iKSP Journal of Business and Economics
http://iksp.org/journals/index.php/ijbe/index
iKSP Publisher

Global Regulators Assessments on Operational Risk Management, International Fines and Sanctions Violations

Nizam Shah Allabasc*[1]
[1]University Tun Abdul Razak (UNIRAZAK), Malaysia

Abstract - This study proposes to examine and review the responses from international regulators in relation to operational risk management. This review also seeks to measure the effect management support has in influencing and improving these four outcomes, namely; the safety of assets and infrastructure, customer satisfaction, cost reduction and employee performance. Further, it examines the record-breaking fines imposed on banking and financial institutions by global regulators, especially with regard to cases of fines for Anti-Money Laundering (AML) and sanctions violations, and considers recent operational risk loss events that have occurred on a global scale. In addition, certain issues identified in this study were valid enough to disclose a major moral hazard risk and operational risk implication to global banking and financial institutions. The results obtained from this study are pertinent owing to the operational loss and the reputational risks faced by nations in general and financial institutions in particular.

Keywords: Operational Risks Management, Risk Management, AML, Sanctions

INTRODUCTION

Operational risk practices are generally maintained and controlled by, amongst others, having proper management policies and procedures including adequate books, channels and records with basic internal accounting control, a strong compliance, internal audit which functions independent of the trading and revenue side of the business, clear limits on personnel, and risk management and control policies. Had the required proper management oversight, as well as the fundamental risk management and control practices of separating backroom and trading functions been in place, the losses at Barings and Daiwa could perhaps have been avoided, or at the very least, mitigated to a large degree. The obvious importance of maintaining proper operational risk management and control is underscored by these financial failures. BCBS (2019) sets out a list of recommendations in the consolidated version of its international standards framework for the regulations and supervision of banks. The consolidated framework sets out proposals on how to improve the approachability of the Basel Committee's ethics standard and to endorse dependable global clarification and implementation.

With the governance and supervisory spotlight on Operational Risk Management, there have been continuous as well as cumulative considerations in relation to the quantification of Operational Risk. This requirement for prospective overwhelming influence has been indicated by numerous big operational losses caused by or influenced by, among others, the safety of assets and infrastructure, customer satisfaction, cost reduction as well as employee performance. Due to the size of the above actions and their worrying impact on the monetary community, not to mention the potential for additional operational risk damages due to an ever-increasing number of products and processes, a sound monitoring

*Corresponding author:
Email: nizam_shah@hotmail.com (N.S. Allabasc)
iKSP Journal of Business and Economics (2021) 1(2): 44-50

and quantification of operational risk losses becomes progressively essential. According to Abdul Rahim, Noor & Faeeq, Munadil (2016), vigorous internal control systems are the most crucial principles in developing a compact operational risk management policy in banks. Due to the challenges and the competitiveness inherent in the corporate and commercial environment it is of particular importance for banks and financial institutions to recognize the risks that may arise and the significance of having proper operative policies, processes, procedures, systems and skills in place to mitigate any such risk that may arise.

In a regulatory statement issued by the Bank of Albania (BoA) with regard to operational risk, the following iterated procedures were carried out (Albania: Regulator Statement (2016)). Initially the core and supporting functions that BoA uses for exercising its role and achieving its objectives were identified. A consolidated and centralised chart of BoA's functions, responsibilities and segregation of duties were then created resulting in an improvement in BoA's governance. However, although BoA managed to improve the risk management process, the issue was not addressed comprehensively. In conclusion, as a result of the above, this institution would be more responsible, particularly with regard to governance, and confidence in this institution will have improved.

In a statement issued in 2016, The Office of the Superintendent of Financial Institutions Canada (OSFI) reiterated that the main issue for consideration by the financial organisations was the protection of their data, their systems and their customers from cyber-attacks and other online threats (Canada: Regulator Statement (2016)). OSFI had in 2013 released cyber-security self-assessment guidance to the financial institutions it regulates and supervises to facilitate and contribute to dialogue and conversation between these financial institutions, OSFI and their service providers. Although there are some issues still persisting, especially in matters such as those that lie outside of the institution's scope, collaborations with key partners and investments in employee training and awareness, OSFI would appear to be well placed to deal with cyber-attacks if and when they occur.

