Cyber Risk Management Frameworks for the South African Banking Industry

C Koto, RJ Smith and B Schutte
University of Johannesburg, South Africa

Abstract: Since the dawn of technology, the banking industry has relied on technology to support its operations. Unfortunately, the banking industry has been exposed to cyber risks as a result of the same technology, which has resulted in enormous financial losses. South Africa has the world's third-highest number of cyberattacks, with the banking industry being the most targeted. As a result, it is critical for the banking industry in South Africa to implement effective cyber risk management procedures. The South African Reserve Bank (SARB) requires that these procedures be aligned to the cyber resilience guidelines of the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). The CPMI–IOSCO cyber resilience guidance provides guidelines that should be addressed by a bank's cyber risk management framework. The aim of this research is to determine if the Improving Critical Infrastructure Cybersecurity (ICIC) framework addresses the CPMI–IOSCO cyber resilience guidelines. The results were gathered by examining the ICIC framework and mapping it against the CPMI–IOSCO cyber resilience guidelines. It was revealed that, the ICIC framework addresses up to 71% of the CPMI–IOSCO cyber resilience guidelines.

Keywords: Banking industry, Cyber risks, Cyber resilience guidance, Cyber risk management, ICIC framework

1. Introduction

Technology is developing rapidly, causing changes in the way business is conducted in various industries (Nuskiya, 2018; Nejad, Mansour & Karamipour, 2021). From the earliest stages of technological developments, the banking industry has been affected by technology (Mujinga, Eloff & Kroeze, 2018; Nuyens, 2019; Krasonikolakis, Tsarbopoulos & Eng, 2020). Most banking goods, services, and functions are now heavily reliant on technology (Krasonikolakis et al., 2020). It is no surprise that the industry continues to invest substantial amounts of money in technology (Mujinga et al., 2018; Evdokimova, Shinkareva & Egorova, 2019).

Given the multiple benefits banks receive and opportunities they are exposed to as a result of technology, banks' massive investments in technology are warranted (Coetzee, 2018; Evdokimova et al., 2019). Competitive advantage, fast service delivery, greater customer service, and higher profitability are just a few examples of those benefits (Ahmed, Vveinhardt, Streimikiene, Ashraf & Channar, 2017; Evdokimova et al., 2019). However, the banking industry is also faced with managing cyber risks as a result of the same technology, and yet this risk is sadly developing in lockstep with technical improvements (Mujinga et al., 2018; Evdokimova et al., 2019; Mapimele & Mangoale, 2019; Nuyens, 2019).

Cyber risk is among the main issues for the banking industry in South Africa, and this has resulted in enormous financial losses (Griffiths, 2017; Abdullah, 2019; Duvenhage, 2020). According to the South African Banking Risk Information Center, South African banks experienced 13 438 cybercrime events in 2017, resulting in losses exceeding R250 million (Kgosana, 2018; Smith, 2018). South Africa has had the third largest number of cybercrimes in the world for over a year, the banking industry being targeted more often than other industries (Griffiths, 2017; Lekha & Prakasam, 2017; Kundu, Islam, Jui, Rafi, Hossain & Chowdhury, 2018; Hubbard, 2019; Madiba, 2020). Consequently, it is obvious that South African banks must invest more in cyber risk management.

2. Literature Review

2.1 Cyber Risk Management

According to prior studies, banks should seek for effective cyber risk management procedures (Evdokimova et al., 2019). A framework developed

to manage all risks is insufficient and ineffective in managing cyber risks, because cyber risks are complex in nature (National Institute of Standards and Technology (NIST), 2018). As a result, it is critical for the banking industry to have a framework in place that particularly targets cyber risk management, assuring successful cyber risk management (Kopp, Kaffenberger & Wilson, 2017). In terms of section 6(5) of the Banks Act 94 of 1990, the South African Reserve Bank (SARB) published a guidance note through the office of the Registrar of Banks (SARB, 2017). This guidance note requires all South African banks to align their cyber risk management procedures with the cyber resilience guidance document issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) (Securities Industry & Financial Markets Association, 2016; Standard Bank, 2017). This guidance note is referred to as the CPMI–IOSCO cyber resilience guidance (SARB, 2017).

2.2 CPMI–IOSCO Cyber Resilience Guidance

On June 29, 2016, CPMI and IOSCO released the cyber resilience guidance (World Federation of Exchanges, 2018; Tsen, Ko, & Slapniar, 2020; KPMG, 2021). This guidance is used by the South African Registrar of Banks to determine the appropriateness of cyber risk management procedures in South African banks (SARB, 2017; European Central Bank, 2019). This guidance is the most recent best practice in cyber risk management, and it is intended to help banks create or improve their cyber risk management frameworks (SARB, 2017; Deloitte, 2018).

The CPMI–IOSCO guidance includes eight guidelines that should be addressed in any cyber risk management framework for banks, consisting of five fundamental risk management categories and three overarching categories (CPMI & IOSCO, 2016; European Central Bank, 2019; Tsen et al., 2020). Governance, identification, protection, detection, response, and recovery are the fundamental risk management categories, while testing, situational awareness, learning, and changing are the overarching categories (World Bank Group, 2017; Deloitte, 2019; Delort, 2019). These guidelines were developed to help the banking industry prevent cyberattacks, respond swiftly and effectively to them, and recover as rapidly as possible (European Central Bank, 2019).

