, password theft, service outages, power failures, and many more should be considered even more seriously.

REFERENCES

Brillinger, AS., Els, C. & Schäfer, B. & Bender, B. (2020). "Business model risk and uncertainty factors: Toward building and maintaining profitable and sustainable business models," Business Horizons, Elsevier, vol. 63(1), pages 121-130.

Brunner, G., Hinz, R., Rocha, R., (2008), ‘Risk-based Supervision of Pension Funds: Emerging Practices and Challenges.

Cormican, K. (2014). Integrated Enterprise Risk Management: From Process to Best Practice. Modern Economy, 5, 401-413. http://dx.doi.org/10.4236/me.2014.54039

Department for Work and Pension. (2021, July 21) Taking action on climate risk: improving governance and reporting by occupational pension schemes. Retrieved from https://www.gov.uk/government/consultations/taking-action-on-climate-risk-improving-governance-and-reporting-by-occupational-pension-schemes-response-and-consultation-on-regulations/taking-action-on-climate-risk-improving-governance-and-reporting-by-occupational-pension-schemes.

Doxey, C. (2021). Information Technology Risk. 10.1002/9781119700586.s7.

Eerden, L. (2013). Risk Governance in Pension Funds: Management Control in Dutch Pension Funds. 10.1057/9781137332158_10.

Feher, C. & de Bidegain, I. International Monetary Fund, Pension Schemes in the COVID-19 Crisis: Impacts and Policy Considerations (2020)

Financial Services Technology 2020 and Beyond: Embracing disruption, PWC. 2020.

Godwin, A. (2016). Brave new world: digital disclosure of financial products and services. Capital Markets Law Journal, 11(3).

Kemp, M. & Patel, C.. (2012). Entity-wide risk management for pension funds. British Actuarial Journal. 17. 10.1017/S1357321712000086.

Lavell, J. (2004). Business continuity plans: An overview. Journal of Investment Compliance. 5. 62-64. 10.1108/15285810410636172.

Lizarzaburu, E. & Salquero, J. (2011). ISO standards a potential path for emerging markets: An initial literature review. Risk Governance and Control: Financial Markets and Institutions. 1. 65-71. 10.22495/rgcv1i4art5.

Lukić, R. (2019). Pension Insurance At The Beginning Of The Fourth Industrial Revolution.

OECD (2017), Technology and Pensions: The potential for FinTech to transform the way pensions operate and how governments are supporting its development

OECD (2017), Technology and Pensions: The potential for FinTech to transform the way pensions operate and how governments are supporting its development.

Philippon, T. (2017). The FinTech Opportunity. BIS.

Risk Management in Technology, Central Bank of Malaysia (2020) Bank Negara Publication BNM/RH/PD 028-98.

Shendalev, A. & Shendaleva, O. (2020). Model of Technologic Risk Assessment. Vestnik NSU. Series: Information Technologies. 18. 76-87. 10.25205/1818-7900-2020-18-2-76-87.

Sreejesh, S., Paul, J., Strong, C., & Pius, J. (2020). Consumer response towards social media advertising: Effect of media interactivity, its conditions, and the underlying mechanism. International Journal of Information Management, 54, 102155.

Stewart, F. (2010), "Pension Funds' Risk-Management Framework: Regulation and Supervisory Oversight", OECD Working Papers on Insurance and Private Pensions, No. 40, OECD publishing, © OECD. doi:10.1787/5kmlcz7qq3zx-en.

Technology and Innovation Report 2021, United Nations Conference On Trade And Development (UNCTAD).

Valdevit, T., Mayer, N., & Barafort, B. (2009). Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings. Communications in Computer and Information Science 42:201-212. DOI: 10.1007/978-3-642-04133-4_17

Williams-Grut, O. (2016, October 10). UBS Launches Robo-Advice Product Smart Wealth. Business Insider. https://www.businessinsider.com/ubs-launches-robo-advice-product-smartwealth-2016-10.

Y Ching, H., & Fauvel, C. (2013). CRITICISMS, VARIATIONS, AND EXPERIENCES WITH BUSINESS MODEL CANVAS. European Journal of Agriculture and Forestry Research, 1(2), 26-37.