The Central Bank of Finland, also known as the Bank of Finland or Suomen Pankki in Finnish, Nordic still exist as the national monetary authority, but many of its functions have been taken over by the European Central Bank (ECB). However, in 2016, the Central Bank of Finland issued a statement in relation to the management of operational risk focusing on honing the governance of the organization towards excellence, and thereby reducing any uncertainty (Finland: Regulator Statement (2016). The challenge is in correctly prioritising the analysis and risk control measures, which are inherently complex and difficult to measure, and leading to focus on operational risk too easily losing out in the competition for the time and the attention of boards and management teams. Therefore, the regulators not only have to focus on best standards but also have to find ways to enforce a systemic view, making sure that network effects, i.e., the shared benefits of good risk management, are adequately considered.

The central bank in the French Republic is the Bank of France or Banque de France in French. According to the Bank of France, a cyber-attack is not only a potential risk but also an operational risk (France: Regulator Statement (2016)). Cyber risk is not only of a technical nature but requires a governance framework that is able to protect critical information and recover accurate data in case of an attack, and cyber threats should promote notably the role of governance and cyber risk culture within organisations. Therefore, it shows that information sharing among the stakeholders, comprising financial institutions and market infrastructures, financial supervisors and national security agencies, is of utmost importance to avoid contagion phenomena and facilitate global resilience (Malik et al., 2017; Abro et al., 2020).

The central bank of the Federal Republic of Germany is the Deutsche Bundesbank. A statement by the Deutsche Bundesbank said that operational risks could be categorised as conduct risk, IT risk, and identify and assess risk (Germany: Regulator Statement (2016)). In the "conduct risk" cases that occurred in the European Systematic Risk Board (ESRB) in the period between 2009 to 2014 alone, global losses from internal misconduct at banks amounted to approximately 200 billion euros. Where institutions fail to adjust to digitalization and its inherent challenges, there is IT risk. Bank finance includes detecting major deficits relating specifically to identifying and assessing the operational risks. Operational risks may become a serious issue in all parts of an organisation because of decisions and processes made or practiced in a bank's division.

The Hong Kong Monetary Authority (HKMA) is Hong Kong's currency board and the de facto central bank. The HKMA has stated that in the new era, the application and development of Fintech will definitely be the focus of this ongoing digital revolution (Hong Kong: Regulator Statement (2016)). The increasing reliance on technology in the delivery of financial services has led to an increase in systematic risk as a result of cyber threats to financial market infrastructure and the financial service industry. HKMA has further stated that it will continue to relentlessly enhance market infrastructure, investor protection, promote innovation and ensure the balance between novel products and services and investors' understanding and tolerance of risks (Hong Kong: Regulator Statement, 2016).

The Central Bank of Ireland (CBI) in the United Kingdom also known as Banc Ceannais na hEireann is Ireland's central bank, and is part of the ESCB. A 2015 PWC survey by the central bank found a 38% increase in the number of

cybersecurity incidents detected compared to the previous year. Subsequently in a statement by the CBI, it was pointed out that adequate investments in information security needed to be made by all financial institutions to achieve a robust and effective business aligned IT strategy (Ireland: Regulator Statement, 2016). Lastly, Boards and senior management should ensure that their organisations have adequate plans to identify and address any resourcing and capability gaps and take appropriate steps to handle any risks that may arise, including cybersecurity risks, IT risks and technical risks, any of which could strike at the heart of financial services businesses and have strategic implications for organisations.
The Bank of Japan (BoJ) is the central bank in Japan. However, as stated by the BoJ, the Japanese Financial Service Authority (JFSA), a Japanese governmental agency and an integrated financial regulator, would be responsible for overseeing banking, securities, exchange and insurance sectors in order to ensure the stability of the financial system of Japan (Japan: Regulator Statement, 2016). Two main challenges financial institutions face are adding more value to and for their clients and fully servicing clients through each business cycle and although easy to highlight, these challenges are difficult to solve. JFSA has indicated that it intends to contribute to improving efficiency in financial markets, reducing risks and crises, and trading costs and providing solutions to the global community including regulators, financial institutions and professionals. JFSA is also eager to continue tackling cyber security issues as well as continue discussions in relation to any clues that may pave the way for a new paradigm for managing operational risks in Japanese financial institutions (Ali et al., 2015).

