Operational Risk Implications; A Case Study of Locally Incorporated European Bank

Nizam Shah Allabasc, Ravindran Ramasamy
University Tun Abdul Razak (UNIRAZAK), Malaysia
Email of corresponding auhtor: nizam_shah@hotmail.com

Abstract

The purpose of this study is to examine the implication of the operational risk in the locally incorporated European Bank in Malaysia. The operational risk constitutes a small part of a bank's risk profile which includes unpredicted measures that might possibly source the failure of the whole bank. Therefore, the bank has implemented permanent control plan methods which arise from the annual risk assessment plan. Moreover, the Permanent Control Plan for each department of the bank resulting in the process and procedure review on the risk assessment task to reduce or eliminate unwanted issues and problems arise from the process and system in the organisations. Each risk assessment activity with the permanent control plan was approved by the bank's top level management before executed by phases in the year. There are 4 phases' in the permanent control plan; monthly, quarterly, half yearly and yearly. In this study the researchers has looked into the half yearly control plan. The half yearly permanent control plan exercise executed by the Operational Risk Officer found non-compliance issues on a few department's work processes. As a result, a few key operational risk management implications faced by the bank with this incompliance activity. Besides that, the issues identified in this study was firm enough to address a major operational risk implication to the bank. Furthermore, there was no any action taken by the Permanent Control Manager to prevent this incompliance activity in future. As a conclusion, the results obtained from this study is necessary due to the operational loss and the reputational risks faced by the financial organization.

Keywords: operational risk, assessment, permanent control, non-compliance.

Introduction

The Operational Risk comprises of a wide scale of mixed mode risks. The risks are business interruption, stakeholder dissatisfactions and implications on the organization, increased cost of products services in the organisations as well as employee health and safety hazards. It also includes other primary risks such as fraud, transaction failures, legal and regulatory breaches, inferior human technical performance, physical damage, and stakeholder safety and assets. These operational risk factors may cause huge financial losses directly or indirectly as well as reputational damages to the financial institutions. On the other hand, the Bank for International Settlements (BIS) in 2015, interpreted the operational risk management as the risk of loss resulting from inadequate or failed internal process, people and systems or from any other external events. In addition, it also includes legal risks, but eliminates strategic and reputational risk. To support this, there are few real incidences which took place that clearly indicates the existence of the operational risks and the risk management implications faced by the organisations.
On a different not, the Basel Committee on Banking Supervision (BCBS) is a team of Banking and Financial Institutions regulatory consultants that was established by the Central Bank of Governors of the

Group of Ten Countries in 1974. From the basic ground of the Basel regulation of worldwide active financial institutions set, capital adequacy soon become the main emphasis of the BCBS. There was also a robust credit within the organisation for superseding multinational accord to reinforce the steadiness of the international financial institution system and to eliminate a foundation of reasonable dissimilarity arising from the differences in nationwide capital requirements.

One of the incidents worth mentioning here is, the clear indication of the change in the estimated cost to the Deposit Insurance Fund (DIF), United States as the sum of money paid out of the Federal Deposits Insurance Corporations (FDIC) DIF to the investors that likely won't be recovered by the sale of the bank's internal and external assets properties.

Table 1 shows the bank's failures ranging from the year 2009 – 2016. This data was obtained from the analysis carried out by the Federal Deposits Insurance Corporations (FDIC) in August 2017. According to the analysis, the costs of the bank failures for the past 8 years which encompasses 495 banks, amounts to a total of US$75,103,000,000. This may be due to the inappropriate management of the operational risk associated with other risks of the banking institutions. In addition, FDIC also declared that the bank's failure was caused by the managerial weakness, internal routine control's weakness and failure to prevent the frauds due to volatile economic conditions.

Table 1 Bank Failures ranging from the year 2009 – 2016 in United States of America**.**

No	Year	Bank Failure Cost to DIF (USD) Million	No of Banks
1	2009	38,732	140
2	2010	22,904	157
3	2011	7,945	92
4	2012	2,785	51
5	2013	1,165	24
6	2014	399	18
7	2015	894	8
8	2016	279	5
Total		75,103	495

Source: Federal Deposits Insurance Corporations, (2017) United States of America (USA).

The Figure 1 and Figure 2 below shows the comparison of the operational loss globally throughout the year of 2009 to 2016. Stringent Basel III regulations, had reduced the operational losses drastically from US$39 billion in 2009 to meagre US$279 million. In terms of percentage, the drop is at 137.82% which is indicates better operational risk management globally that helps in reduction of losses within the banks.

