**ADDIS ABABA UNIVERSITY**

**COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES**

**SCHOOL OF INFORMATION SCIENCE**

# ASSESSMENT OF INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICE IN ETHIOPIAN BANK

By

**TSEDALE YOHANNES**

JUNE, 2018
ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

# ASSESSMENT OF INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICE INETHIOPIAN BANK

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in
Partial Fulfillment of the Requirements for the Degree of
Master of Science in Information Science

By: **TSEDALE YOHANNES**

Advisor: **LEMMA LESSA (PhD)**

June, 2018

Addis Ababa, Ethiopia

# ADDIS ABABA UNIVERSITY

# COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE

# SCHOOL OF INFORMATION SCIENCE

## ASSESSMENT OF INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICE INETHIOPIAN BANK

By: **TSEDALE YOHANNES**

Name and signature of Members of the Examining Board

**LEMMA LESSA (PhD)** ___________ __________
Advisor Signature Date

**GASHAW KEBEDE(PhD)** ___________ ___________
Examiner Signature Date

**WORKSHET LAMENEW(PhD)**__________ ___________
Examiner Signature Date

# Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

I declare that the thesis is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature: _________________________

**TSEDALE YOHANNES**

This thesis has been submitted for examination with my approval as university advisor.

Advisor’s Signature: _________________________

**LEMMA LESSA (PhD)**

# ACKNOWLEDGEMENT

Next to God, I owe my special gratitude to my advisor Dr.Lemma Lessa! Without his assistance and dedicated involvement in every step throughout the process, this paper would have never been accomplished. I would like to thank you very much for your support and understanding. Dr. Lemma, me and my classmates always appreciate your teaching style at classroom. You were punctual, respectful and generous to provide all helpful resources what you have for your students. May God pay you back for your unforgettable extraordinary effort to help your students!

My special thanks also goes to all my teachers at school of information science and the participants of this research at bank x!

Finally, I must express my very profound gratitude to my families, coworkers and friends for providing me with unfailing support and continuous encouragement thorough out my years of study and through the process of researching and writing this thesis. With a special mention to my mother Tsehai.M, my sisters & my brothers, my children Hilary & Michael, Thank you so much for all your support and encouragement!

# Abstract

Banks facilitate spending and investment, which fuel growth in the economy, however, despite their important role in economy, banks are nevertheless susceptible to failure. Banks, like any other business, can go bankrupt. But unlike most other businesses, the failure of banks, especially very large ones, can have far-reaching implications.

Ethiopian Banks continually increase their dependence on IT systems. Bank x is one of the largest banks in Ethiopia. It adopted internationally recognized banking technologies. One of the major technologies is the core banking solution, it also provide banking services such as the ATM, mobile banking, Internet and payment terminals.The advancement of technology and an increasing use of IT solutions exposed banks for attacks more than ever.

Even though, banks are deploying prevention mechanisms to keep out hackers and attempts of cyber-attacks, incidents occuroccasionally. This tells there is a need for an effective and efficient management of information security incidents. International standards and guidelines for incident management exist but,researchesthat assess current practices are few in literature. This research conducted as a qualitative case study in which bank x's information security incident management current practice assessed. Where the data collection methods were face-to-face and E-mail interview.

The finding from this study revealed that bank x does not have a predefined and separate information security incident management plan. But, to some extent it was compliant with international standards and guidelines in some of incident handling procedures. An alarming finding that indicated bank x never performed rehearsal was highlighted in this study. Lack of employee awareness, information gap among departments,and lack of experienced and skilled incident handlers and enhancement of new threats were among prominent challenges identified in this research.Finally, recommendation for successful information security incident management was proposed.

**Keywords**: information security incident, information security incident management, incident response team.

## Contents

## List of Tables

## List of Figures

# List of Acronyms

| | |
|---|---|
| ATM | Automated Teller Machine |
| BC | Business Continuity |
| CERT | Computer Emergency Response Team |
| CIRT | Computer Incident Response Team |
| CSIRT | Computer Security Incident Response Team |
| DMZ | Demilitarized Zone |
| DR | Disaster Recovery |
| ENISA | European Network and Information Security Agency |
| ICT | Information and Communications Technology |
| IDPS | Intrusion Detection and Prevention System |
| IDS | Intrusion Detection System |
| IEC | International Electro technical Commission |
| INSA | Information Network Security Agency |
| IRT | Incident Response Team |
| ISIRT | Information Security Incident Response Team |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| IR | Incident Response |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| NIST | National Institute of Standards and Technology |
| PoC | Point of Contact |
| SANS | South Africa National Standards |
| SIEM | Security Information Event Management |
| SOC | Security Operation Center |
| SP | Special Publication |
| USB | Universal Serial Bus |
| UTM | Unified Threat Management |

# CHAPTER ONE

## INTRODUCTION

This chapter introduces the background of the research, statement of the problem,research questions and the objectives of the research, thesignificance of the study and the scope of the research.Moreover it presents organization of the thesis.

## 1. Background of the Study

Worldwide, businesses continually increase their dependence on IT systems, even for routine business processes. The business processes which directly rely on information systems and the supporting IT infrastructure often require high levels of availability and recovery in the case of an unplanned outage. Industries and governments are becoming increasingly accountable for how data is managed, protected, and secured. Policies and regulations vary from industry to industry, and the overall landscape of technical requirements continues to grow in complexity(Hove.G.&Tarnes.M,2013).

The financial industry traditionally leads in terms of stringent regulations for data protection, security, and contingency copies of financial data; others are quickly migrating towards a completely electronic format for data. Banks facilitate spending and investment, which fuel growth in the economy, however, despite their important role in economy, banks are nevertheless susceptible to failure. Banks, like any other business, can go bankrupt. But unlike most other businesses, the failure of banks, especially very large ones, can have far-reaching implications. As we saw during the great depression and most recently during the global financial crises and the ensuing recession, the health of the bank system can trigger economic calamities affecting millions of people. **(**Temsgen, 2016**)**

Organizations can’t afford to be nonoperational due to regional power outages, cyber-attacks or hardware failures. Every minutes applications and systems are down translates into lost revenue. Like any other organizations, banks are exposed to some kind of risks that can damage their business in different ways and threaten their survival. Therefore, it is vital to develop and implement contingency plans to prevent the risk, to be to recover from disaster and to minimize the damage when the risk occurs as well. Incident response, disaster recovery, and business continuity planning are components of contingency planning (Michael.E.&Herbert.J.,2011).

The discussion of contingency planning begins with an explanation of the differences among its various elements, and an examination of the points at which each element is brought into play. An **incident** is any clearly identified attack on the organization’s information assets that would threaten the assets’ confidentiality, integrity, or availability. An **incident response (IR) plan** addresses the identification, classification, response, and recovery from an incident. A **disaster recovery (DR) plan** addresses the preparation for and recovery from a disaster, whether natural or man-made. A **business continuity (BC) plan** ensures that critical business functions continue (Michael.E.&Herbert.J.,2011)

If a catastrophic incident or disaster occurs, the primary functions of these three types of planning are as follows:

- The IR plan focuses on immediate response, but if the attack escalates or is disastrous (e.g., fire, flood, earthquake, or total blackout) the process moves on to disaster recovery and the BC plan.
- The DR plan typically focuses on restoring systems at the original site after disasters occur, and as such is closely associated with the BC plan.
- The BC plan occurs concurrently with the DR plan when the damage is major or ongoing, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site (Michael.E.&Herbert.J.,2011).