The Monetary Authority of Macau (AMCM) based in Macau, People's Republic of China and which is under the Macau Special Administrative Region is the sole regulator of the financial sector. It has expended a lot of effort to strengthen corporate governance and the management of risk by financial institutions under it in order to cope with the changing economic and financial environment. The AMCM understands that financial supervision plays an important role in order to put in place and strengthen risk management systems and build confidence in the sector (Macao: Regulator Statement (2016)). AMCM has also stated that the therein mentioned principles, laws and regulations could form a policy framework which could effectively assist the financial sector to enhance their corporate governance and their management functions in relation to the observance of risks (Manaa & ul Haq, 2020).

Norges Bank is the central bank of Norway. In addition to having traditional central bank responsibilities such as monetary stability and price constancy, Norges Bank also manages the Government Pension Fund of Norway, a stabilisation fund that could be the world's largest independent wealth fund. The Norway Central Bank Statement (2017) states, inter alia, that inflation has been mainly low and stable since inflation targeting was introduced in 2001; the aim of leading against the wind is a way to achieve a sustainable path for inflation, output and employment and that the main task of monetary policy is to provide the economy with a nominal anchor. As an example, when inflation is firmly anchored, monetary policy can also contribute to real economic stability.

The Central Bank of the United Arab Emirates, located in Abu Dhabi, is the state institution accountable for the supervision and management of the currency, financial policy and banking regulations in the United Arab Emirates (UAE). The UAE: Regulator Statement (2016) states, among others, that financial institutions in UAE are all about their people and that operational risks exist because people make mistakes. It goes on to say that a healthy culture is one that recognizes mistakes for what they are, that encourages individuals to learn from their mistakes, encourages staff to escalate their concerns and that adjusts controls to mitigate the risks of mistakes being repeated. It further states that regulators, as supervisors, should work with financial institutions to encourage this sort of culture and to prevent the re-emergence of the more excessive practices of recent years.

The Federal Reserve System (FRS) is central banking and investment system of the United States of America (USA). The history of central banking in the USA encompasses various bank regulations, from early wildcat practices through to the present Federal Reserve System. To help in understanding the new regulatory paradigm, the FRS stated that there are seven key political developments and dynamics at play: namely, capital, liquidity, rate repurchase (RRP), the uniform fiduciary standard, foreign banking organisations (FBOs), anti-money laundering (AML) and cybersecurity (US regulatory developments (2017)). Notwithstanding the new approach to financial regulation in Washington, firms should not assume that key requirements will be significantly amended or repealed. There is industry wide acceptance that many of the practices to comply with these regulations are essential for establishing strong risk and capital management regimes, which provide institution specific and macro benefits.

A perusal of the regulatory reviews in the above discussed countries, would seem to suggest that inspection has an impact on the regulatory and management support of each country and could lead to improvements in the safety of assets and infrastructure, customer satisfaction, cost reduction and employee performance. In addition, Ion Croitoru (2014) explained that the exposure to operational risk in organisations could have an upward or downward risk appetite depending on the volume and complexity of transactions carried out as well as the quality and reliability of systems used in the internal control systems implemented. Therefore, all risks associated objectives, activities or actions taken should, as far as possible, be identified and recorded.

LITERATURE REVIEW

BCBS, (2016) proposes that the reviewed operational risk capital framework is to be constructed on a single non-model-based method for the approximation of operational risk capital, which it designated as the Standard Measurement Approach (SMA).

BCBS, (2018) describes the diversity of approaches thematically whilst emphasising that this would assist banks and supervisors steer the regulatory environment as well as provide beneficial contribution for recognising ranges where supplementary policy mechanisms could be acceptable. Moving forward, the BCBS Committee proposes to integrate the cyber measurement into its broader operational resilience work.