Although this guidance may be useful in other industries, it is primarily intended for the banking industry (Deloitte, 2019; European Central Bank, 2019). According to the guidance, banks should have already, a cyber risk management framework, policies, cyber risk controls, and practices in place, as the guidance is not meant to substitute but to strengthen them (CPMI & IOSCO, 2016; European Central Bank, 2019). Most importantly, the principles outlined in this guide should not be used in violation of any applicable laws or regulations (SARB, 2017).

2.3 Cyber Risk Management Frameworks

BASEL is a framework that the South African banking industry is currently using (Oyetade, Obalade & Muzindutsi, 2020; Martins, 2021). BASEL is a regulatory framework aimed at bolstering the banking industry's capital foundation, as a poor capital base might lead to a financial crisis, which weakens the economy (Boora & Kavita, 2018). As a result, the BASEL framework's main goal is to foster a more secure and robust financial system, which will help to stabilise the banking industry and the economy (Rahman, 2018). The BASEL framework is broad in scope and significantly weighted in terms of liquidity risk (Kopp et al., 2017; Dina, 2019). Its principal goal is to allow banks to continue operating in the event of a financial crisis without relying heavily on government assistance (Shakdwipee & Mehta, 2017; Liu & Molise, 2018; Rahman, 2018). On the other hand, the ICIC framework is intended to assist critical infrastructure owners in identifying, assessing, and managing cyber risks (Almuhammadi & Alsaleh, 2017; NIST, 2018). Critical infrastructure pertains to assets and systems, both virtual and physical, that are so important to a country that their failure could have a detrimental impact on the country's health, safety, security and economy (Ciglic, McKay, Hering & Moore, 2017; Kure & Islam, 2019). One example of such infrastructure is the banking industry (Dantis, 2017; Zachozova, Kutsenko, Koval & Kovalenko, 2021). This framework is also applicable to industries that rely substantially on technology for their operations, such as banks (Bishnoi & Devi, 2017; NIST, 2018). As a result, it is widely used by a large number of banks all over the world (Barret, 2018; Deloitte, 2019).

In terms of managing cyber risks, the ICIC framework is commended for its effectiveness, efficiency, reliability, and cost effectiveness (Spitzner, 2017;

NIST, 2018; Barret, 2018). The ICIC framework was created primarily to manage cyber risks and does not impose any additional regulatory requirements (NIST, 2018). It is also worth noting that the ICIC framework allows for modification to fit an organisation's specific cyber risks, cyber risk tolerance, and cyber risk management goals, making it simple to adopt (Spitzner, 2017; NIST, 2018). The Financial Stability Institute believes the ICIC framework is a good place to start when it comes to properly addressing cyber risks (Crisanto & Prenio, 2017).

3. Methodological Approach

As derived from the literature review it is clear that banks need effective cyber risk management procedures. In South Africa, these procedures must be aligned to the CPMI–IOSCO cyber resilience guidance as required by SARB. Failure to do so will result in the office of the Registrar of Banks deeming those procedures inappropriate. According to the CPMI–IOSCO cyber resilience guidance, banks should have a cyber risk management framework that addresses the guidelines encompassed in the guidance. It is important that this framework is effective in managing cyber risks. Currently, South African banks are using the BASEL framework. The BASEL framework is broad in scope and significantly weighted in terms of liquidity risk, making it ineffective in managing cyber risk (Kopp et al., 2017; NIST, 2018). The ICIC framework on the other hand, is specifically intended for the management of cyber risks (NIST, 2018). Furthermore, it is commended for its effectiveness, efficiency, reliability and cost effectiveness in managing cyber risks (Spitzner, 2017; NIST, 2018; Barret, 2018). If the ICIC framework is effective in managing cyber risks, it is beneficial for South African banks to adopt it. However, it needs to address the CPMI–IOSCO guidelines. Therefore, this study seeks to answer the question: Does the ICIC framework address the CPMI–IOSCO cyber resilience guidelines? The objective of this study is to establish whether the ICIC framework addresses the CPMI–IOSCO cyber resilience guidelines, thereby determining whether the ICIC framework is aligned to the CPMI–IOSCO cyber resilience guidance. In order to achieve the aforementioned objective, mixed research methods were applied. Mixed methodology involves merging qualitative and quantitative data methods in order to achieve research objectives (Hlongwane, 2020). This study applies a qualitative method to collect data, that is, document analysis. Document analysis is a technique for collecting documents and analyzing them in order to obtain information from them (Dalglish, Khalid & McMahon, 2020). The researcher analyses the ICIC framework and the CPMI–IOSCO cyber resilience guidance document. The ICIC framework and the CPMI–IOSCO cyber resilience guidance document are obtained from internet sources.

