The Challenges of Information Risk Management (IRM) in the Gaborone Commercial Banking Sector

D. R. Sakia¹ and R. M. Sakia²*

¹ AIM Group, Tanzania
² University of Botswana, Botswana

Abstract

The purpose of this paper is to study the information risk controls in the Gaborone (Botswana) retail banking industry. This entails investigating information security measures, their implementation and effectiveness, as well as the challenges faced in implementing such measures. Apart from looking specifically into the retail banking sector, information security is assessed from the management standpoint. Hence, this study offers insight into the non-technological side of Information Risk Management. While most other studies look solely at the effectiveness of information security by looking at design and implementation of single organizational security measures, this research attempts to look at the effectiveness of these controls, or lack thereof, in relation to the external stakeholders, namely, the consumer and other stakeholders that are often overlooked in similar researches. It was found that IRM practices are streamlined into the banking practices. Internal Risk controls are moderately satisfactory and most recorded security incidents are external. A standard IRM policy is in place in Gaborone Commercial Banking sector but an effective implementation framework is what is lacking.

Keywords: Information, Risk, Information Risk, Information Security

1. Introduction

Information, in whatever form, is a valuable asset to any organization just as any other resource and could be viewed as the ‘currency’ of the modern organization, as Smith (2010) put it. It is the basis on which daily organizational tasks are performed, as well as the basis for strategic decisions. Information risk is inherent in organizations that require information (and the exchange of information) for their operations. In essence information risk is inherent to every organization. Information Risk Management adapts the generic process of risk management and applies it to the integrity, availability and confidentiality of information assets and the information environment (Queensland Government Information Risk Management, 2001).

The process involves identifying, analyzing, assessing, treating and monitoring risk in all areas of agency operations and business¹; in essence, managing the mitigation of risk. This is done to reduce the probability of occurrence or impact of an event upon occurrence of risks. These risks include security threats from malware and data breaches. Fundamentally, they stem from failure to implement standards or best practices (Blakely et al., 2002). The rapid growth of technology simultaneously causes an influx in these security threats as businesses face a constant barrage of threats to proprietary information such as information breach by hacking or exposure caused by dishonest employees. Apart from satisfying legal and regulatory requirements, businesses effectively
identify and prioritize risks as a precursor to developing risk mitigation strategies. This mitigation of risk is particularly important in a business that requires a secure business environment to effectively operate, compete and ensure business continuity.

It, therefore, goes without saying that the managing of confidentiality of private information is at the heart of all banking operations. Such an industry needs its data to be available at all times, strictly confidential and of high integrity. Compromising the security of the banks’ information increases exposure to risks of information loss or fraud, and may damage its operations, and even its reputation and goodwill. Risk management attempts to actively reduce the likelihood of such risks occurring and provides a framework for decisions to be made on where and how to invest in the banks’ private assets. The discipline therefore entails implementation and maintenance of appropriate management controls including policies, procedures and practices to reduce the effects of such risk to an acceptable level\(^1\). It is also concerned with the timely availing of correct information to internal parties that require it. Information risk in itself is not entirely bad, as it is often essential for progress (Smith, 2010), and so the principles of risk management can be directed both to limiting adverse outcomes and achieving desirable ones as a basis to drive improvement (Blakely, 2002).

Due to the relaxed enforcement of controls and laws, information risk is particularly widespread in banking industries of the African continent as opposed to the first world. The Botswana Banking sector is a vital part of the economy, as a collective entity and in terms of the support it gives to the development of other sectors and so it is currently heavily regulated and supervised by the Bank of Botswana (B.O.B). As the banking sector has grown in importance, scrutiny of the sector has become more intense and so have the challenges for the sector, with respect to the environment in which the sector operates.

This research collectively focuses on all risk controls in order to identify weaknesses, gaps and progress in managing risks in the banking sector under the following areas;

- Information Risk Management policy
- Data Privacy
- Records Management

It is also aimed at assessing the risk measures in place in the local retail banks in Gaborone to address various industry risks. Such risks are:

a. Risk to information availability
b. Risk to Information Integrity
c. Risk to Information Confidentiality
d. Risks to the logical and physical environment

The bank’s data privacy standards will also be assessed. On a broader scope, this research aims to investigate their data management practices and the challenges collectively or individually faced by the banks in trying to adhere to such practices. In addition, other aspects of information risk management are also covered, such as, the framework for availing and dispensing information internally to different stakeholders.

