INCIDENT RISK MANAGEMENT: THE CASE OF BANKS IN EAST AND WEST AFRICA

J Marx, Ronald H Mynhardt***

Abstract

An incident is the occurrence of a seemingly minor event, which is important enough that, if not properly managed, can lead to serious consequences. In contrast, a crisis is a stage in a series of events that significantly determines the direction of all future events. Following the much-publicised financial crises around the world, research was conducted amongst banks in East and West Africa to establish whether these banks are actively managing their incidents and crises. The study on which this article is based found that little was being done with regard to managing incidents. It was concluded that banks need assistance to prevent incidents turning into crises. A specific incident management framework is recommended that when implemented could reduce the risk of incidents becoming crises.

Keywords: Banks, Crisis Management, Economic Crisis, Incident Management, Incident Management Framework, Policies, Response Strategies, Risk Management

**Department of Finance, Risk Management and Banking, University of South Africa*
***Department of Finance, Risk Management and Banking, University of South Africa, PO Box 392, Unisa 0003*
Tel: +27 12 429 4927
Fax: +27 86 640 0793
Email: mynhart@unisa.ac.za

Introduction

In the modern economy, the financial system of any country has three major components, namely financial institutions, financial markets and payment systems. These financial systems facilitate the allocation of capital, the management of risks, and also the exchange of goods and services.

There are many potential incidents that could directly or indirectly affect the financial system in a way that could significantly damage the soundness or efficiency of the system (MercoPress 2011). These incidents could threaten the financial system's ability to perform its core functions, dilute public confidence in the system, or reduce the system's toughness. Examples of these incidents are bank failures, a failure of payment and settlement systems, or infrastructure failure such as a general power failure.

Banks play a significant role in the financial system of any country. Bollard (2011) mentions that banks exist because they specialise in assessing the creditworthiness of borrowers and providing an ongoing monitoring function to ensure borrowers meet their obligations. Banks are rewarded for these services by the spread between the rates they offer to the accumulated pool of savers, and the rates they offer to potential borrowers.

Should any incident occur within a bank, the consequences could be far-reaching not only for that particular bank but also for the particular country's economy and even the world economy. Banks are exposed to two types of incidents, namely incidents as a result of internal causes and incidents as a result of external causes. An example of an internal incident is the Barings bank case (Riskglossary, 2010). An example of an external incident is that of North Rock bank, which approached the Bank of England for emergency financial assistance (BBC, 2007).

An incident is therefore defined as the occurrence of a seemingly minor event, yet important enough that, if not properly managed, can lead to serious consequences. In the world of business an incident can be defined as any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to or a reduction in the quality of that service.

In contrast, a crisis is a stage in a series of events that significantly determines the direction of all future events. The North Rock incident is a classic example of an incident turning into a crisis. The news of the incident leaked, and soon afterwards customers started withdrawing deposits because they had apparently lost confidence in that particular bank (BBC, 2007). A further example of an external event causing a crisis for banks is the Subprime crisis (Investopedia, 2007).

The global economic crisis, an external crisis, which started in the United States of America, definitely caused a crisis in African economies (Congressional Research Services, 2009). Through their financial links with other regions in the world, Nigeria, Ghana and Kenya were hit first, suffering

falling equity markets, capital flow reversals, and pressures on exchange rates. Ghana and Kenya had to postpone planned borrowing, and in Nigeria, external financing for corporations and banks became scarce.

The growth rates in these countries also plummeted. Some African countries have consequently experienced negative growth rates. The biggest concern about Africa was that the crisis could turn into a development crisis as it continued and become a major threat to the African continent's poverty reduction goals. In Africa, the attention to financial crises has thus far focused on minimising its impact. A possible answer for African countries to avoid the negative effects of financial crises was to strike a balance between short-tem crisis response strategies and other measures to avoid crises (African Development Bank, 2011).

As a result of the statements made by the African Development Bank (2011), a study was conducted amongst 26 banks in Eastern and Western Africa with the main objective to ascertain by means of questionnaires during interviews whether these banks had the ability to manage financial incidents and financial crises.

The second objective was to use, amongst other, the results obtained from the study to develop an incident management model that, when implemented, could reduce the risk of financial incidents becoming financial crises in banks in East and West Africa.