The practices of the ICIC framework are then mapped against the CPMI–IOSCO cyber resilience guidelines. The mapping is conducted to determine the extent to which the ICIC framework addresses the CPMI–IOSCO cyber resilience guidelines. The results of the mapping are quantitative in nature as they represent the extent to which the ICIC framework addresses the CPMI–IOSCO cyber resilience guidelines as a percentage. The percentage is calculated as the number of the CPMI–IOSCO cyber resilience guidelines addressed by the ICIC framework in relation to the total number of CPMI–IOSCO cyber resilience guidelines. Therefore, the exploratory sequential design was adopted in this study. Exploratory sequential design is a design whereby qualitative exploration yields quantitative results (Hlongwane, 2020).

4. Mapping of the ICIC Framework Against the CPMI–IOSCO Cyber Resilience Guidelines

Five fundamental risk management categories and three overarching categories make up the CPMI–IOSCO cyber resilience guidelines (SARB, 2017). The CPMI–IOSCO cyber resilience guidelines under each category are presented in Column 1 of Tables 1 and 2. This data was taken from the CPMI–IOSCO cyber resilience guidance document. In the second column of the tables, the mapping takes place. The mapping was conducted by answering 'YES' or 'NO' in the second column next to each CPMI–IOSCO guideline. 'YES' means there is an ICIC framework practice that corresponds to the CPMI–IOSCO guideline. 'NO' means there is no ICIC framework practice that corresponds to the CPMI–IOSCO guideline. The ICIC framework practices were acquired through an analysis of the ICIC framework's most recent version 1.1, which refines, clarifies, and improves the previous version (NIST, 2018).

In Table 1 on the next page, the ICIC framework is mapped against the CPMI–IOSCO cyber resilience guidelines under the fundamental risk management categories.

Table 1: CPMI–IOSCO Guidelines – Fundamental Risk Management Categories Mapping

CPMI–IOSCO CYBER RESILIENCE GUIDELINES	ICIC FRAMEWORK PRACTICES
CATEGORY 1: GOVERNANCE	
1.1. The board of directors should establish a cyber risk management framework, approve it, and determine the bank's cyber risk tolerance.	YES The bank would not need to put up a new framework if they adopted the ICIC framework. According to the ICIC framework, the bank must identify the amount of cyber risk that is acceptable to them, and this level must be defined as their cyber risk tolerance.
1.2. The cyber risk management framework, as well as the controls, policies, and practices that underpin it, should be overseen by management.	YES According to the ICIC framework, management should approve and convey the performance of framework activities, as well as ensuring that they are carried out correctly.
1.3. The framework should lay out how the bank will define its cyber risk tolerance.	YES According to the ICIC framework, a bank's cyber risk tolerance should be based on its involvement in the country's essential infrastructure and industry risk assessment. This outlines the criteria for determining a bank's cyber risk tolerance.
1.4. The framework should spell out how the bank will set its cyber resilience goals.	NO The ICIC framework makes no mention of how cyber resilience goals will be set. It just explains ways to determine unmet cyber resilience goals.
1.5. The framework should specify how the bank will detect, mitigate, and manage cyber risks efficiently.	YES The core of the ICIC framework is made up of functions that are designed to detect, mitigate, and manage cyber risks.
1.6. To manage cyber risk, the framework should identify its people and processes.	YES The ICIC framework provides that an organisation should identify and comprehend cyber risk management systems, procedures, and people. The processes are specified in the framework core, and the people involved should include executive management, business/process, and implementation/operation level personnel.
1.7. To manage cyber risk, the framework should specify technology needs.	NO The technical needs to mitigate cyber risk are not mentioned in the ICIC framework. It also does not compel banks to do so.
1.8. The board's tasks and responsibilities in relation to cyber risk management should be clearly defined in the framework.	NO The ICIC framework does not specify the board's role and obligations in terms of cyber risk management.
1.9. Management's duties and responsibilities in relation to cyber risk management should be clearly defined in the framework.	YES The ICIC framework clearly defines management's roles and responsibilities. That is, to keep track of and monitor the framework's implementation.
CATEGORY 2: IDENTIFICATION	
2.1. Determine the functions, procedures, information assets, and system configurations of the bank.	YES As provided by ICIC, an organisation must define and comprehend its business context, important functions, systems, information, and physical assets.
2.2. Conduct a risk assessment on the items identified in 2.1	YES An organisation must perform a risk assessment on the company, its important functions, systems, information, and physical assets as part of the ICIC framework's 'identify' function.
2.3. Sort the items in 2.1 by importance.	YES The items listed in 2.1 should be prioritised according to their criticality and business value.
2.4. The list created in 2.3 should be reviewed and updated on a frequent basis.	NO The framework makes no mention of reviewing and updating the list of items generated in 2.3 on a regular basis.
2.5. Determine the cyber risks that the bank assumes and poses to other organisations with which it is connected.	NO According to the ICIC framework, some cyber risks are assumed and posed to other organisations with which they are connected. It does not, however, essential that an organisation indicate where the detected cyber risk originates or is posed to.