In recent years, an increasing number of information security incidents have been reported. Typical incidents include both general and single purpose attacks caused by malware, in addition to minor errors with severe consequences. Hence, organizations need to be prepared to handle incidents caused by both known and unknown vulnerabilities. Several well established standards and guidelines addressing incident management exist and a number of factors are also involved in determining how successfully organizations respond to information security incidents (Hove.G.&Tarnes.M,2013).

## 2. Statement of the problem and its justification

The 2014 pricewaterhousecoopers Global state of Information Security Survey (2014) claims that the rate of security incidents detected in the past twelve months increased by more than 25% and more than double since 2011. The Kaspersky 2013 Global Corporate IT Security Risks Survey (Kaspersky 2013), estimate that the financial losses from security incidents and data breaches are in the millions of dollars within the past years.

Responding to security incidents is becoming increasingly imperative in business environments. A poneman(2016) study on data breaches reports that 48% of attacks involved malicious activity, 25% were due to negligent human factors, and 27% involved business and information technology process failures. The report goes on to indicate that the mean time to identify an incident is, approximately, 201 days and the mean time to contain an incident once discovered is 70 days. The reality is that the effects of a breach can be very destructive to an organization. This destruction can be experienced in the form or ransom ware, system downtime, intellectual property theft, reducing customer confidence, and facilitating attacks on other organizations (Grispos et al, 2017).

Banks are one of the huge elements that constitute the financial system of Ethiopia. They dominate the Ethiopian financial system with nearly 95% share of assets,97% share of deposits, 94% share of loans and advance, and 77% equity share of the financial sector on average( Nigussie, 2017,p.9). Such a huge financial sector needs to have a structured way to continue business and restore operations in the event of a sudden outage. Like any other organizations, interruptions to information technology system services can have a severe impact on banks and its ability to carry out its basic functions. IT resources are essential to most business processes and organizations depend up on information systems that operate effectively without serious interruptions. (Susan Snedaker, 2007)

An increasing use of digital solutions suggests that organizations today are more exposed to attacks than before. Recent reports show that attacks get more advanced and that attackers choose their targets more wisely. Despite preventive measures being implemented, incidents occur occasionally .This calls for effective and efficient information security incident management (Hove.G.&Tarnes.M.,2013) .

According to Grispos et al( 2014), security incident increasingly impact organizations, it is imperative that organizations have the ability to investigate, report and, ultimately, improve overall security efforts based on previous security incidents.

Several standards and guidelines addressing incident management exist. Using those standards, Hove.G.&Tarnes.M(2013), has studied information security incident management current practice in three Norwegian organizations, the researchers described that: As we have only studied a limited number of organizations, our result is not generalizable and thus it would be interesting to conduct the same study with a larger number of organizations. This can verify whether our findings apply to organizations in general (p.112).

Few student researchers in Ethiopia have tried to study information security in financial industries from different perspectives.Kelime(2013), he proposed information security management framework for banking industries in Ethiopia. Another student,Abeselom(2015), he assessed thatpractice, challenges and prospects of information security policy in Ethiopian banking industries.Recently,Daniel(2017), has tried to study the effectiveness of information security management in Ethiopian financial sectors. His focus was card banking. Onthe other hand, among the elements of contingency plan, BC and DR has got some coverage by local student researchers.Asheber(2017), has tried to identify potential challenges in relation to business continuity management.Negussie(2017), has studied about information technology disaster recovery practices of Ethiopian commercial banks.Whilethe student researchers studied information security, they haven’t discussed information security incident management practicein their research.DR and BC have beenstudied by the student researchers specifically. but the third element of contingency, incident response didn’t get enough attention by the researchers., literature shows that there is lack of local research that address information security incident management practice.

Hove.G&Tarnes.M(2013), also mentioned that few studies of current practices in information security incident management have been conducted. As per the knowledge of the researcher, there is no study which is conducted on information security incident management current practice of Ethiopian Banking Industries. Therefore, this research is intended to study the current information security incident management practice at bank x of Ethiopia.

## 3. Research Questions

How does Bank X of Ethiopia perform information security incident management?

What gaps or challenges exist in information security incident management at bank x of Ethiopia?

## 4. Objective of the study

**The general objective** of this research is to assess the current practice of information security incident management at bank x of Ethiopia using international standard.

**Specific Objectives**

- Identify plans and procedures for information security incident management at bank x of Ethiopia.
- Compare standards/frameworks in literature to select one to compare current practice against
- Identify challenges and successful practices in managing information security incidents at bankx of Ethiopia in relation to the selected international standard.
- Forward recommendation for management to enhance information security incident management at bankx of Ethiopia in the future.

## 5. Significance of the study

The result of this research will be of great benefits to the followings.

**Banks**: the result will provide banks in Ethiopia with detail knowledge how they can perform their information security incident management in line with international standard in order to assure their business continuity.

**Other organizations**: it will also aware other Ethiopian organizations to pay attention in managing information security incidents.

## 6. Scope of the study

Due to time restriction for this research, this study focused on bank x of Ethiopia information security incident management practice. The study doesn't include disaster recovery and business continuity plan though both are components of contingency plan like incident response plan.

## 7. Organization of the Thesis

This research is organized in five chapters. It includes:

Chapter 1: it introduces the background of information security incident management practice in financial sectors especially in banks. Moreover it discusses about business continuity of such sectors by considering contingency plan, IT disaster recovery plan and information security incident response.Thechapter also includes statement of the problem, research questions, and research objectives,significance of the study and scope of the study

Chapter 2: in this chapter, literature about information security management in financial sectors, information security incident management practice, information security incident response team, international standards for information security incident management, similarities among international standards, best practice in information security incident response and related works information system viewed and discussed thoroughly in order to explore the topic.

Chapter 3: this chapter describes the research design and methodology used. Thus, the chapter includes, research design, source of data, sampling technique,datacollection methods, validity, reliability, data analysis.

Chapter 4: in this chapter, the collected data is analyzed, interpreted, described and discussedbased on the significance of the key findings in light of what was already known about theresearch problem.

Chapter 5: this chapter concludes the research and provides recommendations depending up on the findings.

# CHAPTER TWO

## LITRATURE REVIEW

This chapter focuses on the most important concepts that clarify the issue of the research and it discusses the major and widely used international standards and guidelinesfor information security incident management practice.Moreover related works of this research also reviewed in this chapter. The following are among concepts which are discussed here: information security management in financial sectors, overview of information security incident, definitions, information security incidents, information security incident management, information security incident response team, international standards and guidelines for information security incident management (The ISO/IEC 27035 Standard, The ITIL Framework and NIST Special Publication 800-61,ENISA,SANS), similarities among the mentioned international standards and best practice methods of security incident responses.

### 2.1 Information security management in financial sector

Information security management is an ever changing issue. The need for better services and functionality must constantly be supplemented by stronger security measures to counteract the risks. Moreover, these security measures must be highly swift and must be quickly deployed evolve customers trust. To that end, the financial sector should work very hard towards addressing this issue and the top management should play the biggest role to fulfill these needs (Daniel, 2017).

Banks’ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. Having a reputation for safeguarding information and the environment within which it resides enhances an organization’s ability to preserve and increase market share (Ula, et al., 2011). To attain this, management must allocate sufficient resources to carry out day-to-day activities to accomplish both short-term and long-term information safety goals. An effective information security management program needs an appropriate level of resource commitment including sufficient staff, time, money, information, methods used in safety works, facilities, tools, machines, etc.(Aksorn and Hadikusumo,2008).