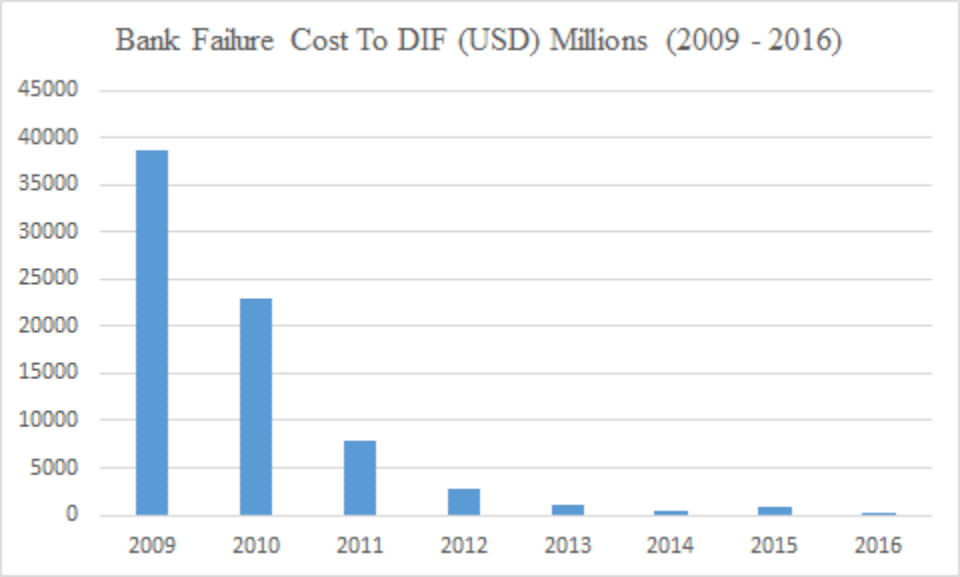

Figure 1: Bank Failure Cost to DIF (USD) Millions from 2009 to 2016 in USA.

Figure 2: Number of Bank Failures from 2009 to 2016 in USA.

In summary, the stringent Basel III regulations were able to increase the capital requirements for banks, which systematically prime banks to be more efficient, thus hindering their growth. Moreover, it doesn't change the risk-weighting technique which was the main motive behind the subprime catastrophe. Nevertheless, Basel III is still relying on the bond rating agencies, as weights are allocated based on the rating. It also aims to be in accordance with banking regulations across the world. According to Saul Perez, 2014, some countries have different regulatory requirements. For example, in India, they have better regulatory frameworks compared to Basel III. However, some past studies suggested that, when regulations are sought to be harmonised across the world, they tend to move towards the worst regulations. In addition, according to Saul Perez, 2014, some economist has suggested that Basel III

Accord is likely to hurt a country's growth by keeping the infrequent tied up for less and developing nations. However, the Malaysian monetary system includes a variety of financial institutes to serve the wide range and complex needs of the national economy. The Malaysian financial system comprises of conventional and Islamic banking and financial institution. Even though, banking and financial institution may sound the same, however, according to Central Bank of Malaysia (BNM), not all banks has full banking license for example, Malaysia Building Society Berhad is a Scheduled Institution under the Banking and Financial Institution Act and Bank Rakyat is still on biggest Islamic Co-Operative Bank. Both of the banking and financial institutions, co-exists and functions in par with each other. The stability and growth of the banking and financial institutions in the country is a reflection of the concrete development of the nation's financial sector itself. It indicates that the banking and financial institutions are vital for a nation's development.

In the recent years, Malaysia's monetary structure has experienced a global financial catastrophe. However, the global financial crisis experienced by Malaysia is partly being helped by monetary mediators on cross border capital. The well-developed regulatory and the governance administrations as well as with a well-capitalized banking system, it will further strengthen Malaysia's financial sector. Nevertheless, the stress tests may result in the financial institutions being robust on the economic shocks. Moreover, other risks faced by the banking system generally are those connected to quick financing evolution, rising house prices, and high domestic leverage, which call for improvements on the observations of the domestic leverage. Table 2 below, shows an overview of the number of licensed banks and financial institutions under the preview of BNM as at 31st December 2016. Primarily The Malaysian Banking and Financial Institutions comprises of Islamic, Commercial, International Islamic, Investment and Other Financial Institutions.