Table 1 Continued: CPMI–IOSCO Guidelines – Fundamental Risk Management Categories Mapping

CATEGORY 3: PROTECTION	
3.1. Banks should establish a robust Information Communication Technology (ICT) control environment (e.g. encryptions, access controls, and ICT system configurations).	YES Access control, defensive technologies, and data security should all be implemented by an organisation.
3.2. The bank should implement adequate protection controls linked to the bank's cyber risk tolerance from the design stage of a system.	YES Safeguards should be implemented in accordance with the established cyber risk tolerance.
3.3. Put in place safeguards against internal threats, such as former and even current bank personnel.	YES Both internal and external threats should be safeguarded against.
3.4. Put in place safeguards against cyber risks posed by the organisations with whom the bank is linked.	YES Despite the fact that an organisation is not needed to declare that some identified cyber risks are posed by another organisation with whom it is linked, safeguards should be applied against all identified cyber risks.
CATEGORY 4: DETECTION	
4.1. Set up a security operations center to continuously monitor and detect cyberattacks in real time.	NO The ICIC framework requires an organisation to build detection processes and regularly monitor cybercrime incidents. It does not, however, necessitate real-time detection and detection of cybercrime incidents.
4.2. Detect cyberattacks that are both publicly known and unknown.	YES All cyberattacks, whether publicly known or unknown, must be detected.
4.3. Set up a multi-layered detection system that includes processes, technology, and people.	YES For probable cybercrime incidents, detection controls must include monitoring the physical environment, personnel activities, external service provider activities, devices, software, and systems.
4.4. Detected cyberattacks should be recorded and assessed.	YES In order to analyse how cyberattacks are managed, an organisation should keep track of those that are detected and identified.
CATEGORY 5: RESPONSE AND RECOVERY	
5.1. A bank should initiate an investigation after identifying a cyberattack and determine the type and extent of the harm caused by the attack.	YES An organisation should assess the determine the impact of a cyberattack after it takes place.
5.2. Take action to remedy the situation and prevent further damage..	YES After discovering a cyberattack, the following actions should be taken: analyse the impact, execute measures to mitigate the impact, enhance protective measures that were breached by the cyber-criminal, and return to regular operations.
5.3. Design the bank's system in such a way that operations can be resumed within two hours of the cyberattack.	NO ICIC does not specify the duration of the resumption of operations following a cyberattack. It does, however, emphasise that normal operations should be resumed as quickly as feasible.
5.4. Prepare for circumstances in which resuming operations within two hours may not be possible due to the prolonged absence of key people, processes, or systems.	NO ICIC does not specify the duration of the resumption of operations following a cyberattack. It does, however, emphasise that normal operations should be resumed as quickly as feasible.
5.5. The effectiveness of the response, resuming, and recovery programs should be evaluated.	YES To ensure that response and recovery programs are effective, they should be tested and analysed.
5.6. The bank's business continuity management, disaster recovery plans, and crisis management should all be synced with the response, resumption, and recovery programs.	YES Business continuity strategies should be in sync with an organisation's reaction preparations. Disaster recovery plans should be in sync with recovery programs.
5.7. Ascertain that processes and systems are established and tested to retrieve accurate data following a cyberattack.	YES Data backups must be created, maintained, and tested to ensure data recovery in the event of a cyberattack.

Source: Own analysis

Table 2: CPMI–IOSCO Guidelines – Overarching Categories Mapping

CPMI–IOSCO CYBER RESILIENCE GUIDELINES	ICIC FRAMEWORK PRACTICES
CATEGORY 6: TESTING	
6.1. Test the effectiveness of the bank's cyber risk management framework on a regular basis.	NO The subject of framework testing is not addressed in this framework.
6.2. Use the findings of the tests to strengthen your cyber resilience procedures. Vulnerability assessments, scenario-based testing, penetration tests, and red team tests are all examples of testing approaches.	NO The subject of framework testing is not addressed in this framework.
CATEGORY 7: SITUATIONAL AWARENESS	
7.1. Identity cyber risks that could have a major impact on the bank's ability to conduct business and meet its obligations.	YES According to the ICIC framework, for each cyber risk identified, an analysis, including an impact analysis, must be done.
7.2. Recognise cyber threats that could jeopardise the availability, integrity, and confidentiality of business processes.	YES According to the ICIC framework, for each cyber risk identified, an analysis, including an impact analysis, must be done.
7.3. Recognise cyber risks that could jeopardise the bank's reputational standing.	YES According to the ICIC framework, for each cyber risk identified, an analysis, including an impact analysis, must be done.
7.4. The list of cyber risks in 7.3 should be analysed, and the analysis should be reviewed and updated on a regular basis.	NO All cyber risks should be assessed, according to the ICIC framework. However, nowhere in the ICIC framework does it state that the analysis should be evaluated and updated on a regular basis.
CATEGORY 8: LEARNING AND EVOLVING	
8.1. Establish systems to identify lessons learned from cybercrime incidents.	YES Identifying and documenting lessons learned from cybercrime incidents should be part of response plans.
8.2. Use the lessons learned to strengthen the procedures for managing cyber risk.	YES Lessons acquired from cyberattack detection and response efforts should be incorporated into organisational response and cybersecurity activities.
8.3. Keep up with the newest cyber risk management technologies and practices.	YES In order to properly manage this ever-changing cybercrime, an organisation must actively adapt to evolving technology and cybersecurity measures.