As Smith and Jamieson (2006) explained, the active support of top management was ranked the most important issue and rated number one in priority survey. While top management is ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources, they can also support information security as an important enterprise-wide function in many ways, including funding, allocation of human and financial resources, promotion of buy-in, and stressing the importance of security to other groups within the organization (Kayworth and Whitten, 2010).

Jassal and Sehgal (2013) also points out that, the unique aspect about information security in banking industry are that the security posture of a bank does not depend solely on the safeguards and practices implemented by the bank; rather it is equally dependent on the awareness of the users. This makes the task for protecting information confidentiality and integrity a greater challenge for the financial sectors. Financial institutions have made, and should continue to make, efforts to educate their customers. Thus, management should implement a customer awareness program and periodically evaluate its effectiveness.

## 2.2 Incident Management Overview

This section provides an overview of common concepts and terms used in incident management.

### 2.2.1 Definitions

In information security incident management there are a few terms that need to be defined clearly. Two such terms are information or computer security incidents and information or computer security events. It is important to recognize these as two terms of different meaning. The standard ISO/IEC 27000 (ISO/IEC: 2012(E)) specifies the following definitions:

**Information security**: Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

**Information security event**: Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

**Information security incident**: Single or a series of unwanted or un-expected information security events that have a significant probability of compromising business operations and threatening information security.

**Information Security Incident Response Team (ISIRT)**: Team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle.

The guidelines NIST Special Publication (SP) 800-61: Computer Security Incident Handling Guide (Paul et.al, 2011) specifies the following definitions:

**Event**: An event is an observable occurrence in a system or network.

**Adverse event**: Adverse events are events with a negative consequence, such as system crashes, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

**Computer security incident**: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

## 2.3. Information security incident management

Incident management is a collective term that comprises all activities associated with managing security incidents. Incident management is not restricted to incident handling alone, but includes activities for the entire incident lifecycle; from planning, training and raising awareness to detecting, responding and learning from incidents.

Various guidelines and standards describe best practice and suggest activities for effective and efficient incident management. It is important to note that incident response requires a substantial amount of planning and resources. Two of the most important parts of incident management are the existence of guidelines for communication and prioritization of incidents as well as the use of an evaluation process to gain experience from previous incidents. (Paul et.al, 2011)

As part of an incident management capability, organizations should have an incident management policy, a plan and procedures, all of which should be tailored to the specific organization's needs. Additionally, it is important to have a planned approach to reporting of vulnerabilities that have not yet been exploited (ISO/IEC 27035:2011(E)).

Incident management is not purely an IT related issue as information security incidents threaten an organization as a whole. Having a well-planned and tailored incident management capability is therefore important for organizations in order to protect information. Incident management seeks to prevent, contain and resolve incidents

## 2.4.Incident Response Team

Having an Incident Response Team (IRT) will aid organizations in responding to incidents more effectively and efficiently, in addition to providing a structured approach for learning from previous incidents.

As the various definitions in section 2.1.1 indicate, an incident response team is  team that responds to computer security incidents by providing all necessary services to solve the problem(s) or to support the resolution of them" (ENISA,2008). The team structure, members, tasks and responsibilities may vary depending on organizations' resources and needs.

NIST recommends having one person in charge of incident response, taking the role as team manager. The team manager should act as a liaison to senior management and ensure that the team has the necessary resources, personnel and skills. It is recommended that team members have diverse backgrounds so they can handle different incidents that occur. The team manager should assess the situation and assign responsibility for incidents to the most appropriate team member (Paul et.al, 2011).

Usually teams consist of highly technically skilled persons, and teams should have at least one member with expertise in each major technological category. Good problem solving skills and communication skills are essential to the team as effective incident response requires collaboration and coordination within the team and throughout the organization (Paul et.al, 2011).

The structure of the team may vary. The number and frequency of incidents as well as team responsibilities should guide organizations' choice of team structure. However, whenever justified the ISO/IEC 27035 standard recommends having a permanent team (ISO/IEC 27035:2011(E)).

Participating in a community of teams will be beneficial for teams due to collaboration on standards and procedures as well as information and resource sharing. To minimize the frequency of incidents and to mitigate negative impact caused by them, most IRTs do not only provide reactive services, but may also have other responsibilities, such as intrusion detection, advisory distribution, education and raising awareness within the organization(Paul et.al,2011).

## 2.5. Standards and Guidelines inrelation to information security incident management

Widely implemented standards and guidelines for information security incident management will be discussed in this section

### 2.5.1 The ISO/IEC 27035 Standard

This section explains what an ISO 27035 standard is and the content is, unless specified otherwise, derived from (ISO/IEC 27035:2011(E)).

Implementing this standard will aid organizations in dealing with information security incidents properly and mitigate both direct and indirect adverse business impact. This standard provides an extensive and structured approach to incident management by presenting five phases with recommended activities for large and medium sized organizations.

One of the standard's objectives is to provide guidelines to aid organizations in meeting the requirements specified in the ISO/IEC 27001 standard.

TheISO/IEC 27035 standard is a supplement to the implementation guidelines relevant to incident management that are presented in the ISO/IEC 27002 standard. This standard represents a code of practice for information security management and establishes guidelines for initiating, implementing, maintaining and improving information security management in an organization. The standard is intended to be a starting point for developing organization specific guidelines and contains 11 security control clauses that out-line various security objectives and provide implementation guidance.

ISO/IEC 27035 divides the incident management process into five phases: 1) plan and prepare; 2) detection and reporting; 3) assessment and decision;4) responses; and 5) lessons learnt.

**Plan and Prepare:** This phase is by far the most extensive phase and involves many activities. Individual organizations have to ensure that their uses of resources are proportional to their needs. Each organization should formulate an incident management policy that reviews current vulnerabilities, states the need for an incident management scheme and identifies benefits for the organization. Security and risk management policies should be reviewed and updated regularly. The standard highlights the importance of ensuring commitment from senior management in the security incident management policy to ensure the organization's commitment to resources and maintenance of an incident management capability.

One of the main activities in the plan and prepare phase is to make a detailed incident management scheme. The scheme should include reporting forms (preferably electronic) and a classification scale for grading incidents.

Another important activity in this phase is the establishment of the Information Security Incident Response Team (ISIRT). Organizations should establish and implement required mechanisms of support for their incident management scheme to operate efficiently during this phase. This includes technical tools such as Intrusion Detection Systems (IDSs) and log monitoring systems as well as relationships and connections to other organizations.

All personnel should be familiar with the incident management scheme, when it becomes operational and be able to recognize its benefits. Users' awareness and participation is essential for the success of a structured incident management approach. It is recommended that an appropriate awareness and training program is developed and repeated regularly as personnel change over time.

The entire incident management scheme should be tested to verify that the scheme and the ISIRT work in complex and real situations. After going through this phase, organizations should be fully prepared to manage security events, incidents and vulnerabilities.

**Detection and Reporting:** The first operational phase of an incident management scheme involves detection, collection of information and reporting of occurrences of security events, incidents and vulnerabilities either discovered by humans or automated systems. It is important to preserve information about vulnerabilities and incidents in a database operated and maintained by the ISIRT. Organizations should implement security monitoring systems, Intrusion Detection System/Intrusion Detection and Prevention (IDS/IPS) and antivirus programs to aid the detection of security events, incidents and vulnerabilities. Logs from various entities should be analyzed and registrations of incidents should be made in an Incident Tracking System.