Table 2 List of Licensed Banks and Financial Institutions in Malaysia (as at 2016)

Banking and Financial Institutions	Malaysian Controlled Institutions (L)	Foreign Controlled Institutions (F)	Total
Islamic	10	6	16
Commercial	7	21	28
International Islamic	0	3	3
Investment	11	0	11
Other Financial Institutions	2	0	2
Total	30	30	60

Source: Bank Negara Malaysia (2016)

The Malaysian financial sector consists of 30 locally controlled institutions and 30 foreign controlled institutions. They are all very well established organizations with high level of governance whereby they are monitored constantly and supervised timely by the Central Bank of Malaysia. These banks are separated into four main sections, namely; Islamic, Commercial, International Islamic, Investment and other financial institutions. The governance and supervision on risk administrations for financial institutions displays a high degree of compliance with global banking standards. The areas that have the potential for improvements are mainly, the enhancement of the framework, renewal of the policies and procedures of consolidated management and addressing the Islamic Financial Services Act 2013 (ISFA 2013) (formerly known as Islamic Banking Act 1983) provisions that could theoretically reflect on independence of supervisory aspect for all financial institutions.

As a conclusion, the Operational Risk Management in Malaysian Banking and Financial Institutions is defined as the risk or threat of subsequent losses from insufficient or unsuccessful internal processes, procedures, people, employee, stakeholders, systems and external events. On a different note, the

operational risk exists in various activities, products and services of banking and financial institutions and has the possibility to contribute to malpractices through numerous activities and business units within the banking industry.

Literature Review

In the world of digitization, where every information is stored digitally, it creates a problem of security for everybody. There a numerous cases on operational risk associated with cyber-attacks that effects the financial institutions all around the world due to the breach of security.

On May 2017, a worldwide cyber-attack on computers running using Microsoft Window operating system took place. The attack was created by WannaCry ransomware crypto worm, which targeted user's computers by encrypting the data in it and demanding ransom in the Bitcoin cryptocurrency. It's a major attack on the Russian Central Bank. This incident was reported via Russian state media agency. Based on the report, the bank discovered that malware bulk emails were send to banks whereby, no resources were detected to be compromised. The bank reported that those monitoring the cyber-attacks found no compromising data resources of banking institutions. Moreover, according to Sam Jones (2017), countries such as Russia, Ukraine, India and Taiwan were the most seriously affected countries based on reports from the cyber security company known as the Kaspersky Lab.

In February 2016, the Bangladesh Bank hackers managed to steal USD81 million from the Bangladesh Central Bank, in one of the largest bank heists in history. They cleared their tracks after hacking into the heart of global financial system Society for Worldwide Interbank Financial Telecommunications (SWIFT), an international payment network used globally. SWIFT is a global messaging network which is used for most international money and security transfers. The heist was detected by the Bangladesh police department. Based on their investigation, they found evidence that the reason for the heist in the bank was because of using a second-hand USD10 network switch without a firewall to run its network. Without firewall, the hackers managed to access the bank's entire infrastructure, including the SWIFT servers resulting in the failure of the network security.

In April and May 2012, a huge loss in the trading transpired at J.P. Morgan's Chief Investment Office which made dealings through its London branch. An approximate trading loss of USD$2 billion was declared, with the actual loss expected to be considerably higher. These events gave rise to a number of investigations to examine the firm's operational risk management systems and internal controls. As a result of the investigations, it was found that the bank is expected to lose US$800 million in its corporate segment in the second quarter of the year 2012, compared to the previous estimates that the segment would post US$200 million profit. The scenario began when the unit run by Chief Investment Officer, Ina Drew stepped down. A series of derivatives transactions involving credit default swaps (CDS) was entered, reportedly as part of the bank's hedging strategy. The trader, Bruno Iksil, nicknamed as the London Whale, accumulated outsized CDS positions in the market. Due to that, some of the hedging losses were offset by taking US$1 billion in previous unrealized gains from the bank's portfolio.

In the early of September 2011, the Swiss Bank UBS announced that it had lost over US$2 billion dollars, as a results of unauthorized trading performed by Kweku Adoboli, a director of the bank's Global Synthetic Equities Trading team in London. The revelation could be the third largest loss of its kind in banking history. This implication resulted in the UBS being traded down 11% on the US stock exchange at trading, even as the European markets closed higher on that day.

Findings and Implications

The half yearly permanent control exercise executed by the Operational Risk Officer in locally incorporated European Bank) whereby, bank found non-compliance issues of few departments in their daily tasks. Due to reputational issues, the researcher has refrained from mentioning the bank's name. The Permanent Control exercise resulted due to the risk assessment severity and risk frequency rating process of each department during the annual review of the department's work process of task flow. The function of risk assessment process in the organisation was to reduce the operational loss which might be a reputational risk of the bank.