2. Statement of the Problem

Due to the banks’ confidential ways in information disclosure, very little is made public about the occurrences of negative events that affect banks and their operations, or related consequences. Consequently, the effectiveness of the risk-curbing measures that are in place in the banking industry remains unclear. Past research (Blakely et al., 2002; Nnolim and Steenkamp, 2007) suggests no uniform information (or data) standards exist or are adhered to internationally for the banking industry. A clear and central framework for information standards is not made transparent. Further, consumers are never directly addressed in similar studies that have been carried out, though all risk management procedures are done with consumers being the focus. Related to the problem statement are subsequent research questions that draw from aspects of the problem. The main question that will be addressed in this research is whether a standard information security framework improved the effectiveness of information risk management for Banks.
3. Scope of the Study

The main purpose of this research is to investigate and draw conclusions on information security practices under the Gaborone retail banking industry. Only the commercial banking sector will be considered as retail banks in Gaborone will be used for the study, which are: FNBB, Barclays PLC, Standard Chartered Bank, Stanbic Bank and new smaller commercial banks such as Banc ABC, Bank of Baroda and Capital bank. The reason for the sample is that they collectively account for about 90% of total banking assets in the industry (Botswana Financial Sector Overview, 2011), hence, results obtained will be representative of the banking industry. The research will attempt to uncover the information risk management framework in place and the level at which information security is at in the industry. In addition to the aforementioned banks being used as primary research participants, the Central Bank (BOB) would be a secondary research participant, as it is the sole regulator of banking services in Botswana. Limited research participants are considered so as to obtain detailed results from the professionals in the field. Due to the sensitive nature of the industry that the research focuses on, the study may be limited in depth and substance. Two hypotheses of interest are:

H1: Frequent review of information risk policy reduces occurrence of security incidents.

H2: Introduction of newer information security technology does not limit information risk

4. Literature Review

The management of information risk is an essential activity, illustrated by some highlights from a recent Dynamic Markets research (Smith, 2010):

− Fifty-five per cent of staff store work-related files such as e-mails and files in locations other than a shared drive.

− One in six employees lies to cover up mistakes caused by using the wrong version of a document and 63% of employees say incorrect information has resulted in negative consequences.

4.1 Trends in Information Risk

A recent survey of corporate risk professionals (Smith, 2010) revealed the growing concern regarding the continued neglect of the value of business information. From financial markets to public services, a range of opinion was sought on the impact of the global recession and what this would mean for risk management, particularly positive risk-taking within sectors. A sample of risk professionals highlighted that the decline in positive risk-taking had been evident since 2008. Fewer than 25% of risk officers sampled stated that individual organizations were prepared to consider risk-taking in a tough economic environment. These findings contrast with research into success psychology that states that organizations should be willing to innovate just as much during a recession as during prosperous times (Smith 2010). Robin (2010) advised that Information professionals who are seeking to introduce improvement techniques should consider corporate attitudes to innovation in order to harmonize new initiatives with strategic plans. This will avoid clashing with corporate planners who are seeking to avoid and reduce risk-taking at certain times.

4.2 The range of Information Risk

As per Robin (2010), information risk can be classified in accordance with a simple taxonomy, allowing information professionals to tag different types of risks for ease of reference. The following taxonomy for information risks was proposed:

Strategic: This type of information risk relates to risks and threats to the strategic position of an organization, including economic and legal threats and risks. For example, updates to legal compliance required by the introduction of new laws in relation to flexible working for staff present a strategic planning risk for an organization that is not able to adapt to new statutory requirements.

Operational: These relate to risks and threats impacting the operation of an organization including staff skills shortages which might demand significant investment at a time when finances are limited.

Financial: Economic and capital threats are of primary concern and will include loss of earnings, limited finances, fines or other related financial issues. A specific financial risk is the level of capital available for investment. If there is no
capital available then there is a limit to the research and development possible to develop new products to secure an organization’s commercial position.