It is the person first notified about an event that is responsible for starting the activities involved in this phase. There are several ways a security event or incident can be detected and thus all employees should be aware of and have access to the guidelines for reporting. There should be clear procedures to follow for people involved in handling an incident. All relevant information should be passed to the Point of Contact (PoC) and the responsible ISIRT member. It is recommended that one of the ISIRT members is appointed the responsibility for incoming reports and for making assessments about further actions. A reporting form should be specified to ensure that all necessary and relevant information is preserved and that there is consistency in the information gathered.

**Assessment and Decision**:This phase includes assessment of information regarding security events and decisions about whether events should be treated as incidents. The assessment and decision phase also includes assessment of information received regarding vulnerabilities and decisions of how to handle these in accordance with previously agreed actions.

The PoC should use a predefined classification scale to make an assessment of security events, whether they are incidents or false alarms and what impact they may have on the organization's core services, information and affected assets. The initial assessment made by the PoC should be verified by an ISIRT member. The ISIRT makes decisions about how the incident should be handled, by whom and in what priority. To be able to respond to security incidents in an efficient and effective way, a prioritization process should be conducted based on the level of adverse business impact and the required effort to solve them. All information pertaining to an incident should be recorded in the database by the ISIRT. A main activity for the ISIRT is to allocate responsibilities for incident management actions and provide thorough and structured procedures for people involved.

**Responses**: The third operational phase presents guidelines and activities for organizations to use when responding to security incidents. The response should be in accordance with the actions agreed in the previous phase. This phase also involves responding to vulnerabilities reported either internally or by external parties. As a first step, the ISIRT has to deter-mine whether the incident is under control, and then initiate appropriate actions. For situations out of control, escalation to crisis handling might be necessary. Otherwise, response activities including recovery, proper documentation and communication to relevant parties can be started.

The ISIRT should consider which internal and possibly external resources to utilize for optimal incident response. It is important that every action conducted by the ISIRT in this phase is logged properly and that guidelines are used to ensure thorough documentation. Logging will aid in analyzing how effective and efficient the incident response process was as well as ensuring that any possible evidence is not compromised. It is the ISIRT's responsibility to make sure affected assets become operational again and that they are not vulnerable to the same attacks. Once an incident has been handled, the case should be closed formally by the ISIRT and recorded in the database.

**Lessons Learned**: The final phase starts after an incident has been re-solved and/or closed and focuses on analyzing whether the organization's incident management scheme worked successfully. During this phase improvements are identified and implemented. One of the main activities is reviewing how effective the entire incident management process was in responding to, assessing and recovering from the incident. Shortcomings and improvements in policies, procedures, security control implementations, re-porting formats and risk assessments should be identified during this phase. Improvements may be implemented immediately or incorporated into future plans. The ISIRT should make sure improvements are made to the entire system and not only the affected parts.

The lessons learned phase has many iterative activities. An essential post-incident activity is documenting incidents properly as well as ensuring that the incident trend analysis is accurate. Sharing experiences with trusted communities and partners should be done on a regular basis, regardless of whether incidents occur internally. Reviews, trend analysis and testing should be performed frequently to improve the incident management scheme over time.

## 2.5.2. The ITIL Framework

Information Technology Infrastructure Library (ITIL) is a framework and a source of good practice for service management that is aligned with the ISO/IEC 27000 standard (Hove.G&Tarnes.M, 2013). This section gives a brief introduction to the ITIL framework, focusing on the parts related to incident management and the content is, unless specified otherwise, derived from (Ernest et al, 2012). The definitions presented in this section are directly retrieved from (Ernest et al, 2012).

To describe service management, the ITIL framework uses the following definitions:

**Service**: A service is a means of delivering value to customers by facilitating outcomes that customers want to achieve without the ownership of specific costs and risks.

**Service Management**: Service management is a set of specialized organizational capabilities for providing value to customers in the form of services.

The specialized organizational capabilities include the processes, activities, functions and roles that a service provider uses in delivering services. The ITIL framework is generic and is meant to be useful for any type of organization. It describes a set of functions and processes that can be implemented in order to be able to perform service management. The terms function and process are defined in the following ways:

**Function**: A team or group of people and the tools they use to carry out one or more processes or activities.

**Process**: A process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities and work instructions if they are needed.

This section describes processes and functions related to incident management.

**Availability Management**: Availability management is essential for an organization and is primarily a proactive process, In addition to activities such as preparing and maintaining an availability plan and monitoring.

Availability levels, this process includes assisting investigation and resolution of availability related incidents and problems. The latter is a reactive part of availability management. This process is related to other processes including IT service continuity, information security, and event, incident and problem management.

**IT Service Continuity Management**: This process is concerned with key systems in the event of a failure. The purpose of the process is to ensure that IT resources, systems and services can be restored within agreed timescales in the event of a major incident. The process is related to avail-ability and information security management.

**Information Security Management**: This process is concerned with enforcing the security policy. The system in place for this is the ISMS. The security policy in an organization is something everyone should have access to and be aware of. Information security management is related to availability, incident, problem and IT service continuity management.

**The Service Desk**: The service desk is a function. One of the processes the service desk carries out is incident management. The service desk should be the single point of contact for IT users in an organization. This means that if users wish to log incidents or report events they should contact the service desk. The service desk is the owner of incidents throughout their lifecycle, regardless of who is working on the incident. They should be trained to obtain the skills needed in order to perform incident management as effectively and efficiently as possible.

**Incident Management**: This is the process for dealing with incidents. An incident is defined as being an unplanned interruption or reduction in quality of an IT service. An incident can also be the failure of a configuration item that has not yet impacted service. Hence, incident management includes both incidents where service has been disrupted or where service has not yet been disrupted. Each organization should have its own definition of a major incident. Large organizations may havededicated teams available 24/7 to handle major incidents.

In the incident management process resources are allocated to minimize and mitigate the impact of incidents and service unavailability in line with business priorities. The main objectives are to restore service as quickly as possible in addition to limit adverse impact on business operations. Incident handling may reveal areas that are in need of improvement. Organizations can adopt incident models, which are methods for handling groups of similar incidents. If the incident turns out to be major, the major incident process is initiated. The incident handling may also need to be escalated. Functional escalation is when the service desk is not able to resolve the incident or when they have not been able to resolve it within the target resolution time. Hierarchical escalation is when the problem of a specific incident within the IT organization and also within business areas needs to be raised. All incidents need to be investigated and diagnosed in order to subsequently be resolved and closed. The incident management process is closely related to the problem management process.