One of the issue is related to relief function. Customer Service Management Department was faced with disbursements by reason of corporate finance agreements. However, the Client Service Officer from the European Bank who was in charge of the disbursements was on medical leave for 2 months. In the absence of the Client Service Officer (CSO), there was no remedial action taken by the Head of Department in having a relief officer. As a result of this delay, the bank faced implications in onboarding of new clients with this incompliance activity. These lead to failure on the practice of Know Your Customer (KYC) policy. Regular review of due dates are not closely monitored for clients and trigger outdated assessment which may lead to jeopardise continuation of client-relationship. Apart from that, document custody of bank-client transactions was inappropriately retained. Due to that, the imposed financing surcharge on late payments and receipts data are not recorded into the client's account. This clearly was a loss to the bank due to the improper management of the bank-client relationship in the organisation. The issues were serious enough to trigger a major operational risk implication to the bank, and the action to rectify this matter were conducted by stages.

Policy and Procedures which falls under the supervision of the Organisation and Methods Department, their manuals were not reviewed for the past 3 years. Moreover, 28 procedure manuals and 7 policy manuals involved key business units. The general practice of banking institution is that each procedure must be approved by two committee members, namely Department Head and Executive Risk Management Committee (ERMC). However, the bank's policy of practice is that they are approved by procedure level and additionally as final step by Board and Top Management. The actual process for reviewing each procedure and policy, then followed by the endorsement and approval takes a few months. The concerns in policy and procedure remained to contribute to operational risk implications to the organization as the approval of entire manual of the organisation took nearly 12 months for the review and approval process.

Service Level Agreements (SLA) procedures and methods are in fact a quality process which uses internal customer inputs to set target. The SLA dashboard performances was not maintained and sustained as per agreements, and the bank as customer did not concern about the deliverables of the service provider. According to the agreement, it has a specified duration period, and it is clearly indicated and outlined as of the responsibility of each party including expectation outputs with performance measures. However, the bank officers who are supposed to be knowledgeable on the procedures for monitoring the performance of the services as well as problem solving procedures, was not aware of his responsibilities and was not given any training on that task. The officer was only being a custodian keeper of the SLAs documents and maintaining the timeline. All the deliverables of the service provider were kept as general records and was not subjected for review of their performance and continuous improvement of tasks.

Adequate data management and retention will enable a successful Information Technology (IT) Management and Infrastructure. However, there were issues regarding the server room control system's Air Condition and Ventilation where the temperature rose up to 82 degrees Fahrenheit during a normal

business day. The ideal server room temperature is in the range of 65^{o} to 70^{o} Fahrenheit (18^{o} – 21^{o} Celsius). Moreover, phone equipment application should have notified the IT Department Officers, Head of Department and the Chief Operating Officer (COO) on the rise in temperature. The phone application system would have considered fail when the server room temperature reached 82 degrees as there was scale setting to trigger alarm at 71^{o} – 73^{o} Fahrenheit. Incidentally, there was an alternative method, by way of email, where notification was sent to the respective person to highlight the issue. The relevant officers manage to handle the issue by rescaling the temperature in the server room on time and subsequently the IT department reported in their incident management report. The main matter is what the server's internal thermometers were reading. This incident occurrence incurred additional costs to the organisation on the replacement of phone alarming application system and reading status due to increase in the server room temperature range. Referring to the above issue, the BNM Governor Datuk Muhammad Ibrahim (May 2016) mentioned about the prospective influence of technological interruptions to the monetary sector and advised that a predictable 10% to 40% of overall financial transaction revenues could be at risk by 2025 due to financial technology or fintech innovations. This may be caused by the commercial sectors incorporating software to deliver quicker and low-cost financial facilities.

There was another non-compliance issue found in the Human Capital Department due to non-existence of Exit Form. It's crucial to study details of the employee's exit, on the foundation that condemnation is a cooperative act for the banks developments and assist working affiliation end on a good communication. However, it was found that the exit procedure for a particular employee was not conducted as per the organisation's procedure. The Department's manual states on exit procedure but there was no form as records to record proper exit of the employee. The prime concern is that an employee's departure with take along a few desk drawer cupboard keys and employee parking pass. As a result, the alternative keys could be retrieved by Administration Department's from their safe keeping of spare keys, but the organization incurs additional cost for replacement of the parking access card.