Source: Own analysis

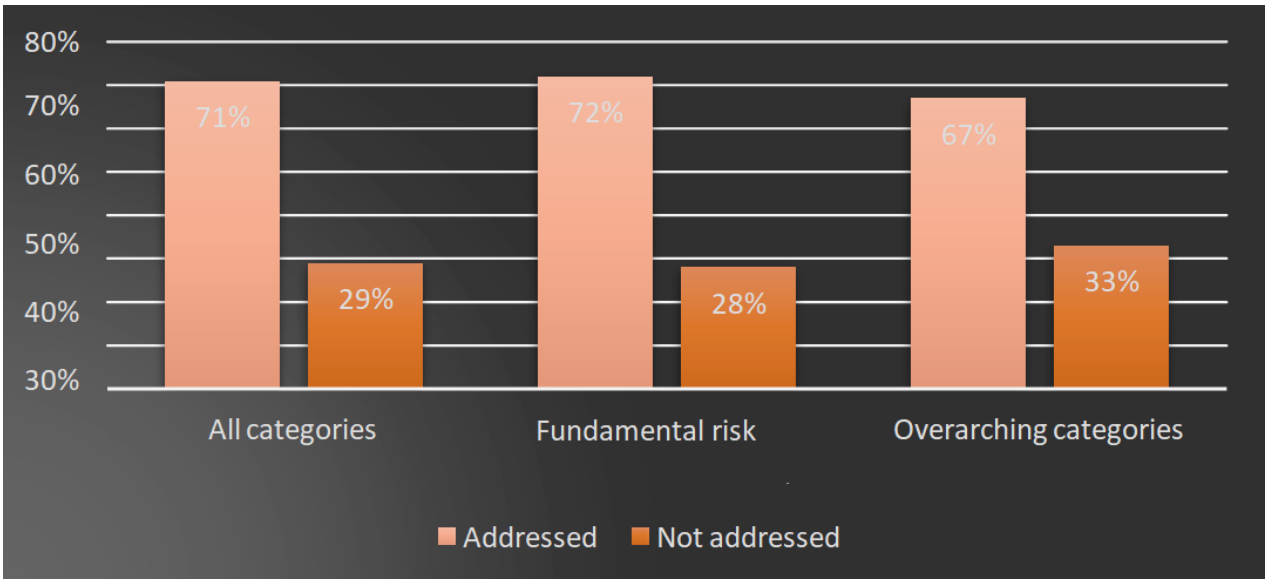
In Table 2 above, the ICIC framework is mapped against the CPMI–IOSCO cyber resilience guidelines under the overarching categories.

5. Research Findings and Discussions

The objective of this study is to establish whether the ICIC framework addresses the CPMI–IOSCO cyber resilience guidelines. The mapping in Tables 1 and 2 was carried determine the extent to which the ICIC framework addressed the CPMI–IOSCO cyber resilience guidelines. Figure 1 on the next page presents the analysis of the results from the mapping.

The mapping results indicate that the ICIC framework does, in fact, address the CPMI–IOSCO cyber resilience guidelines to an extent of 71%. The CPMI–IOSCO cyber resilience guidelines are largely made up of guidelines provided under the overarching categories, which are not addressed by the ICIC framework. The 'testing' category accounts for the majority of the 33% of guidelines not addressed by the overarching categories. This is the case because the ICIC framework does not cover 'framework testing'. Only 28% of the guidelines provided under the fundamental risk management categories are not addressed by the ICIC framework. The guidelines presented under the 'governance' category account for the majority of the 28%, as the ICIC framework core is made up of the identical categories of guidelines under fundamental risk management, except 'governance.'

Figure 1: An Analysis of the Mapping of the ICIC Framework against the CPMI–IOSCO Cyber Resilience Guidelines



Source: Authors

6. Conclusion and Recommendations

According to the SARB guidance note issued to South African banks in 2017, South African banks must align their cyber risk management procedures to the CPMI–IOSCO cyber resilience guidance. The guidance requires that banks should have a cyber risk management framework in place. This cyber risk management framework must address the CPMI–IOSCO cyber resilience guidelines. The ICIC framework addresses up to 71% of these guidelines. It was established that as a result of the ICIC framework being flexible, an organisation can modify it to meet its specific needs and objectives. Therefore, the study recommends the following:

- The South African banking industry should adopt the ICIC framework for the management of cyber risks for the following reasons:
  - » The ICIC framework created primarily to manage cyber risks;
  - » It is proven to be effective, flexible, efficient and cost effective;
  - » It is widely adopted by banks across the globe; and
  - » It already addresses a considerable number of the CPMI–IOSCO guidelines
- In order to be fully compliant to SARB and pass the appropriateness assessment by the office of the Registrar of banks, South African banks should modify the ICIC framework by adding only 29% of the CPMI–IOSCO guidelines not addressed by the ICIC framework. In that manner, all the CPMI–IOSCO guidelines will be addressed bythe modified version of the ICIC framework by South African banks.

References

Abdullah, F.M. 2019. Using big data analytics to predict and reduce cyber crimes. *International Journal of Mechanical Engineering and Technology*, 10(1):1540-1546. Available at: https://www.researchgate.net/profile/Fatma-Abdullah-3/publication/331113136_Using_big_data_analytics_to_predict_and_reduce_cyber_crimes/links/5d8f21 b8299bf10cff153270/Using-big-data-analytics-to-predict-and-reduce-cyber-crimes.Pdf. Accessed 17 June 2021.