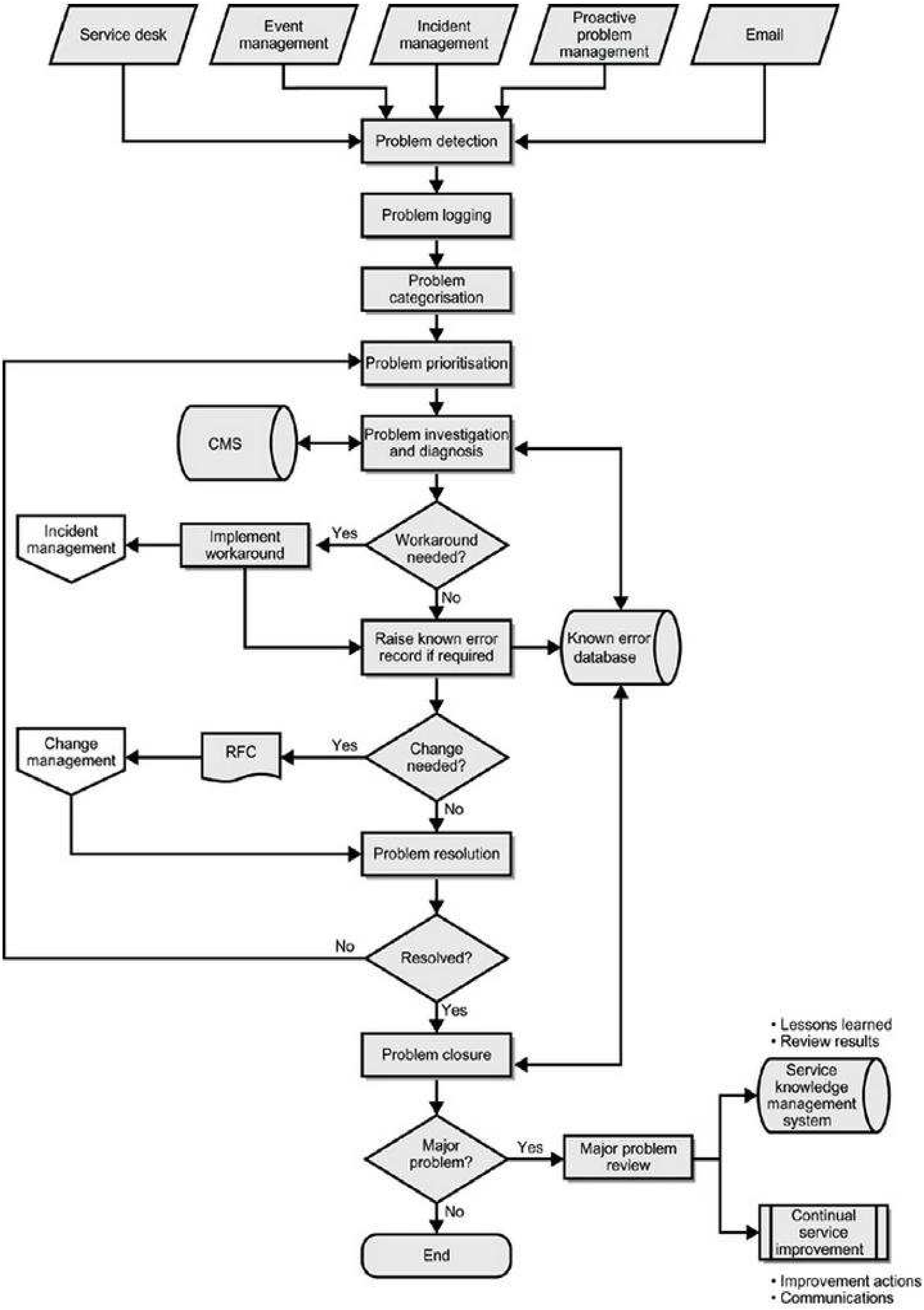


Figure 2.1: Problem Management Process (Ernest et al, 2012)

**Problem Management**: The problem management process concerns analysis of the root cause as well as resolving problems. A problem is defined as being the cause of one or more incidents. The process is both proactive and reactive and seeks to prevent problems and incidents as well as reduce the impact of those that cannot be prevented. The problem management process is illustrated in figure 2.1.The figure shows the various inputs to the process. It is important to log all details of the problem. All problems need to be categorized and prioritized. The problem needs to be resolved as soon as a permanent x is available and subsequently closed. If the problem is major, a major problem review must be conducted.

**Event Management**: The event management process handles normal messages and detects, escalates and reacts to exceptions. An event can be informational, a warning or an exception. The event management process is similar to the incident management process and should ideally be automated. Some events are triggers for the incident management process.

### 2.5.3 NIST Special Publication 800-61

This subsection gives an introduction to the guideline NIST SP 800-61 and the content is, unless specified otherwise, derived from (Paul et.al, 2011). This publication aims to assist organizations in mitigating risks from computer security incidents by providing guidelines on how to respond to incidents effectively and efficiently.

NIST SP 800-61 describes the four phases of incident response; preparation, detection and analysis, containment, eradication and recovery and post-incident activity. The phases and the relationship between them are illustrated in figure.2.2.

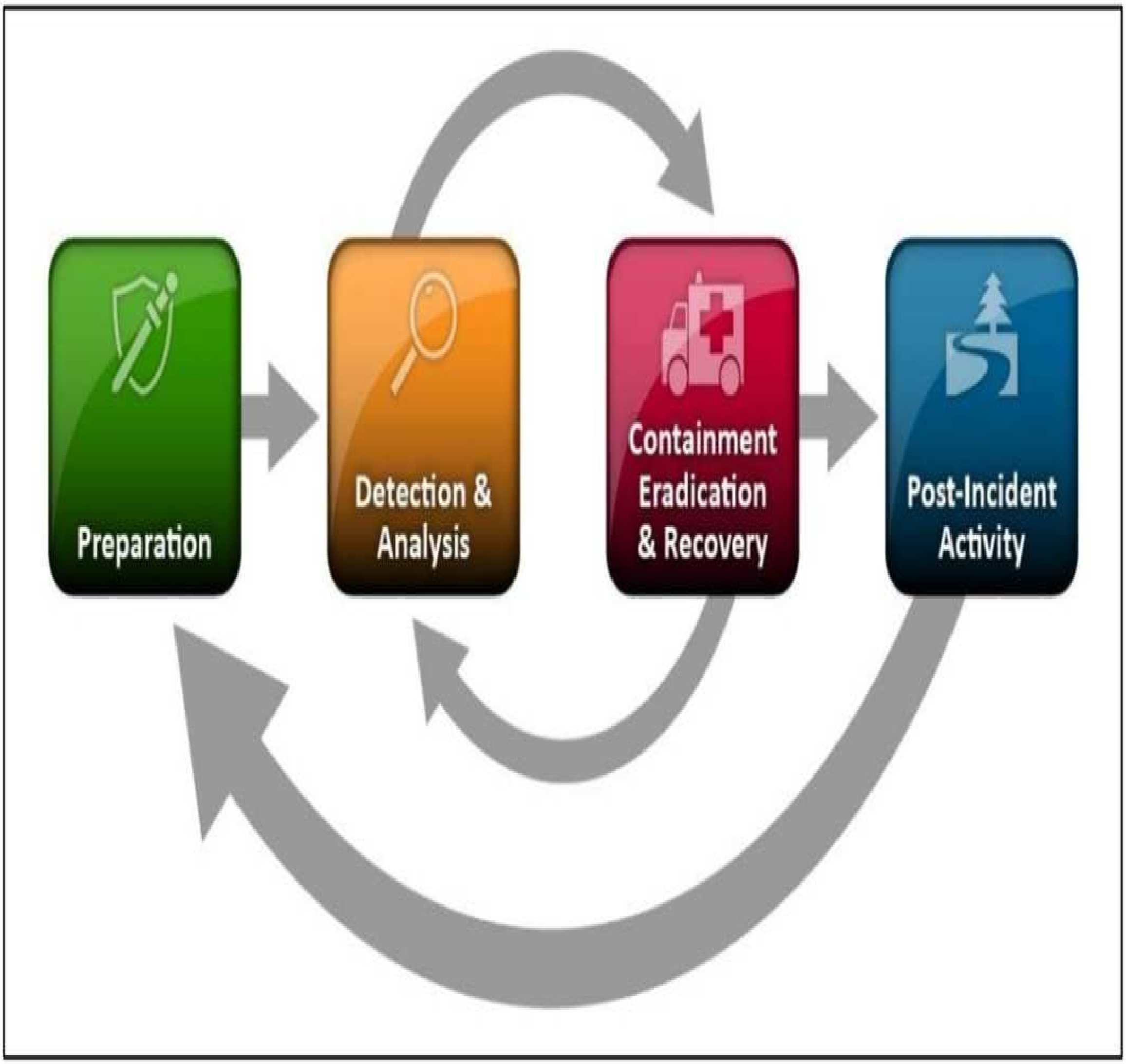


Figure 2.2: Incident Response Life Cycle (Paul et.al, 2011)

**Preparation**: This phase includes establishing an incident response capability as well as preventing incidents. The latter is not typically part of the IRT's tasks, but it is fundamental to the success of the organization's incident response. If a large number of incidents occur, it may overwhelm the IRT. To prepare for incidents, the incident handlers should have tools and resources such as contact information, incident reporting mechanisms, issue tracking system, digital forensic workstations and digital forensic software.