On the part of employees, Nnolim and Steenkamp (2007) identify three safeguard standards that must be met by organizations, namely; administrative safeguards, physical safeguards, and technical safeguards. The focus of these requirements is mostly improvement of corporate governance, that is, corporate accountability and responsibility of officers of the organization.

They noted that human factors have always had some impact on information security programs in organizations. Besnard and Arief (2004) used a multi-disciplinary approach to investigate some of the human factors in computer security. For example, a legitimate user may devise workarounds if the security control measure that has recently been installed cannot provide good usability to the user. In some cases, legitimate users could unknowingly facilitate attacks from outside the organization. Ultimately, end user responsibility is a key component to improving user behavior in information security (Nnolim and Steenkamp 2007). Stakeholder involvement is an important component of Information Risk Management. Tsohou et al., (2006) examined the potential use of cultural theory as a tool for identifying patterns in stakeholders’ perception of risk, and its effect on information system risk management. They maintain that awareness and training are not the only social factors that influence stakeholders’ perception on security threats. (Tsohou et al., 2006, p.198). The fundamental principle of cultural theory is that the way people socially interact encroaches on the systems of symbols they use to understand the world. The study uses this theory, as a foundation framework, to associate social context with information security risks and security management practices (Tsohou et al., 2006, p.207).

4.3 Proposed Frameworks

– A basic IRM model outlined by Robin (2010) suggests that scanning, assessment and development are the critical steps within IRM, forming a cycle of activity for information professionals. By linking these steps, an integrated IRM framework can be developed which can provide a number of products for an organization, from a corporate risk and threat assessment to policies and action plans for improvement. Current practice often leads to intelligence gathered from scanning not being integrated into policies and action plans at the development stage. Using this approach to integration IRM can be positioned as a strategic process that governs the management of information risk from initial identification to final resolution and performance reporting. Positioning IRM strategies within an organization can determine the success or failure of a risk initiative (Robin 2010).

International Standards Organization/International Electro-technical Commission (ISO/IEC) 17799 (2000) provides procedures and code of practice for information security management in the organization. It outlines a general framework that provides a common basis for developing enterprise security standards and effective security management practices (Nnolim and Steenkamp, 2007). Other independent organizations that may be relevant to information security management include British Standards Institution (BS), Committee of Sponsoring Organizations (COSO) of the Treadway Commission, and International Federation for Information Processing (IFIP) Technical Committee 11.

– Eloff and Eloff (2003) proposed that organizations use a holistic approach to information security management, and establish an information security management system. This system would integrate policies, standards, guidelines, code-of-practice, technology, human issues, legal, and ethical issues. This means using a ‘process’ model approach to manage information security. Nnolim and Steenkamp (2007) proposed both “process security” and “product security” in information security management. In “process security”, the focus would be on planning and implementing management practices, procedures, and processes to establish and maintain information security (Nnolim and Steenkamp, 2007). In “product security”, the focus would be on the use of certified software products in the IT infrastructure in order to establish and maintain information security (Eloff and Eloff, 2003).

– Doherty and Fulford (2006) discussed the aligning of information security policy with
strategic information systems plan (SISP). This notion of aligning information security policy with corporate policy strategy could be better in the long run. The argument in support of aligning information security policy with SISP is that it would provide a framework to ensure that systems are developed with security built-in (Nnolim and Steenkamp, 2007). However, if information security policy is aligned with corporate policy, the same systems development objective could still be accomplished (Nnolim and Steenkamp, 2007)

Botha and Von Solms (2004) presented a theoretical model of business continuity planning methodology that could be generally applied to most businesses, as part of an information security management strategy. Out of the three information security fundamental principles of confidentiality, integrity and availability, this study maintains that availability tends to assume greater importance than the other two principles in business continuity planning. However, as (Nnolim and Steenkamp, 2007) cautioned, before most organizations can use this methodology they would need to first identify their specific organizational properties as these properties become variables in the organization’s business continuity plan.