The governance and supervisory spotlight on Operational Risk Management by the Risk Officer, consideration has been continually cumulative. Considerations keen to the quantification of Operational Risk perspectives' overwhelming influence has shown numerous big operational losses. Since the size of the above actions and their worrying impact on the monetary community as well as the rising likelihood of operational risk damages due to an ever-growing difficulty of products and processes, a sound monitoring and quantification of operational risk losses becomes increasingly essential.

Conclusion

The analysis from the above five major issues rose from the inter-departmental connections, customer service management, organisation and methods, SLA business management, IT and human capital. The Operational Risk Officer produced a comprehensive report on monitoring and improvement plans for the departments. The issues conveyed in the banks internal Incident Management Reporting System, Compliance Department, Internal Audit Department with another set of report to External Auditor and regulator, is to ensure supervisory expectations on Banking and Financial Institution's operational risk management outline and foundation for the Bank's superintendent assessment. Subsequently, the Operational Risk Officer must handover the matter to Executive Risk Management Committee (ERMC) for considerations. ERMC is a monthly Risk Management Meeting chaired by Chief Executive Officer, Chief Risk Officer (CRO), Chief Operating Officer (COO), with senior managements of the organisation. The reporting is necessary due to the operational loss and reputational risk issues faced by the organisation. This is also to create awareness to address, top of the incident management and new improvement plans for the organisation for better operational risk mitigation plan. Moreover, the Basel III trend could also be observed in Malaysian Banking and Financial Institutions, as Malaysia being a

member of the World Bank, International Monetary Fund (IMF) and follows all BIS regulations. Hence the Basel III is strictly implemented in Malaysia. All these regulatory measures not only reduce the losses and Bank's failures but also increases the confidence in banking services. A healthy banking system will help the nation in terms of economy, policy and development.

Acknowledgement

The author research titled Robust Comparisons of the Operational Risk of Malaysian Banks (Islamic and Conventional) and this journal was supported by MyBrain15, which is a program introduced by the Malaysian Ministry of Higher Education (MOHE) which finances postgraduate student's education. Portions of this study was presented in abstract form at the 9th Social Sciences Postgraduate International Seminar (SSPIS2017), University Science of Malaysia, Penang, Malaysia on the 29th of November 2017.

References

Basel Committee on Banking Supervision (BCBS), 2015. Guidelines on Corporate Governance Principles for Banks. [pdf] Basel, Switzerland, Bank for International Settlements. [online] Available at: < https://www.bis.org/publ/bcbs294.pdf> [Accessed 1st November 2017]

Datuk Muhammad Ibrahim, 2016. A Grim Reminder by Bank Negara, Global Islamic Finance Forum 5.0 (GIIF 5.0): Key note address by Governor, Central Bank of Malaysia on 11th May 2016, Sasana Kijang, Kuala Lumpur.

Federal Deposits Insurance Corporations (FDIC), 2017. Failed Bank List. [online] Available at: < https://www.fdic.gov/bank/individual/failed/banklist.html> [Accessed 10th August 2017]

Frank Jordansgregory Kayz, 2011. Rogue Trader Suspected in $2 Billion Loss at UBS. Oklahoma, United States of America, NewsOK [online] Available at: < http://newsok.com/article/feed/296444> [Accessed 28th October 2017]

Sam Gustin, 2012. 'Whale' Fail: JPMorgan's $2 Billion Blunder Tied to London Trader. New York, United States of America, Time Inc. [online] Available at: < http://business.time.com/2012/05/11/whale-fail-jp-morgans-2-billion-derivates-blunder-tied-to-mysterious-london-trader/> [Accessed 15th October 2017]

Sam Jones, 2017.Global Alert to Prepare for Fresh Cyber Attacks. London, United Kingdom, The Financial Times [online] Available at: <https://www.ft.com/content/bb4dda38-389f-11e7-821a-6027b8a20f23> [Accessed 10th November 2017]

Saul Perez, 2014. Why the Basel Committee on Banking Supervision came to be. Global Regulations: Making Banking and Economies Safer Across the World. [online] Available at: <http://marketrealist.com/2014/09/overview-basel-committee-banking-supervision-came/> [Accessed 25th September 2017]

Serajul Quadir, 2016. Bangladesh Bank Exposed to Hackers by Cheap Switches, No Firewall. United States of America, Thomson Reuters [online] Available at: < https://www.reuters.com/article/us-usa-fed-bangladesh/bangladesh-bank-exposed-to-hackers-by-cheap-switches-no-firewall-police-idUSKCN0XI1UO> [Accessed 23rd September 2017]