Ahmed, R.R., Vveinhardt, J., Streimikiene, D., Ashraf, M. & Channar, Z.A. 2017. Modified SERVQUAL model and effects of customer attitude and technology on customer satisfaction in banking industry: mediation, moderation and conditional process analysis. *Journal of Business Economics and Management*, 18(5):974-1004. Available at: https://doi.org/10.3846/16111699.2017.1368034. Accessed 1 July 2021.

Almuhammadi, S. & Alsaleh, M. 2017. Information security maturity model for NIST cyber security framework. *Computer Science and Information Technology*, 52-62. Available at: https://airccj.org/CSCP/vol7/csit76505.pdf. Accessed 2 July 2021.

Barret, M. 2018. Framework for improving critical infrastructure. Available at: http://isawaterwastewater.com/wp-content/uploads/2018/08/WWAC-2018-NIST-Barrett_final.pdf. Accessed 2 July 2021.

Bengtsson, M. 2016. How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, (2):8-14. Available at: https://doi.org/10.1016/j.np ls.2016.01.001. Accessed 13 September 2018.

Bishnoi, T.R. & Devi, S. 2017. Information Technology in banking system. In Palgrave Macmillan Studies in Banking and Financial Institutions. Palgrave Macmillan: n.p. Available at: https://www.palgrave.com/gp/series/14678. Accessed 5 March 2018.

Boora, K.K. & Kavita, J. 2018. Implementation of Basel III Norms in Banking Industry: A Review of Empirical Literature. *The IUP Journal of Bank Management*, 17(3):7-24. Available at: http://content.ebscohost.com/ContentServer.asp?EbscoContent=DgJyMNLr40Sep7E4zOX0OLCmr1CeprVSsaa4SrKWxWXS&ContentCustomer=dGJyMPGssVGup7VRuePfgeyx9Yvf5ucA&T=P&P=AN&S=R&D=bth&K=131613195. Accessed 13 November 2018.

Ciglic, K., McKay, A., Hering, J. & Moore, T. 2017. Cybersecurity policy framework. A practical guide to the development of national cybersecurity policy. Available at: https://www.microsoft.com/en-us/cybersecurity/content-hub/Cybersecurity-Policy-Framework. Accessed 28 August 2018.

Coetzee, J. 2018. Strategic implications of Fintech on South African retail banks. *South African Journal of Economic and Management Sciences,* 21(1). Available at: https://journals.co.za/doi/abs/10.4102/sajems.v21i1.2455. Accessed 1 July 2021.

Committee on Payments and Market Infrastructures & International Organization of Securities and Commissions. 2016. Guidance on cyber resilience for financial markets infrastructures. Available at: https://www.bis.org/cpmi/publ/d146.pdf. Accessed 28 July 2018.

Crisanto, J.C. & Prenio, J. 2017. FSI insights on policy implementation No 2. Regulatory approaches to enhance banks' cyber-security frameworks. Available at: https://www.bis.org/fsi/publ/insights2.pdf. Accessed 20 September 2018.

Dalglish, S.R., Khalid, H. & McMahon, S.A. 2020. Document analysis in health policy research: The READ approach. *Health Policy and Planning*, 35(10). Available at: https://academic.oup.com/heapol/article/35/10/1424/5974853?login=true. Accessed 4 October 2021.

Dantis, D. 2017. 'Banking system as critical infrastructure', International Scientific Conference. Available at: https://www.proquest.com/openview/0d6054c4efe651153eb79aabb8fb17fa/1?pq-origsite=gscholar&cbl=2026346. Accessed 6 July 2021.

Deloitte. 2018. Cyber risk and regulation in Europe. A new paradigm for banks. Available at: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/IE_FS_Cyber_risk_regulation_0218_draft32.pdf. Accessed 20 June 2018.

Deloitte. 2019. IOSCO Cyber Task Force (CTF) Report: Assessing progress in the implementation of the core cybersecurity standards. Available at: https://www2.deloitte.com/lu/en/pages/risk/articles/iosco-cyber-task-force-report.html. Accessed 6 July 2021.

Delort, D. 2019. Risks in digital financial services and cyber resilience for financial market infrastructures. Available at: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Documents/Dorothee%20Delort.pdf. Accessed 6 July 2021.

Dina, A.E. 2019. 'Comparative assessment of insurance and banking regulation: Solvency II Versus Basel III', Strategica International Academic Conference, pp. 368-375. Available at: https://www.researchgate.net/profile/Alexandra-Zbuchea/publication/339041758_Strategica_2019_Proceedings_Upscaling_Digital_Transformation_in_Business_and_Economy/links/5e3a4a98a6fdccd96587f439/Strategica-2019-Proceedings-Upscaling-Digital-Transformation-in-Business-and-Economy.pdf#page=369. Accessed 5 July 2021.

Duvenhage, F.J. 2020. A comparison of cyber risk disclosure in the banking sector between South Africa and China. (Unpublished Masters Dissertation). North-West University. Available at: http://repository.nwu.ac.za/bitstream/handle/10394/36655/Duvenhage_FJ.pdf?sequence=1&isAllowed=y. Accessed 2 July 2021.