Research Methodology

The research on which this article is reporting, was aimed at obtaining information about incident and crisis management in banks in East and West Africa.

The banks interviewed in East and West Africa included banks active in countries such as Nigeria, Ghana, Uganda, Kenya and Tanzania. A total of 26 banks (out of a possible 32 banks invited) were interviewed and included Nigerian-, Ghanaian-, Ugandan-, Kenyan- and Tanzanian-owned banks, foreign-owned banks and branches of foreign banks.

The research focused mainly on the following:

- Firstly, a review of the international perspective on crisis/incident management was performed and attention was paid to amongst other current trends in the G10 countries.
- Secondly, incident and crisis management policies, procedures and structures in the banks in the mentioned regions were investigated. To achieve this goal a questionnaire was used in order to identify the types of incident and crisis management policies, procedures and structures that existed in these banks.
- Thirdly, the banks were asked how incident and crisis management policies, procedures and structures in the mentioned banks were being used.

The questionnaire was specifically designed to obtain information pertaining to incident and crisis management policies, procedures and structures in the banks. The questionnaires were completed during personal interviews with the applicable staff of the relevant banks. The interviews conducted were strictly confidential and, at their explicit request, none of the banks or staff members interviewed was named.

The questionnaire consisted of specific questions divided into the following segments:

- crisis management;
- incident management; and
- supplementary information.

The table below provides more detail on the questionnaire used:

Table 1. Content of the questionnaire

Concept tested	Rationale
Crisis management	• Ascertaining whether a crisis management policy exists in the bank and the identification of areas covered by such policy; • identifying the crisis management procedures employed by the banks; • identifying the crisis management structures in the banks; and • identifying the crisis management responsibilities in the banks.
Incident management	• Ascertaining whether an incident management policy exists in the bank and the identification of areas covered by such policy; • identifying the incident management procedures employed by the banks; • identifying the incident management structures in the banks; and • identifying the incident management responsibilities in the banks.
Supplementary information	• Obtaining other relevant supplementary information.

An International Perspective on Incident and Crisis Management

An international perspective on incident and crisis management was researched with the sole purpose of identifying international trends, which could possibly be used in the banks in East and West Africa.

Internationally, it is recognised that having an effective incident management capability is an important part of any bank and any business process (Articleslash 2008). Banks are beginning to realise

that performing incident management activities can prevent incidents from turning into crises. It is realised that the speed with which a bank can recognise, analyse, prevent and respond to an incident will limit the chances of the incident turning into a crisis. Staff, resources and infrastructure are needed to perform the incident management function (Homeland Security, 2008)

There are different ways in which the incident management function is structured. It is, however, recognised that any group responsible for performing incident management actions cannot operate in isolation and that communication and interaction with all appropriate entities is key. It is recommended that an incident management strategy be implemented in the bank that could ensure that all operational units understand their role in the incident management process.

It was also observed that crisis management was receiving increasing attention from organisations around the world (IntraPoint, 2011). Typically, crises have the capacity to produce negative financial, legal, political or governmental repercussions on the company, especially if such crises are not dealt with in a prompt and effective manner. Internationally, crisis management is commonly referred to as a plan of action that is implemented quickly when a negative situation occurs. In addition, a business crisis is defined as a problem that –

- disrupts the way a bank conducts business, and
- attracts significant new media coverage and/or public scrutiny.

It was noted that most business crises occur as one of two types, namely a sudden crisis or a smouldering crisis. A sudden crisis is a disruption in the bank's business that occurs without warning and which is likely to generate newsworthy coverage. Examples of sudden crises include business-related accidents, natural disasters, sudden death or disability of a key person, or workplace violence.

In contrast smouldering crises are defined as any serious business problem that is not generally known within the bank, which may generate negative news coverage if or when it becomes public knowledge and which could result in fines, penalties, legal damage awards, unbudgeted expenses, and other costs (E-notes, 2010).

With regard to incident and crisis management, it was almost unilaterally recommended that all banks have the following in place:

- incident and crisis management policies;
- incident and crisis management procedures;
- incident and crisis management structures, which normally consist of dedicated personnel as well as specific dedicated systems and facilities;
- specific education and training of staff and directors with regard to incident and crisis management;
- ongoing monitoring of incident and crisis-related risks;
- regular reviews of systems and procedures as a preventative measure; and
- investigations following incidents and crises.