4.4 Risk

Risk is inherent in the everyday operations of a business. Blakely et al., (2002) defines ‘risk’ in business terms, as the possibility of an event which would reduce the value of the business were it to occur. Such an event is called an "adverse event." Risk has been called the element that gives the trust dilemma its basic character (Johnson-George and Swap, 1982). That is, if there was no risk and actions could be taken with complete certainty, no trust would be needed (Yousafzai et al., 2003). Hence, behind every risk is an associated cost, and as Blakely et al., (2002) suggested, the risk can, in most instances, be precisely quantified.

Measurement of Risk

A common measure of the cost of risk is "Annualized Loss Expectation," or ALE (Blakely et al., 2002). As Blakely et al., (2002) explained with illustration, ALE is the expected cumulative cost of risk over a period of one year as estimated in advance. For example, an IT company estimates the probability of one of its data centers crashing during the year 2001 as one in a million. If a crash occurs, it will cost the company 150 million dollars in direct and indirect expenses, (for example, repair costs, legal costs, or lost business). The ALE created by the risk of a data center crash for the year 2001 is simply: ALE = $150,000,000 x (1/1,000,000) = $150

Blakely et al., (2002) did, however, make it clear that the actual cost of this risk will never be that of the ALE, that is, it will never be $150 during a particular year - it will be either $0 or $150 million.

Managing Risk

Blakely et al., (2002) states a variety of techniques to manage risk including:

Liability transfer: Liability for an adverse event can be transferred to another party, thus taking the risk off the business’s books. Liability can be transferred in two ways: by disclaimer and by agreement. A business disclaims liability when it undertakes an activity with the explicit understanding that it will not be held responsible for the consequences of certain adverse events, but without specifying who will be responsible for those consequences. By entering into an agreement; the business must engage in an activity with counter-party after they both agree that the counterparty will be responsible for the consequences of certain adverse events (Blakely et al., 2002).

Mitigation: Another way of reducing risk entails reducing the consequences that follow, if the risk occurs. Consequences can be reduced by reducing the damage the event may cause by accelerating detection and recovery. As Blakely et al., (2002) stated, this may mean redesigning systems/processes that are known to create the adverse event or shorten the time during which the event causes damage.

Indemnification: A business can indemnify itself by hedging or pooling. In pooling schemes, businesses collectively share the costs of some risks. This decreases the cost of risk for each business while increasing the predictability of the cost of risk to each organization in the pool. Insurance policies are the most common type of risk-pooling schemes. In hedging schemes, as
Blakely et al., (2002) explained, a business essentially bets on the occurrence of an adverse event and receives or pays off bettors accordingly, depending on the outcome. The business uses its winnings to settle the costs of the adverse event. Businesses make money off hedging like how casinos make money off card games. Options are the best examples of hedging schemes.

Retention: As Blakely et al., (2002) explained, if the benefits to be realized for taking a risk are great, a business may choose to retain the risk which the adverse event creates. The business may or may not set aside funds to offset the cost of the retained risk.

Gerber, et.al (2001) attempted to determine the importance of risk analysis in identifying security controls, and whether there are other alternative approaches to risk analysis for accomplishing similar goals. They identified several factors that influence an organization’s security requirements. These are:

a. Business requirements for confidentiality and integrity
b. Legal, statutory, or regulatory requirements
c. Risks to the infrastructure.

They argue that if the security requirements analysis determines the appropriate security controls, then this alternative analysis is called “security requirements analysis”.

4.5 Benefits in Improved Information Risk Management

Robin (2010) outlined the following as benefits accruing from improved IRM:

Integration with corporate strategy development: Scanning for external information risks can help corporate strategists to develop agile and responsive programs that are future-proofed (Robin 2010).

Reduced operating costs: By reducing duplication and the ongoing retention of orphan records through improved information risk scanning, an organization can make substantial progress.

Improved communication and collaboration: Better quality information can be shared and re-used by staff with confidence to improve networking and collaboration.

Proactive planning: Responding to information risk is reactive. Better planning can place information professionals in a position to have full view of upcoming risks and threats. As Robin (2010) noted, IRM provides both the necessary tools and supporting techniques to manage the value of business information and in turn create business intelligence.