**Detection and Analysis**: Organizations should prepare to handle any type of incident. A classification of incidents can be used as a basis for incident handling. The guideline focuses onall kinds of incidents and does not address specific incident categories. A challenge related to incident handling is to detect the incident and determine the potential impact the incident may have. The actual detection may be the hardest part of incident handling. The guideline defines two types of signs of incidents; precursors and indicators, with indicators being the most common. These are defined in the following way: A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now." Common sources for precursors and indicators are Intrusion Detection and Prevention Systems (IDPSs), antivirus anti-spam software, third-party monitoring services, logs, people and information on new vulnerabilities and exploits

A challenging part of this phase is the analysis, i.e. to determine which indicators and precursors are legitimate, if they are really related to an incident and what has actually happened. When the team believes an incident has occurred they should try to determine the scope. All steps taken should be documented and time stamped. It is important to note that any such documentation can be used in court. The IRT should maintain a database containing information about incidents, such as status, indicators, related incidents and actions taken by the incident handlers. It is important to prioritize incidents and to handle them accordingly. Factors that can be used as a basis for prioritization include the functional impact of the incident, the information impact of the incident and recovery from the incident. When the prioritization is performed, the IRT should notify the appropriate people. It is important to have procedures regarding who these people should be.

**Containment, Eradication and Recovery**: Containment is obviously an important part of incident handling. The existence of strategies and procedures for containment is helpful. These strategies and procedures are different for different types of incidents. Gathering and handling of evidence are part of this phase. For some incidents eradication is necessary and it is sometimes conducted during recovery. Eradication can include deleting malware and disabling breached user accounts. Recovery consists of restoring systems to normal operations and in some cases eliminating vulnerabilities that could cause similar incidents. The guideline does not offer specific recommendations for eradication and recovery as these are often OS specific.

Post-Incident Activity Learning and improving are two of the most important parts of incident response. It is recommended to hold a lesson learned meeting after each major incident and periodically after minor incidents. One meeting could potentially cover several incidents.

Lessons learned meetings should generally focus on revealing shortcomings as well as what was successful. The desired result is that the organization will be better equipped for the next incident. Often, incident response policies and procedures are updated. Areas these meetings should focus on are how well the staff performed, whether documented procedures were followed, if procedures were adequate and how information sharing with other organizations could be improved to prevent similar incidents in the future.

Potential corrective actions and potential additional tools and resources should be reviewed. Both people involved in the incident(s) in question and people needed for future cooperation should be included in these meetings. A follow-up report that provides a reference that can be used when handling similar future incidents should be created. Other post-incident activities include the use of collected data for risk assessment, measurement processes to determine the success of the incident response team and audits of incident response programs.

### 2.5.4. ENISA - Good Practice Guide for Incident Management

This guide is developed by the European Network and Information Security Agency (ENISA) and provides a description of good practices for security incident management. The content is, unless specified otherwise, derived from(ENISA, 2011). The focus of this guide is IT and information security incidents. It specifically addresses the incident handling part of incident management. The incident management and incident handling processes are illustrated in figure 2.3. The incident handling process has four major components, as shown in the figure.

**Detection**: The CERT can receive incident reports from various sources. This guide recommends using e-mail as a communication channel as people prefer this. Additionally, it recommends using monitoring systems in addition to reports sent by others. Detection includes registration of incident reports in an incident handling system. This stage is a good place to implement profiteering mechanism for incident reports. The registration process could include the use of an incident report form.

**Triage**: This stage consists of the three phase’s verification, initial classification and assignment. During these phases the following questions should be answered:

Is it really an IT security incident? What is the impact?

Is there collateral damage?

How many people do you need to handle this incident?

Which incident handler should be appointed to the incident?

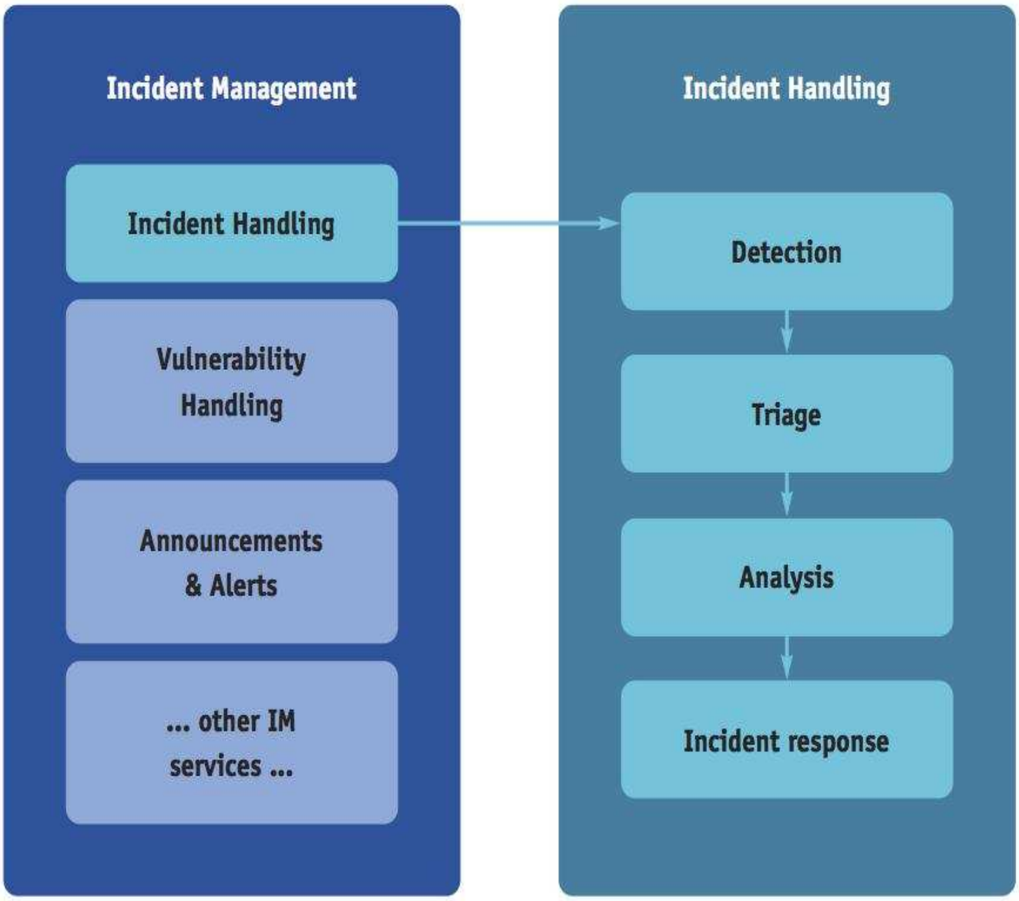


Figure 2.3: Incident Management and Incident Handling (ENISA, 2011)

The verification phase seeks to answer the first question. It is however recommended to respond to and archive all reports, even those not defined as information security incidents. They may include information relevant to other incidents or potentially lead to an incident. After an incident report has been verified the incident should be initially classified according to a classification schema. The last part of the triage component is to assign the incident to an incident handler.