The conclusion drawn from this section of the study was that the majority of banks recognised the importance of having policies, procedures and structures with regard to incident and crisis management in place within the bank. However, banks in the different countries were at different levels of development and implementation. No uniform policies, procedures and structures were found and it was observed that banks in a specific country also differed vastly from each other in terms of the development and implementation of the components of incident and crisis management.

Research Findings on Crisis Management

The figure 1 depicts the findings of the study with regard to crisis management as practiced in the banks surveyed.

On the x-axis, Figure 1 shows the types of crisis management actions are present in the banks surveyed in East and West Africa. The number of banks surveyed in East and West Africa to which a particular action is applicable are shown on the y-axis. The values on the y-axis are out of a possible 26, which is the total number of banks surveyed in the region under review.

Although crisis management seemed to be of importance to the banks, only half the banks (13 out of a possible 26 banks) had formal, board-approved crisis management policies and procedures in place. The main reason for this, as furnished by the banks, was that crisis management was on the to-do list but that they had more important areas of focus, which warranted their immediate attention. It was furthermore indicated that physical crises, such as floods, receive more attention than other types of crises including financial crises.

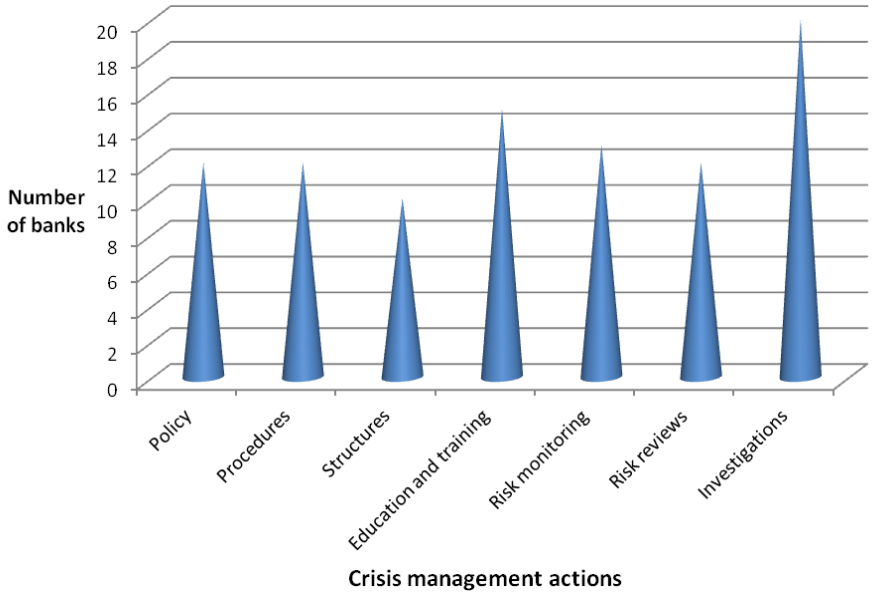
Crisis management structures were observed in less than half the banks surveyed (10 out of a possible 26 banks). The majority of banks indicated that there was no need to implement and maintain specific crisis management structures. Crisis management structures mainly revolved around physical crises such as power outages, fires and damage to infrastructure.

Education and training of staff in terms of what to do in a crisis situation received more attention from the banks (14 out of a possible 26 banks). Again, the banks seemed to focus on physical crises.

Continuous risk monitoring was cited by the banks as being of high importance, and it was remarked that implementation of monitoring procedures was underway at the time of the study. However, just more than half the banks (14 out of a possible 26 banks) have completed this specific task. The main reason provided was a lack of interest in

risk management per se by the top management of the banks as well as in some instances the board of directors of the bank. A number of foreign-owned banks relied on their parent banks to perform the risk monitoring functions on their behalf.