European Central Bank. 2019. Cyber resilience for financial market infrastructures. Available at: https://thedocs.worldbank.org/en/doc/189821576699037673-0130022019/original/FIGIECBOperationalCyberFinalWeb1213.pdf. Accessed 2 July 2021.

Evdokimova, Y., Shinkareva, O. & Egorova, E. 2019. 'Banking Information Technology as an element of the information society'. 54th International Scientific Conference on Economic and Social Development – XIX International Social Congress, pp. 550-555. Available at: https://www.researchgate.net/profile/Gulsum-Mammedova/publication/341443992_Book_of_proceeding_45th_ISCESD_Moscow_2019_1/links/5ec11a93a6fdcc90d67a8472/Book-of-proceeding-45th-ISCESD-Moscow-2019-1.pdf#page=564. Accessed 15 June 2021.

Gao, H. 2017. 'Analysis of the announced BASEL III reforms', International Conference on Education, Economics and Management Research, pp. 16-18. Available at: https://www.atlantis-press.com/article/25876811.pdf. Accessed 5 July 2021.

Griffiths, J.L. 2017. Cyber security as an emerging challenge to South African National Security. (Mini dissertation). University of Pretoria. Available at: https://repository.up.ac.za/bitstream/handle/2263/62639/Griffiths_Cyber_2017.pdf?sequence=1&isAll owed=y. Accessed 2 July 2021.

Hlongwane, P. 2020. 'The Application of Mixed Methods Research in Public Administration: Opportunity Missed or Taken?' The

5th Annual International Conference on Public Administration and Development Alternatives, pp. 441-449. Available at: http://ulspace.ul.ac.za/handle/10386/3223. Accessed 4 October 2021.

Hubbard, J. 2019. SA business underplaying the danger of cybercrime? Finweek. Available at: https://journals.co.za/doi/abs/10.10520 /EJC-1444bed59d. Accessed 26 June 2021.

Kgosana, R. 2018. Cybercrime costs SA almost R2.2bn a year. The Citizen. Available at: https://citizen.co.za/news/south-africa/crime/2047717/cybercrime-costs-sa-almost-r2-2bn-a-year/. Accessed 5 July 2021.

Kopp, E., Kaffenberger, L. & Wilson, C. 2017. Cyber risk, market failures and financial stability. IMF Working Paper. Available at: https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Faiures-and-Financial-Stability45104. Accessed 1 August 2018.

KPMG. 2021. Redefining operational resilience. Available at: https://assets.Kpmg/content/dam/kpmg/xx/pdf/2021/04/redefining-operational-resilience.pdf. Accessed 6 July 2021.

Krasonikolakis, I., Tsarbopoulos, M. & Eng, T. 2020. Are incumbent banks bygones in the face of digital transformation? *Journal of General Management*, 46(1):60-69. Available at: https://journals.sagepub.com/doi/full/10.1177030630702093788 3. Accessed 1 July 2021.

Kundu, S., Islam, K.A., Jui, T.T., Rafi, S., Hossain, A. & Chowdhury, I.H. 2018. Cyber crime trends in Bangladesh, an analysis and ways out to combat the threat', International Conference on Advanced Communications Technology. Doi: 10.23919/ICACT.2018.8323800. Available at: https://0-ieeexplore-ieee-org.ujlink.uj.ac.za/stamp/stamp.jsp?tp=&arnumber=8323800. Accessed 27 June 2018.

Kure, H.I. & Islam, S. 2019. Assets focus risk management framework for critical infrastructure cybersecurity risk management. *The Institute of Engineering and Technology Journals*, 4(4):332-340. Available at: https://ietresearch.Onlinelibrary.wiley.com/doi/pdf/10.1049/iet-cps.2018.5079. Accessed 6 July 2021.

Lekha, K.C. & Prakasam, S. 2017. Data mining techniques in detecting and predicting cyber crimes in banking sector', International Conference on Energy, Communication, Data Analytics and Soft Computing, pp. 1639-1643, doi: 10.1109/ICECDS.2017.838 9725. Available at: https://ieeexplore.ieee.org/abstract/document/8389725. Accessed 17 June 2021.

Liu, G. & Molise, T. 2018. Is Basel III counter-cyclical: The case of South Africa? ERSA working paper 757. Available at: https://www.econrsa.org/system/files/publications/working_papers/working_paper757.pdf. Accessed 5 July 2021.

Madiba, A. 2021. 'The scary nature of cybercrimes and the strain of bringing perpetrators to book', Sunday Independent News. Available at: https://www.iol.co.za/sundayindependent/news/the-scary-nature-of-cybercrimes-and-the-strain-of-bringing-perpetrators-to-book-7faee4e6-a180-4649-8ab5-40ad0590bc91. Accessed 18 June 2021.

Mapimele, F.V. & Mangoale, B.C. 2019. 'The cybercrime combating platform', 14th International Conference on Cyber Warfare and Security. Available at: https://www.ingentaconnect.com/content/hsp/jrmfi/2019/00000012/00000003/art00003. Accessed 1 July 2021.

Martins, A.T. 2021. 'Basel II/III Implementation in Africa and the impact on the resilience of its banking sectors: A case study of Nigeria', World Finance Conference, pp. 1-43. Available at: https://www.world-finance-conference.com/papers_wfc/8c890557e74860de0652fd7f8400c22a.pdf. Accessed 5 July 2021.