5. Methodology

This research was aimed at ascertaining the level of information risk in the banking sector, so it was appropriate that only the major retail banks in Gaborone were chosen as research participants in this study. For purposes of this study, Barclays, FNBB, Standard Chartered, Bank ABC, Bank of Baroda, Bank of Gaborone, Capital Bank and Bank of Botswana were included in the survey. Respondents selected from these institutions were those informed persons directly or indirectly associated with the information risk management division of the banks. For time and economic considerations, a total of ten respondents represented the sample.

6. Results

Data collected for this research was insightful and so the starting of this analysis pertains to the response rate. For the purpose of the research, 10 questionnaires were distributed. The response rate from the questionnaires distributed is summarized in Table 1.

Though the total response rate was 90%, all the banks in the sample participated in the research. Only one questionnaire was not received; the Barclays Chief information officer could not be reached for the research.

Table 2 summarizes the research participants’ job position. As seen on the table, the respondents’ organizational role varied depending on who was the official responsible for information risk management in the bank. The more common respondent was the Information officer, constituting 44.4% of the total respondents. The other respondent roles vary from data privacy manager, internal audit manager and communications officer all having 1 respondent each (11%).
Table 1
Organization and respondents’ professional details

<table>
<thead>
<tr>
<th>Institution</th>
<th>Role of respondents</th>
<th>Response tally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barclays Bank Botswana</td>
<td>Logical access &amp; Data privacy managers X1</td>
<td>1/2</td>
</tr>
<tr>
<td>Standard Chartered Bank Botswana</td>
<td>Chief information officer X1</td>
<td>2/2</td>
</tr>
<tr>
<td></td>
<td>IT officers X1</td>
<td></td>
</tr>
<tr>
<td>FNB Botswana</td>
<td>Communications Administrator</td>
<td>1/1</td>
</tr>
<tr>
<td>Stanbic Bank Botswana</td>
<td>Operational risk manager</td>
<td>1/1</td>
</tr>
<tr>
<td>Bank ABC</td>
<td>Country internal audit manager</td>
<td>1/1</td>
</tr>
<tr>
<td>Capital bank</td>
<td>IT officer</td>
<td>1/1</td>
</tr>
<tr>
<td>Bank Gaborone</td>
<td>IT officer</td>
<td>1/1</td>
</tr>
<tr>
<td>Bank of Baroda</td>
<td>IT officer</td>
<td>1/1</td>
</tr>
<tr>
<td>Response rate</td>
<td>9/10≈ 90%</td>
<td></td>
</tr>
</tbody>
</table>

Table 2
Respondent job position

<table>
<thead>
<tr>
<th>Job position</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information officer</td>
<td>4</td>
<td>44.4%</td>
</tr>
<tr>
<td>Communications officer</td>
<td>1</td>
<td>11.1%</td>
</tr>
<tr>
<td>Internal audit manager</td>
<td>1</td>
<td>11.1%</td>
</tr>
<tr>
<td>Operational risk manager</td>
<td>1</td>
<td>11.1%</td>
</tr>
<tr>
<td>Data privacy manager</td>
<td>1</td>
<td>11.1%</td>
</tr>
<tr>
<td>Chief information officer</td>
<td>1</td>
<td>11.1%</td>
</tr>
<tr>
<td>Total</td>
<td>9</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

From Figure 1, none of the banks recorded zero security incidents over the past year. Three out of 9 respondents recorded between 1 and 5 security incidents. One bank recorded between 6 to 10 security incidents over the past year. The majority of respondents, 5 out of the 9, highlighted that the most number of recorded security incidents in the past year ranged between 10 and greater ‘>10’.

As shown in Figure 3, the most common method of assessing the effectiveness of risk controls is by measuring the exposure to risk, 100% of the respondents noted this (9 out of 9). The second most common risk assessment method is by performing continuous walk through tests; 78% of the respondents noted this (7 out of 9). The third most common method is by measuring associated risk exposure; 56% of the respondents noted this (5 out 9). The least common method is performance measurement; 22% of the respondents noted this (2 out of 9).

Table 3 shows Information risk Policy review periods against the Number of security incidents. 4 Banks (44% of respondents) with a Quarterly
The policy review period (4 times a year) recorded between 1 and 5 security incidents. 1 Bank (12% of respondents) with an Annual review period for risk policy recorded between 6 and 10 incidents.