Figure1. Crisis management in East and West African banks



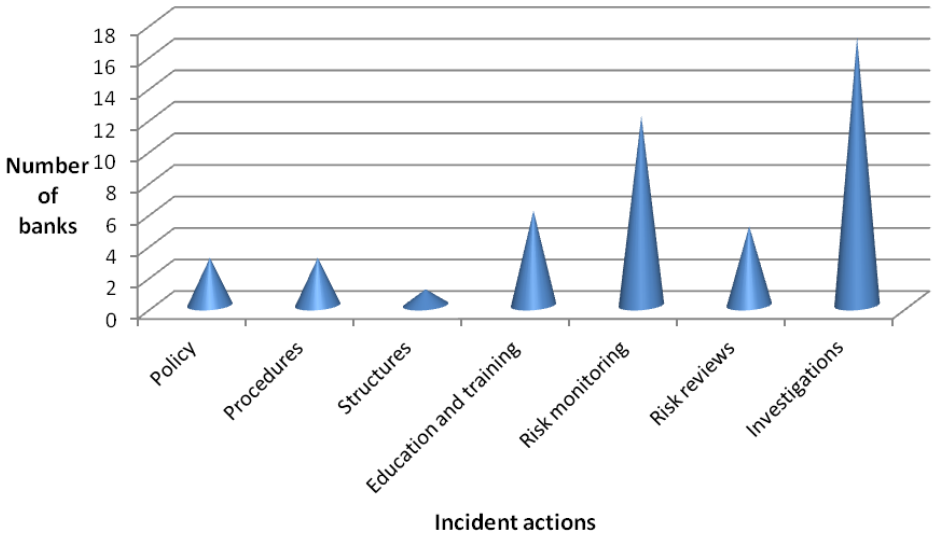
The undertaking of risk reviews was found in 13 banks (out of a possible 26). The banks mentioned that this type of review was mainly the responsibility of the internal or external auditors of the bank. Again, a number of foreign-owned banks relied on their parent banks to perform risk reviews on their behalf.

It was observed that the majority of the banks (19 out of a possible 26) conducted investigations after a crisis had occurred or had been resolved. The banks were unanimous in reporting that their reaction to a crisis was reactive rather than proactive. The investigations mainly centred on finding the reasons for damage caused by and the lessons learned from the crisis. A small number of banks indicated that the results from the investigation were actually used to structure future activities in such a way as to avoid a repeat of the crisis.

Research Findings on Incident Management

The following figure depicts the findings of the study with regard to incident management as practiced in the banks surveyed.

Figure2. Incident management in East and West African banks



In the study, it was found that incident management is even less prominent than crisis management in the banks in East and West Africa. The following are the detailed findings with regard to incident management:

The lack of incident management policies and procedures in the banks was evident in that only two banks (out of a possible 26) had board-approved incident management policies in place. The majority of banks (24 out of a possible 26) in the study reported that official incident management policies were non-existent.

A number of banks indicated that they did however have documented emergency plans to contend with certain types of incidents but that these plans were generally outdated and untested. Some foreign-owned banks mentioned that they relied on the policies of parent banks in this regard. These banks also indicated that they relied on support from the parent banks.

Only one of the banks had a specific structure within the bank to deal with incidents in the bank. The majority of banks indicated that they recognised the need to implement such structures but that it was not a priority to implement and maintain incident management structures. The main reason provided was that top management was not yet convinced of the benefits of incident management.

The banks seemed to focus on certain types of incidents. For these incidents, five banks (out of a possible 26 banks) provided education and training to cope with incidents. These five banks placed emphasis on physical crises such as power outages and fires. Again, the lack of capacity to deal with all types of incidents was evident.

With the lack of interest in incident management, little risk monitoring was evident in the banks with regard to incident management. Only 11 banks (out of a possible 26) reported any monitoring activities. In addition, it was found that even these monitoring activities lacked structure and substance. The monitoring activities were mainly performed on an ad hoc basis.

It was observed that the majority of the banks (16 out of a possible 26) conducted investigations after an incident had occurred. The investigations into incidents centred mainly on finding the reasons for damage caused by and lessons learned from the incident.

Recommendations: Incident Management Policies

The primary responsibilities associated with incident management are to identify and respond to suspected or known security incidents, contain or limit the exposure to loss, and mitigate (to the extent practical) the harmful effects of security incidents.