Financial Conduct Authority, (2018) provides for sanctions that are regulatory, government or governmental orders that prohibit a firm from carrying out transactions with a sanctioned person or organisation, and in some cases prohibit a firm from providing any financial services at all to these entities. Pascal Golec and Enrico Perotti (2017), stated, among others, that no asset is unconditionally safe. They describe as safe any debt distributed or assured by a safe government, suggesting a country with its own central bank, a steady currency and good defence of assets privileges.

Okoli, Ifeanyi, Monanu Oge & Gozie, Adibe (2016), specified the emphasis on investigating the influences affecting stakeholders' administration and the degree of stakeholders' consequence influence to the monetary industries.

METHODOLOGY

Operational risk is an exceptional event happening in the financial environment and can only be described up to a certain extend. By nature, they are not repetitive thus making it difficult to apply traditional statistics to them. This is a descriptive study of events that have occurred around the world,-and specially to events that have caused banks and financial institutions significant losses, with some running into billions of dollars. The data collection and source of data was derived from Deloitte & Touche Financial Advisory Services Pte Ltd.

Findings and Implications

The operational risks to financial institutions encompasses risks arising, amongst others, from contracts not entered into in good faith, where misleading information is provided to induce unjustified risks, from an effort to produce revenue before a bond's maturity and where misleading information is given about its assets, liabilities or credit capacity. Then US Federal Reserve Chairman, Bernanke in 2013 discussed the need to make the monetary structure safer and whilst acknowledging the moral challenge that it could pose globally (Bernanke, Ben S. (2013)). In an article in The Daily Reckoning, Bonner states that Citigroup's Chief Financial Officer, Gary Crittenden recognised that Citi's huge losses and damages publicised in November 2007 were due, among others, to unexpected actions (Bonner, B (2007)). Mahathir Mohamad has mentioned that, for Malaysia to be transformed into a value-driven developed nation, everybody needs to play their part in the fight against financial crime and that shared prosperity could only be achieved through shared responsibility (Tun Dr Mahathir Bin Mohamad (2019)). He went on to say that both financial institutions as well as all citizens had a vital role to play in preserving Malaysia's economic system.

Table 1: Fines for AML and Sanctions Violations in 2015

Financial Institutions	**USD Amount Levied**
MoneyGram	100,000,000.00
Barclays	298,000,000
Lloyds Banking Groups	350,000,000
ABN AMBRO	500,000,000
Credit Suisse	536,000,000
ING	619,000,000
Standard Chartered	967,000,000
HSBC	1,920,000,000
BNP Paribas	8,970,000,000
Total	14,260,000,000.00

Source: Deloitte & Touche Financial Advisory Services Pte Ltd, 2015

As can be seen in Table 1 and Figure 1, record-breaking fines have been imposed on financial institutions for Anti-Money Laundering (AML) activities as well as sanctions violations from 2003 to 2014 (Deloitte & Touche Financial Advisory Services Pte Ltd, 2015)). The total amount levied on the nine global financial institutions, namely, MoneyGram, Barclays, Lloyds Banking Group, ABN AMBRO, Credit Suisse, ING, Standard Chartered, HSBC and BNP Paribas, was USD14.26 billion. Of the top-three BNP Paribas incurred fines amounting to USD8.97 billion, HSBC incurred fines amounting to USD1.2 billion and Standard Chartered incurred fines amounting to USD967 million. Alexandra Rosi (2015) has suggested that some banks and financial institutions seem to be purposefully de-risking their client portfolio by terminating accounts of Politically Exposed Persons (PEPs) due to the improved resource and compliance costs associated with reviewing and continuing these relationships. One of the main challenges facing banks and financial institutions is the sheer volume of false positive alerts which could have been caused by, among others, crude rules based on very simple matching criteria that have been plotted against uncleansed customer data, imperfect list records, unexpected changes to sanctions lists, poorly designed and formatted customer information data, misspellings, aliases and possible growth in third party references lists.