**Analysis and Incident response**: These components are illustrated by figure 2.4. The cycle may need to be iterated several times. To perform data analysis there should be collected as much data as possible. Prior to the collection, all involved parties should be notified. Sources for data collection could be an incident reporter, monitoring systems, a referring database and relevant log files. The collected data should be used to try to determine the source of the incident. Prior to the data analysis, decisions about what data to analyze and in what order must be made. During the analysis, people will often exchange ideas and observations as well as draw conclusions. This belongs to the resolution research. It is recommended to advise team members to write down any observations that can be discussed in review meetings. The action proposed part consists of preparing a set of tasks for each party involved. The action performed should be monitored, where possible. The main goal for all actions is the eradication and recovery

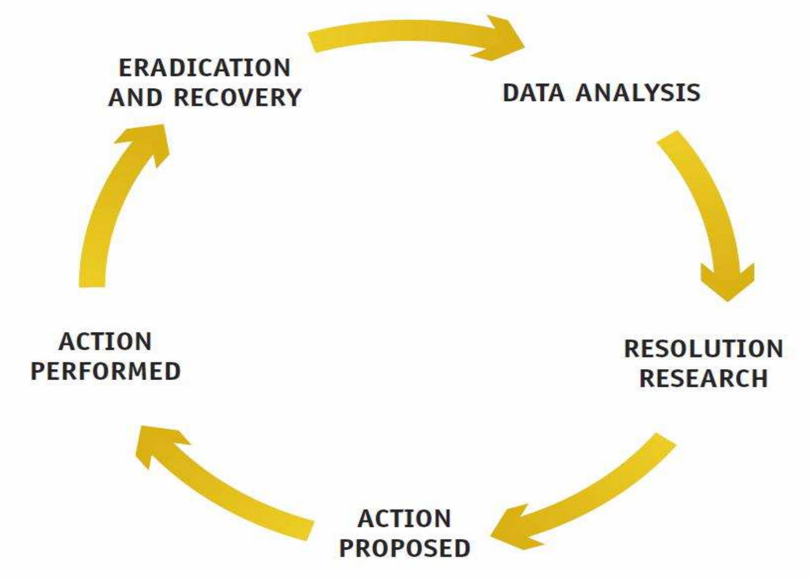


Figure 2.4: Incident Resolution Cycle (ENISA, 2011)

When you have left the incident resolution cycle, there are still tasks to perform. The incident needs to be closed properly. Each involved party needs to be informed that the incident is resolved. The classification of the incident should be revisited and a final classification should be performed. The classification could have been revisited during the resolution cycle as well. It is recommended to have taxonomy and to classify incidents in accordance with it.

After an incident has been resolved or closed a post-analysis should be performed in order to learn from the incident. It is also recommended not to analyze all incidents, but only the most characteristic and complex ones and those that include new attack vectors.

Incidents should be reported to the management. In addition to specific issues, the daily operations should be reported, including costs, positive results, plans and risks. This will save time and resources in situations where you need the management's operational or financial support and

### 2.5.5 SANS: Incident Handler's Handbook

This section gives an introduction to SANS' Incident Handler's Handbook and the content is, unless specified otherwise, derived from (Patrick et.al, 2011). The purpose of this document is to provide sufficient information for IT professionals and managers to create incident response policies, standards and teams for their organization. Six phases of incident management are described and recommended to be followed in sequence as each phase builds on the previous one.

**Preparation**: This is the most crucial phase as it determines how well the incident response team will be able to respond to security incidents. During this phase, several key elements should be implemented to avoid potential problems while responding to security incidents.

Organizations should develop a policy stating the organization's principles, rules and practices. After the establishment of a security policy, organizations should develop a response plan with a prioritization of incidents based on organizational impact. Having this prioritization scheme could aid in obtaining necessary resources for incident management by ensuring commitment from senior management as they will better understand risk and business impact. It is also recommended to have a communication plan so the response process is not delayed by uncertainty of whom to contact in unexpected situations. These plans should also state when it is appropriate to contact law enforcement.

Documenting incidents is beneficial for organizations. A thorough documentation is useful for lessons learned and might also serve as evidence if an incident is considered a criminal act. The establishment of a Computer Incident Response Team (CIRT) is part of the preparation phase. It is vital that also their activities are documented properly.

**Identification** The first step of this phase is identification of security events by detecting deviations from normal operations within the organization. This is followed by a decision of whether the event is categorized as an incident. Organizations should implement various tools to gather documentation about events, such that incidents and patterns can be identified. Examples of such tools include IDSs, firewalls and log files. Typically, incidents are reported to the CIRT that decides the scope of the incidents and how to move forward.

**Containment**: In this phase organizations try to limit the damage and prevent further damage caused by security incidents. It is recommended to isolate compromised systems to avoid escalation. An easy measure could be to disconnect affected parts of the system.

Several steps are necessary for a successful incident response. The first step is called short-term containment and is concerned with limiting the damage by implementing short-term but effective measures. The second step is concerned with ensuring proper back-up of information before system resources can be restored.

The final step is called long-term containmentand involves removing alternations made by an attacker, installing security patches and limiting further escalation of the incident.

Eradication Affected assets and systems are restored during this phase. To avoid similar incidents in the future, defenses should be improved. Continuous documentation is important in this phase to ensure that proper steps were taken in previous phases in addition to determine the overall impact on the organization. It is recommended that all affected systems are scanned with anti-malware software to ensure that all potential latent malware is removed.

**Recovery Activities**: in this phase include bringing affected systems back into operation and preventing future incidents caused by the same problem as previous incidents. Other activities are testing, monitoring and validating systems to ensure they are not re-infected.

**Lessons Learned**: The final phase's main objectives are to learn from incidents to improve the CIRT's performance and to provide material to aid in future incident responses. An important activity is to hold a post-incident meeting that summarizes the incident management process. This phase evaluates an organization's incident management procedures and identifies areas of improvement.