All the banks taking part in the study can benefit from an incident management policy. These events are rare but can be damaging to a bank if not managed successfully. An effective incident management policy can minimise:

- loss of revenue;
- legal costs;
- damage to products, equipment or premises; and
- damage to brand and reputation.

It is recommended that banks implement an incident management policy and that the following should be addressed in such a policy:

- Purpose of the policy – The purpose of an incident management policy is to define the processes and procedures that will enable the bank to identify and respond to a range of incidents.
- Scope of the policy – The incident management policy should apply, as minimum, to any employee or contractor of or visitor to the bank whilst present in any premises or facility owned, occupied or managed by the bank, or any incident that might happen in the course of, or as a result of, any occupational, educational, commercial or bank-endorsed activity, whatever its location.
- Principles upon which the policy are based – Incident management policies should be based on two principles, namely standardisation and flexibility. Standardisation means that the policies should provide a set of standardised procedures, systems and structures to manage incidents. Standardisation should be applicable to incident prevention, bank wide preparedness, responses to incidents and incident risk mitigation. Flexibility means that the policy should provide a consistent, adjustable and framework that applies to the management of incidents in a bank.
- Roles and responsibilities – The roles and responsibilities of each staff member in the bank should be clearly defined in the incident management policy to ensure effective management of incidents.
- Description of possible incidents – In the incident management policy, the description of possible incidents could contribute to the effective management of incidents. In this regard, the policy should not be a static document but a "living" document subject to changes if and when they are needed.
- Incidents outside the scope of the policy – It is of the utmost importance that the policy be confined to the activities/incidents of the bank. A clear description of incidents not covered by the scope of the policy should be included. This will ensure that there is no confusion amongst staff about actions to be taken when an incident occurs.
- Incident management framework – The bank's incident management policy should provide detailed information on the bank's specific

incident management framework (see framework provided below).

- Reporting requirements – The reporting requirements pertaining to incident management should be incorporated in the incident management policy. Reporting is an integral part of the framework and should provide detailed information on the incident.
- Statutory reporting requirements if applicable – Depending on the type of incident, in some jurisdictions there could be statutory reporting requirements. The incident management policy should detail these specific requirements to ensure that appropriate information be provided to the relevant authorities on a timeous basis.

Other Related Recommendations

The following are other important components of incident management of which a bank should be aware and which they should implement:

- Incident management training

A bank must provide incident management training to its staff members at all levels of the bank, detailing how to identify and report incidents.

- Identifying and prioritising types of incidents

A bank should develop and maintain guidelines for identifying and prioritising incidents. In addition, staff from the bank's risk department should evaluate the potential for the occurrence of certain types of incidents.

- Incident monitoring

A bank should develop and maintain guidelines on how to monitor incidents. As part of their risk management programme, bank staff should continuously monitor for incidents according to the guidelines provided.

- Incident detection

A bank should develop and maintain enterprise-wide procedures for collecting, analysing and reporting data.

- Documentation

All incidents should be thoroughly documented by a bank with as much detail as possible to describe the incident, time discovered and impacted area.

- Record retention

Depending on the type of incident and specific statuary requirements, a bank should maintain the incident documentation for a minimum of one (1) year following the incident.

- Media relations

Serious security incidents that are likely to result in media attention should be handled with care and only authorised staff should be permitted to confront the media.

Recommendations: Incident Management Framework

Incident management capability refers to the ability to provide a bank with tools to manage incidents in such a way that they do not become a crisis. It implies end-to-end management for controlling or directing the way incidents should be handled.

Incident management capability involves defining the process to be followed with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure and tools, and having qualified staff identified and trained to perform the work in a consistent, high-quality and repeatable way.

In order to enable banks to reduce the possible risk of an incident turning into a crisis, the implementation of the incident management framework in Figure 3 below is recommended.

The framework is designed in such a way that an incident, depending on the severity thereof, could be resolved at departmental level in the bank or, in the case of more serious incidents, at top management level. The main purpose of the framework is to prevent an incident turning into a crisis.