The majority of the Banks, 4 out of 9 (44 % of respondents) with an annual review period recorded 10 or more security incidents over the past year. Only one bank had a policy review period of 2 years, and it recorded more than 10 security incidents over the past year.

Table 3
Frequency of review versus security incidents cross-tabulation

<table>
<thead>
<tr>
<th>Security Incidents</th>
<th>1-5</th>
<th>6-10</th>
<th>&gt;10</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Years Count</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>%</td>
<td>0%</td>
<td>12%</td>
<td>12%</td>
<td></td>
</tr>
<tr>
<td>Annually Count</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>%</td>
<td>0%</td>
<td>12%</td>
<td>32%</td>
<td>44%</td>
</tr>
<tr>
<td>Quarterly Count</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>%</td>
<td>44%</td>
<td>0%</td>
<td>0%</td>
<td>44%</td>
</tr>
<tr>
<td>Total Count</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>%</td>
<td>44%</td>
<td>12%</td>
<td>44%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Table 4
Chi Square test

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
<th>df</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>9.563</td>
<td>4</td>
<td>.048</td>
</tr>
<tr>
<td>Likelihood Ratio</td>
<td>12.871</td>
<td>4</td>
<td>.012</td>
</tr>
<tr>
<td>Linear-by-Linear Association</td>
<td>7.010</td>
<td>1</td>
<td>.008</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4 gives the results for testing the hypothesis that there is no association between policy review periods and number of security incidents.

From the chi square test, the p-value is equal to 0.048 which is less than a 0.05 significance level. Generally, the null hypothesis is rejected when the p-value is less than the significance level. This leads to a conclusion that there is an association between policy review periods and number of security incidents.

Figure 4 shows the response to whether the introduction of newer security technology has seen the reduction of security incidences and associated costs. As seen, 100 % (9 out of 9) of the respondents reported that occurrences of risk incidences and associated costs have indeed reduced security incidences. The hypothesis that introduction of newer information security technology does not affect security level is not supported by these results. Indeed, newer information security technology does limit information risk.
Figure 4: Occurrence of Security incidences and associated costs

Figure 5 shows that 6 out of 9 banks (67% of sample) report that the most common type of incident to occur in the banks was external incidents such as credit card cloning, identity theft and litigation. Internal incidents such as information misappropriation, network failure and malware threats are less common to the banks, with 3 out of 9 banks (33% of sample) reporting this type of incident. This would lead one to infer that local banks focus more of their efforts on curbing the occurrence of external incidents than internal incidents.

Figure 5: Most common type of security incident

7. Discussion

Information Risk Management is vital to a bank’s operation, all the banks follow an information risk standard, in addition to the central bank information standards, most follow international banking best practice standards. Only few banks, however, follow an internationally recognized framework such as Sarbanes-Oxley Act in addition to the aforementioned standards. As per Mr. Baatholeng of the Banking supervision department at Central bank, whom I interviewed, with regard to central bank standards and a central data security Framework; all banks are required to have robust data management systems. These should include the use of appropriate IT software systems; operation of these IT systems in a secure and safe environment; and routine audit of the IT systems to ensure that their security is intact, and that where necessary, passwords and other IT access devices are changed frequently to minimize potential for fraud or IT security intrusion. The standards for information technology should be put down in writing and signed for by both the bank and IT companies that provide the operating and security software.

Further, banks abide by best international standards in data privacy; employing new security technology reduces the likelihood of risk incidences and associated cost. IT is a critical component of the bank’s operations, therefore, it is mandatory that banks have IT policies, which should be reviewed regularly, and as and when the IT environment changes. There is an association between the frequency of policy review and risk occurrences; more frequent policy review periods are likely to increase data security and reduce the occurrence of risk incidences.

With regard to the respondent roles, it was found that the roles of officials in charge of information risk vary, that is, it is not exclusively confined to a specific type of post, such as information risk manager. There are related roles such as information officer and data privacy manager, and then there are unrelated roles such as internal audit manager and communications officer. There is no standardized post such as information risk manager. The majority of qualifications of information risk personnel were either entry level IT qualifications, or on-the-job (internal) training provided by the bank they are employed in. Only a minority of the respondents possessed a formal recognized certification that is pertinent to information risk; certification in risk and information systems.