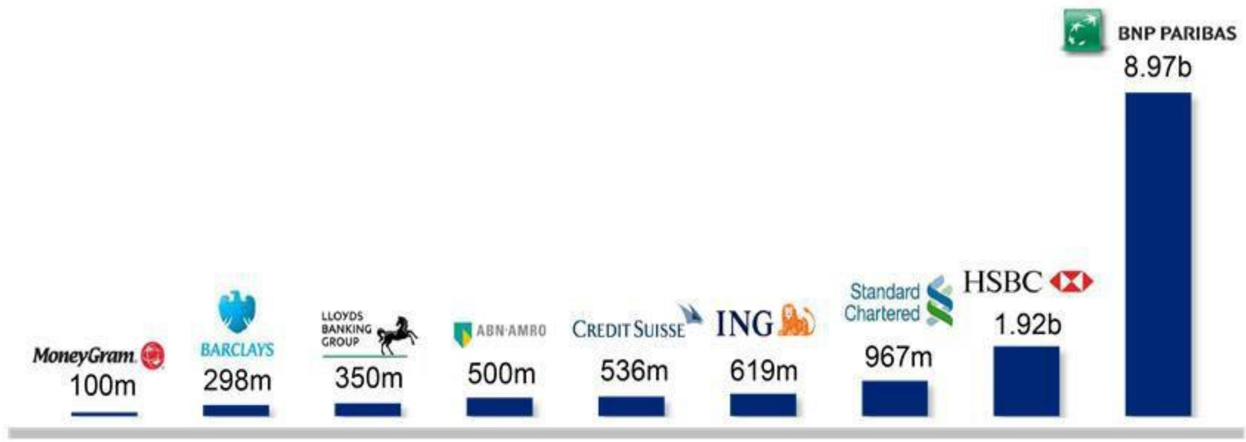

Figure 1 Examples of Fines for AML and Sanctions Violations (in USD million)
Source: Deloitte & Touche Financial Advisory Services Pte Ltd, 2015

Figure 1 shows the increasing trend in fines and penalties from 2003 to 2014 due to increased regulatory scrutiny. It also shows that while the number of fines (150) in 2003 amounted to lower than USD25 million, by 2014 the highest fine was USD8.97 billion.

The above two examples and trends of fines in recent years shows that officials have significantly stepped up execution of AML and Counter Financing Terrorism (CFT) laws and procedures. In recent times, it has not been unusual to see the US Justice Department and other regulators publicise multi-million-dollar penalties as settlements for illegal or domestic AML events. Occasionally the compliance associated penalties surpass countless hundreds of millions of dollars with the 2014 penalty levied on BNP Paribas for AML and related sanctions of USD8.97 billion being an extreme example. Nor Shamsiah, a regulator in Malaysia has executed many policies, guidelines and enforcements to help protect the local financial system against money laundering and terrorism financing related risks (Nor Shamsiah Mohd Yunus (2019)). As stated, Banking and Financial Institutions are responsible as corporate citizens to play their respective parts to safeguard the economy and the monetary system.

CONCLUSION

International supervisory and regulatory entities need to proactively enforce AML regulations and executions efficiently and competently to prevent money laundering and counter financing of terrorism related activities. This change in attitude can be seen in the form of unprecedented financial penalties levied by regulatory agencies, especially in the United States of America. There has been a significant increase in regulations and guidelines targeting banks and financial institutions, notably, with respect to US Bank Secrecy Act, AML and US sanction programs, including sanctions administered by US Department of the Treasury's Office of Foreign Assets Control. According to Tom Groenfeldt (2018), between 2009 and 2012 more than 50,000 regulations and guidelines were published across the G20 (Group of 20) nations, with almost 50,000 supervisory updates being made in 2015 alone.

Additionally, banking and financial institutions should have in place and implement sufficient control measures to help mitigate AML risks of any customer~~s~~ identified in the risk assessment stage by having adequate policies, controls and procedures to manage and minimise any risks that have been identified. This then has to be followed by monitoring and implementing these policies, controls, and procedures, reviewing and enhancing them if necessary, in addition to taking enhanced measures to manage and mitigate the risks where higher risks have been identified. To further enhance the operational and moral hazard risk management and to by lessen any penalties, the monetary industry worldwide is now implementing and accepting new additional technologies such as, electronic KYC (eKYC) via facial recognition, smartphone applications and learning to create a single platform for client engagement and understandings. A paper by Lamarque, Éric, Maurer & Frantz (2009), explained that the financial consequences of reputational risk are almost impossible to evaluate precisely, but it is not considered as an operational risk. Additionally, the banking theory has not considered reputational risk in its analysis of bank risk management.