There are three role players in the framework, namely the department or division where the incident occurs, the group risk department, and the senior management of the bank. Furthermore, there are two possible paths that management of an incident may follow, namely:

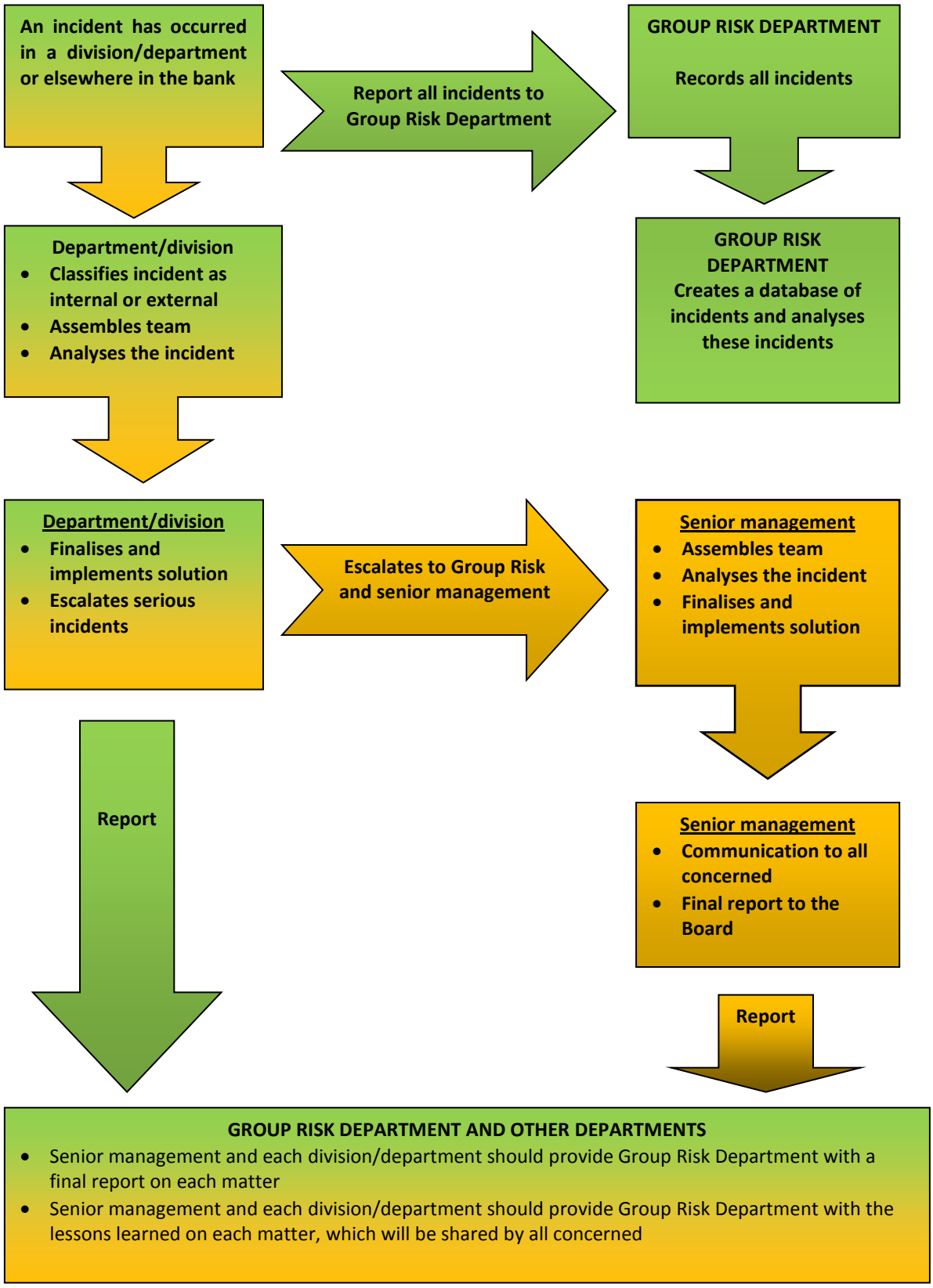
- the path where the incident can be resolved within the department or division itself (shaded orange/green); and
- the path where the incident is resolved at a more senior level in the bank (orange path.)