Mujinga, M., Eloff, M.M. & Kroeze, J.H. 2018. System usability scale evaluation of online banking services: A South African study. *South African Journal of Science*, 114(4):1.8. Available at: http://www.scielo.org.za/pdf/sajs/v114n3-4/14.pdf. Accessed 1 July 2021.

National Institute of Standards & Technology. 2018. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Available at: https://nvlpubs.nist.gov/nist pubs/CSWP/NIST.CSWP.04162018.pdf. Accessed 9 August 2018.

Nejad, M.C., Mansour, S. & Karamipour, A. 2021. An AHP-based multi-criteria model for assessment of the social sustainability of technology management process: A case study in banking industry. Technology in Society. Available at: https://www.Sciencedirect.com/science/article/abs/pii/S0160791X21000774. Accessed 1 July 2021.

Nkopane, T. 2016. The relevance of the BASEL III Accord within the South African banking system. (Thesis). Johannesburg: University of the Witwatersrand. Available at: https://hdl.handle.net/10539/23804. Accessed 14 November 2018.

Nuskiya, A.F. 2018. The effect of information technology on employees' performance in the banking industry in Sri Lanka. Empirical study based on the banks in Ampara District. *European Journal of Business and Management*, 10(6):47-52. Available at: http://rcbrnet.com/journals/rcbr/Vol_4_No_1_June_ 2015/6.pdf. Accessed 26 June 2021.

Nuyens, H. 2019. How disruptive are FinTech and digital for banks and regulators? *Risk Management in Financial Institutions*, 12(3):217-222. Available at: https://www.ingentaconnect.com/content/hsp/jrmfi/2019/00000012/00000003/art00003. Accessed 1 July 2021.

Oyetade, D., Obalade, A.A. & Muzindutsi, P.F. 2020. Impact of the BASEL IV framework on securitization and performance of commercial banks in South Africa. Banks and Bank Systems, 15(3):95-105. Available at: https://www.researchgate.net/publication/343919241_Impact_of_the_Basel_IV_framework_on_securitization_and_performance_of_commercial_banks_in_South_Africa. Accessed 2 July 2021.

Rahman, M. 2018. Banking system resiliency: Basel III, Islamic banking and cyber security. Available at: http://dspace.uiu.ac.bd/handle/52243/534. Accessed 2 July 2021.

Securities Industry & Financial Markets Association. 2016. CPMI-IOSCO Consultative Report: Guidance on Cyber

Resilience for Financial Market Infrastructures. Available at: https://www.sifma.org/wp-content/uploads/2017/05/sifma-submits-comments-to-cpmi-and-iosco-on-their-report-regarding-guidance-on-cyber-resilience-for-financial-market-infrastructures-fmis.pdf. Accessed 18 June 2018.

Shakdwipee, P. & Mehta, M. 2017. Impact of Basel III on Indian banks. *World Journal of Research and Review*, 4(1):40-45. Available at: https://www.academia.Edu/download/52525916/WJRR0401017.pdf. Accessed 5 July 2021.

Smith, C. 2018. Cybercrime now 55% of gross losses in SA banking industry – report. Fin24. Available at: https://www.fin24.com/Companies/Financial-Services/cybercrime-now-55-of-gross-losses-in-sa-banking-industry-report-20181004. Accessed 24 April 2019.

South African Reserve Bank, from the office of the Registrar of Banks. 2017. Guidance Note G4/2017. Available at: https://www.resban.co.za/Lists/News%20and%20Publications/Attachments/7803/G4%20of%202017.pdf. Accessed 7 April 2018.

Spitzner, L. 2017. Feedback on NIST CSF – Identify Function – Page 12 line 320. Available at: https://www.nist.gov/sites/default/files/documents/2018/01/24/2017-12-16-san.pdf. Accessed 18 June 2018.

Standard Bank. 2017. Standard Bank Group Risk and Capital Management Report 2017. Available at: http://annualreport2017.standardbank.com/downloads/Standard_bank_AIR2017_standard_bank_group_risk_and_capital_management_report_2017.pdf. Accessed 18 June 2018.

Tsen, E., Ko, R.K.L. & Slapničar, S. 2020. Organisational cyber resilience and its influence on cyber attack outcomes: An exploratory study of 1,145 publicised attacks. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3735636. Accessed 6 July 2021.

World Bank Group. 2017. Financial sector's cybersecurity: A regulatory digest. Available at: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf. Accessed 23 April 2018.

World Federation of Exchanges. 2018. WFE Response to the ECB: Cyber resilience oversight expectations (CROE). Available at: www.world-exchanges.org. Accessed 9 August 2018.

Zachozova, N., Kutsenko, D., Koval, O. & Kovalenko, A. 2021. Management of financial and economic security of critical infrastructure objects in the conditions of risks of quarantine restrictions: Strategic and personnel aspects', SHS Web of Conferences, pp. 1-8. Available at: https://www.shs-conferences.org/articles/shsconf/pdf/2021/18/shsconf_m3e22021_02002.pdf. Accessed 6 July 2021.