Banks and financial institutions need to efficiently manage their funds in order to accumulate millions of dollars of profit in a year. Moral hazard risk associated with operational risk events that oftentimes occur due to lack of regulatory measures can result in unexpectedly significant losses to these institutions. The profits earned can be wiped out by a single operational risk event. If two or three such events happen in a year, the banks may end up showing net losses instead of net profits. Millions of dollars of profits could be wiped out due to one or two operational risk events. Karambu Kiende Gatimbu, Henry Kimathi & Joseph Masinde Wabwire (2017), noticed, while assessing the effect of corporate risk management disclosure on financial performance of listed firms in Kenya, that risk disclosures were found to have positive effects but with no significant difference on mean financial performance. However, there was a significant relationship between risk disclosure and financial performance.

Acknowledgement

The author research titled a robust comparison among Islamic and conventional banks on operational risks management and this journal was presented virtually in International Conference on Innovative Trends in business and Technology (iCITBT 2020) and supported by MyBrain15, which is a program introduced by the Malaysian Ministry of Higher Education (MOHE) which finances postgraduate student's education.

REFERENCES

Abdul Rahim, Noor & Faeeq, Munadil. (2016). Internal Control System and Perceived Operational Risk Management in Malaysian Conventional Banking Industry, 3rd Annual ECoFI Symposium 2016, 19-20 December 2016, Kedah, Malaysia, Accessed on 5th November 2020 < http://repo.uum.edu.my/25121/>

Abro, S., Shaikh, S., Abro, R. A., Soomro, S. F., & Malik, H. M. (2020). Aspect Based Sentimental Analysis of Hotel Reviews: A Comparative Study. *Sukkur IBA Journal of Computing and Mathematical Sciences*, *4*(1), 11-20.

Albania: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568196/Supplements/Albania-Regulator-statement.html?supplementListld=96382 [Accessed on 30th July 2018].

Alexandra Rosi (2015), How to Audit Controls to Manage Financial Crime Compliance (FCC) Risks Associated with Politically Exposed Persons, Association of Certified Anti-Money Laundering Specialist (ACAMS), USA. Retrieved from: http://www.acams.org/wp-content/uploads/2015/08/How-to-Audit-Controls-to-Manage-FCC-Risks-Associated-with-PEPs-A-Rosi.pdf

Ali, R., Abrar-ul-haq, M., & Ullah, S. (2015). Macroeconomic Indicators and Stock Market Development. *Developing Country Studies*, *5*, 139-149.

BCBS (2016), Standardised Measurement Approach for operational risk. Basel Committee on Banking Supervision (*BCBS*), Bank for International Settlements, Basel, Switzerland. Available at: < https://www.bis.org/bcbs/publ/d355.htm> [Accessed on 15th December 2020]

BCBS (2018), Cyber-resilience: range of practices. Basel Committee on Banking Supervision (*BCBS*), Bank for International Settlements, Basel, Switzerland. Available at: < https://www.bis.org/bcbs/publ/d454.htm> [Accessed on 15th December 2020]

BCBS (2019), Consolidated Basel Framework. Basel Committee on Banking Supervision (*BCBS*), Bank for International Settlements, Basel, Switzerland. Available at: < https://www.bis.org/bcbs/publ/d462.htm> [Accessed on 15th December 2020]

Bernanke, Ben S. (2013), Communication and Monetary Policy, speech delivered at the National Economists Club Annual Dinner, Herbert Stein Memorial Lecture, Washington, D.C., on 19th November 2013

Bonner, B (2007). "Goldman Sachs was wrong and 2 million families may lose their homes." Added to dailyreckoning.com.au on November 14, 2007.