The survey revealed that all information risks (Risk to Information availability; Risk to Information Integrity; Risk to Information Confidentiality; Risk to customer confidence loss) hold the same importance and high consideration to local
Banks. The risk controls in place in Gaborone banks are considered effective. External incidents such as identity theft and litigation were the most common type of security incidents.

Further, Information Risk Management is streamlined and embedded into daily banking operations. As per the Central Bank official that participated in the research; IRM is a component of daily banking operations, that is why local commercial banks have strict IT access codes, authorization levels, regular audit of IT systems and daily review of reports generated by the IT systems.

8. Conclusions

Information risk management is vital to a bank’s dynamic operations, hence the process of managing information resources starts from the board, when they approve IT policies and ends up with the board periodically requiring audit reports and feedback from top level information officers on the adequacy of the bank’s IT systems. Due to this dynamic banking environment, it is a profession that requires continuous internal and external training to keep knowledge and expertise current with the changing IT environment.

A very daunting issue in the Gaborone banking field that is more than apparent is the level of disclosure, even to the central bank (the regulator) itself. To assess the level of risk, one has to know the threshold of economic loss as a result of risk occurrence, especially in an ever dynamic risk environment. Information of this nature is, however, not disclosed by the local commercial banks themselves, and as a result of this non-disclosure, the field of information risk is made murky. Internal failures and problems continue to be internal only; staying in secrecy and silence will not cure one’s ills so one of the major challenges that the banking industry faces, is that to do with disclosure.

Further, the study explored and revealed that a standard information security framework for the Gaborone commercial banking system is in place, what is lacking is proper implementation; absence of a good IT Policy, poor service level agreements with IT companies, and inadequate staff training on IT information risks hampers the effective implementation and use of recognized information risk standards. The study explored these standards and leads into concluding that IRM is a board level issue. But when information policy is brought down to management for daily implementation, the dissemination framework throughout the organization is not properly set up so active monitoring of risk policy is largely relegated to the ‘IT’ or ‘Risk Department’, and not all internal stakeholders. Hence, getting other stakeholders in the business to actively be involved in the business process of practicing and being generally aware of company policies and procedures pertaining to information risk is the real challenge in the Gaborone banking sector.

9. Recommendations

Information risk management is a profession that needs to have a pool of trained specialized persons. This goes beyond class room and general level training that most of the respondents under this study have. There was no standard certification specific to Information risk, and if any training was given, it was on the job, in house training. It is therefore recommend that all Information risk managers or those in similar position receive mandatory entry level qualification. That is, they should receive accreditation specific to the field to improve their credibility so that they should have a professional obligation to more than just the organization they are employed in. The information risk industry should have licensed professionals that are accountable to a central body that oversees this profession. The dominant presence of obligation is critical.

As per the interview with the central bank official, Banks do not report their economic losses to the regulator. This lack of transparency does not allow for the correct assessment of the counter measures effectiveness. If the losses are not quantified or reported, then the effectiveness of the measures themselves cannot be determined. It is therefore recommend that the commercial banks should be made to regularly quantify and publicly report any losses as a result of information mismanagement.

On the actual information framework and controls in place, it is recommended that an independent body that reports to the regulatory authority (Central Bank) should test and assess the system of controls in place at specified periods. One cannot
fully rely on the opinion and findings of the organization itself on the effectiveness of its system to be sound. This will encourage the banks to keep their system maintained at a higher level.

For the information dissemination framework to significantly improve the organization-wide knowledge of information risk management practices and overall business process, all internal stakeholders should be continuously learning and improving their knowledge on internal information risk practices. It is recommended that Gaborone Banks should have a periodic training, review and certification internal program that is mandatory for all employees. This internal program should be standardized to allow an effective implementation of new information frameworks as this is where the most important challenge lies.

**Acknowledgements**

The authors wish to record their gratitude to the cooperation accorded by the relevant bank employees as well as that of the management.

**References**