To illustrate the two possible paths, assume the following two scenarios:

- Scenario one: A computer in the human resources department of the bank has failed and all the personal details of the bank's staff have been lost.
- Scenario two: A morning newspaper article has mentioned that the bank may have liquidity problems due to apparent inability to attract deposits.

In scenario one, the human resources department (HR) will have to report this incident immediately to the group risk department (GR). GR enters the details of the incident into the GR incident data base for further analysis. HR also analyses the incident and classifies it as an internal or external incident. An internal incident is caused by internal influences (such as a malfunctioning drive of a computer) and external incidents by external influences (such a power surge that damaged the computer). In this scenario, the incident could be either internal or external depending on what caused the computer to fail.

Figure 3. Incident management framework



Source: Own composition

HR assembles a team of experts to analyse and to investigate the incident. This team might also include experts from other departments such as the information technology department as might be the case in this scenario. If the incident is successfully resolved and the damage caused by the incident is

contained within HR department, it is reported as such to GR. It is also important that the lessons learned from the incident be reported to GR.

If it is found that the assembled team cannot resolve the incident and that the damage caused by the incident has a bearing on the bank as a whole, the incident should be escalated to GR and senior management. The path now followed is indicated in orange.

In the orange path, GR and senior management now assemble a team at senior management level to resolve the incident. This team resolves the incident and reports the outcome to HR and also eventually to the bank's board of directors. A final report is forwarded to GR. In scenario one, it is unlikely that the orange path will be followed.

In scenario two, the situation is rather more serious than in scenario one. The staff member who notices the article should immediately inform the bank's senior management. Senior management will appoint a senior manager (SM) in the bank who will be responsible for managing the whole incident. The SM will report the incident immediately to the group risk department (GR). GR enters the details of the incident into the GR incident data base for further analysis. SM also analyses the incident and classifies it as an internal or external incident. In scenario two, it is an external incident in that it is an article that appeared in a newspaper.

The SM assembles a team of experts to analyse and investigate the incident. This team might also include experts from other departments such as legal department and treasury department as might be the case in this scenario. The damage caused by the incident could have a bearing on the bank as a whole and the incident should be escalated to the bank's chairperson (MD) or the board of directors. The path now followed is indicated in orange.

In the orange path, the SM and senior management can now add additional members to the team to try and resolve the incident and prevent it from turning into a crisis for the bank. This team resolves the incident and reports the outcome to the MD and also eventually to the bank's board of directors. A final report is forwarded to GR.

Conclusion

Reports have shown that the global economic crisis, which had started in the United States of America, definitely had an influence on and caused a crisis in a number of African countries. Through their financial links with other regions in the world, Nigeria, Ghana and Kenya were the first to feel the crisis when they suffered falling equity markets, capital flow reversals and pressure on exchange rates. As a consequence, Ghana and Kenya had to postpone planned borrowing, and in Nigeria external financing for corporations and banks became scarce. A total number of 26 banks were interviewed during the study being reported here, which included Nigerian-, Ghanaian-, Ugandan-, Kenyan- and Tanzanian-owned banks, foreign-owned banks and branches of foreign banks in these countries.

Other media reports mentioned that in Africa the attention to financial crises has thus far focused on minimising the impact of such crises. A possible answer for African countries to avoid the negative effects of financial crises is to strike a balance between short-tem crisis response strategies and other measures to avoid crises.

Following these reports, research was conducted amongst banks in East and West Africa to establish whether these banks were actively managing their incidents and crises. The subsequent research findings showed that there was evidence that the banks in these African regions were vulnerable to financial incidents. The research also highlighted the absence of incident management policies and frameworks in these banks. The study concluded that the banks needed assistance not only in managing incidents but also in preventing incidents turning into crises.

An international perspective on incident and crisis management was researched with the sole purpose of identifying international trends, which could possibly be used in the banks in East and West African banks.

In order to assist the banks in managing incidents and to prevent incidents turning into crises, this paper proposes specific recommendations with regard to the establishment of incident management policies, other related incident management issues and the implementation of an incident management framework by banks. Some of the issues highlighted include incident management training, incident detection, documentation, records retention and media relations.

The study reported here was limited to banks in East and West Africa but it is possible that banks in other African regions are confronted by the same problem. It will therefore be of value to conduct further research on the topic of incident management in other developing countries.