Canada: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568073/Supplements/Canada-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

Financial Conduct Authority (2018), Financial Sanctions, London United Kingdom. Retrieved from https://www.fca.org.uk/firms/financial-crime/financial-sanctions

Finland: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568206/Supplements/Finland-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

France: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568218/Supplements/France-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

Germany: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568136/Supplements/Germany-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

Hong Kong: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568219/Supplements/Hong-Kong-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

Ion Croitoru, (2014), Operational Risk Management and Monitoring, Internal Auditing and Risk Management, Athenaeum University of Bucharest, Vol. 36(1), Pages 21-31, December 2014.

Ireland: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568227/Supplements/Ireland-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

Japan: Regulator Statement (2016). Retrieved fromhttp://www.iflr.com/IssueArticle/3568163/Supplements/Japan-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

Karambu Kiende Gatimbu, Henry Kimathi, Joseph Masinde Wabwire, (2017), Effect of Corporate Risk Management Disclosure on Financial Performance of Non-Financial Service Firms Listed at Nairobi Securities Exchange, Kenya, International Journal of Business Continuity and Risk Management, Inderscience Enterprises Ltd, vol. 7(2), pages 95-102.

Lamarque, Éric, Maurer, Frantz, (2009), Operational Risk in Banks: Designing A Supervision and Control Framework, French Journal of Management. February 2009, Issue 191, p93-108.

Macao: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568236/Supplements/Macao-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

Malik, H. A. M., Abid, F., Wahiddin, M. R., & Bhatti, Z. (2017). Robustness of dengue complex network under targeted versus random attack. *Complexity*, *2017*.

Manaa, A., & ul Haq, M. A. (2020). The Effects of SMEs, Population and Education level on Unemployment in Kingdom of Bahrain. *iKSP Journal of Business and Economics*, *1*(2), 23-33.

Nor Shamsiah Mohd Yunus (2019), Key Address by Governor of Central Bank of Malaysia at The 11th International Conference On Financial Crime and Terrorism Financing (IFCTF) 2019 Building Trust and Transparency: Collaborate, Accelerate, Strengthen On 5 November 2019, Malaysia. Retrieved from: https://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=842

Norway Central Bank Statement 2017). Retrieved from http://www.iflr.com/IssueArticle/3748149/Norway-Central-Bank-Statement.html [Accessed on 28th July 2018].

Okoli, Ifeanyi, Monanu Oge & Gozie, Adibe (2016). Effective Stakeholders Management in Banking Industry. Volume 4. Page 32 - 36. International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264)Vol. 4, No. 1, April 2016 Available at: <https://www.researchgate.net/publication/310607268_Effective_Stakeholders_Management_in_Banking_Industry> [Accessed 15th December 2020]

Pascal Golec and Enrico Perotti, (2017), Safe assets: a review, No 2035, Working Paper Series, European Central Bank; Frankfurt a. M. Available at: https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp2035.en.pdf [Accessed 15th December 2020]

Tom Groenfeldt (2018), Taming The High Costs of Compliance with Tech, Forbes Media, USA Access: https://www.forbes.com/sites/tomgroenfeldt/2018/03/22/taming-the-high-costs-of-compliance-with-tech/#796acec55d3f

Tun Dr Mahathir Bin Mohamad (2019), Special Address by Prime Minister of Malaysia at The 11th International Conference On Financial Crime and Terrorism Financing (IFCTF) 2019 Building Trust and Transparency: Collaborate, Accelerate, Strengthen On 5 November 2019, Malaysia. Retrieved from: https://www.pmo.gov.my/wp-content/uploads/2019/11/Media-Copy-Special-Address-by-YAB-PM-at-the-11th-IFCTF-2019-on-5-November-2019-1.pdf

UAE: Regulator Statement (2016). Retrieved from http://www.iflr.com/IssueArticle/3568267/Supplements/UAE-Regulator-statement.html?supplementListld=96382 [Accessed on 28th July 2018].

US regulatory developments (2017). Retrieved from http://www.iflr.com/IssueArticle/3748210/US-regulatory-developments.html [Accessed on 28th July 2018].