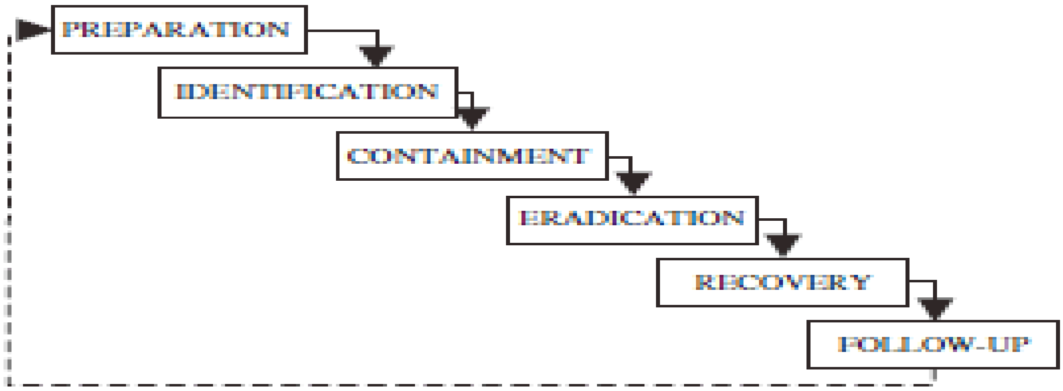
## 2.6 Similarities among Incident Management Standards

The standards and guidelines have a number of similarities and have chosen to divide the incident management process into several phases. Most of them describe a preparation phase, where an incident management capability is built. All of the standards and guidelines have phases for detection, analysis and incident responses, but the structure of these phases varies. All of them highlight lessons learned activities, even though not all describe a separate phase for this. ISO/IEC 27035 “Information security incident management” (ISO, 2011) and NIST Special Publication 800-61 “Computer Security Incident Handling Guide” (Cichonski et al.,2008) stand out as two of the main standards and guidelines related to information security incident management (Anne.I et al,2014). Both offera structured approach to incident management, including planning and preparing for incident response, what to do when incidents strike, and how to extract lessons learnt afterwards. SANS (Kral, 2011) and ENISA (ENISA, 2010) have also provided guidelines for incident handling, which resemble the structure offered by ISO/IEC and NIST. The guide from SANS is quite short and contains just an overview of which activities belong to each phase. ENISA has excluded the preparations phase and just focused on the activities performed by a response team in case of an incident. ITIL (Brewster et al., 2012) describes the incident management process as consisting of six components; Incident detection and recording, Classification and initial support, Investigation and diagnosis, Resolution and recovery, Incident closure, and Ownership, monitoring, tracking, and communication during the progress of the incident handling. Activities related to planning and preparations are included in other parts of ITIL and hence not presented as part of the incident management process itself. FIRST provides a couple of guidelines on how to set up an incident response team within an organization. These are specifically concerned with planning and preparations, and do not cover the complete incident management process. CERT/CC describes comprehensive guidelines for establishing and operating an incident response team in their CSIRT handbook (West-Brown et al., 2003). Furthermore, they describe their CERT/CC Incident Handling Life Cycle process.

This resembles the processes described by ISO/IEC and NIST; an incident is detected and considered in a triage before a report is generated. Then there are the states of analysis, obtaining contact information, providing technical assistance, and coordinating information and response, before the incident is finally resolved. The main recommendations of ISO/IEC and NIST are similar. The ISO/IEC 27035 standard stands out as the most recognized, as it is developed by international consensus by experts worldwide(Anne.I et al,2014).Therefore it is worth noting that the guidelines presented are developed by single organizations, whereas the ISO/IEC standards are developed by groups of experts from all over the world. The development and approval of the ISO/IEC standards are extensive processes with many contributors and should therefore be widely accepted (Hove.G&Tarnes.M, 2013).Hence, ISO/IEC 27035 is used as analytic frame in this research.

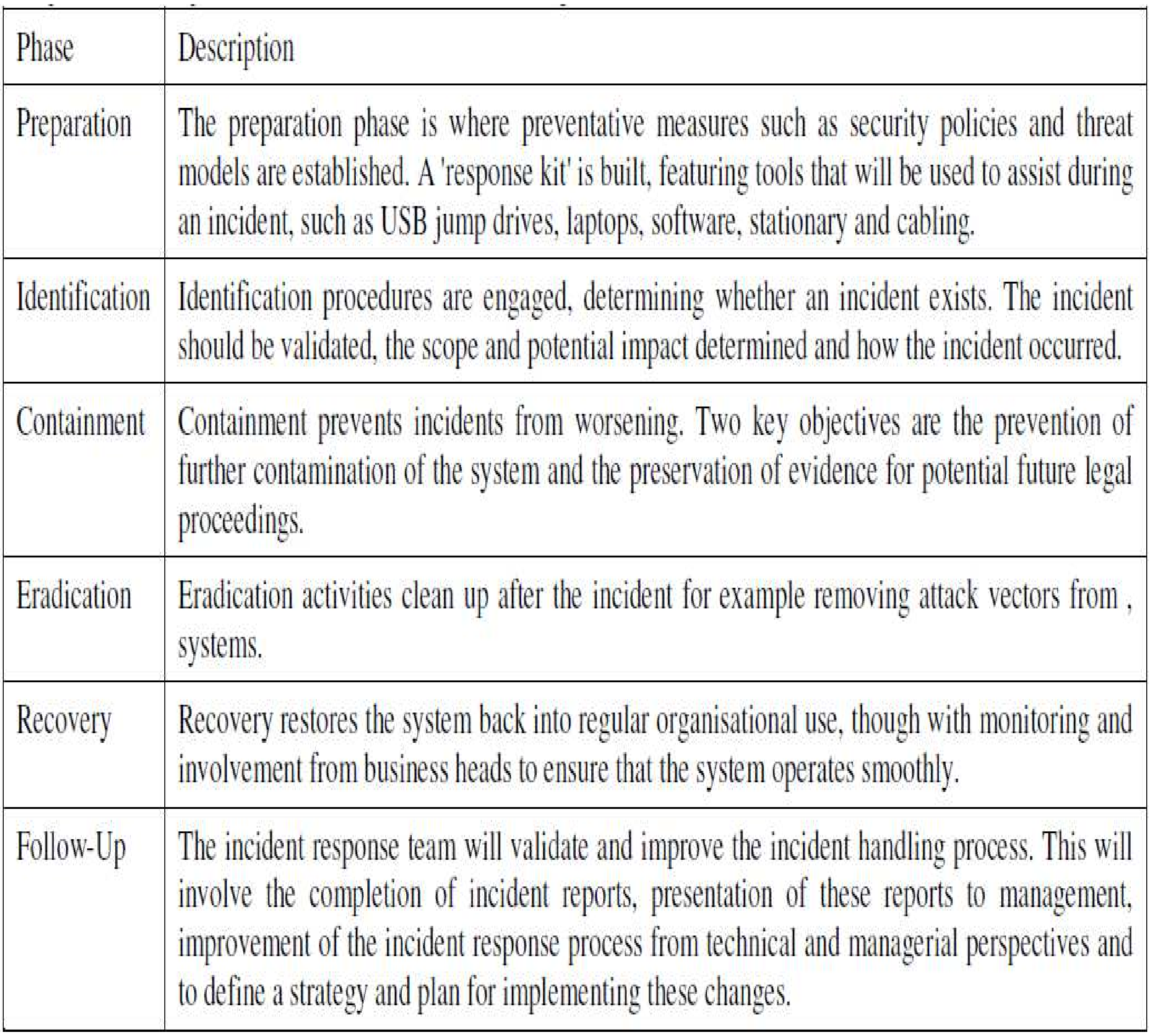
## 2.7. Best-Practice Methods of Security Incident Response

Security incident response refers to the process by which organizations engage dedicated or ad hoc teams to identify and treat information security incidents (West-Brown, 2003; Wiik et al, 2005). Depending on the scope of the team, they can be either technical or multidisciplinary, featuring members across a variety of business lines, balancing a range of skills that may include the technical, diplomatic and organizational (Murray, 2007). The formal process of security incident response is summarized in Figure.2.5



|Figure 2.5.The Incident Response Process (Mitropolous et al, 2006)

The phases of this process in figure 2.5, are explained in the following table 2.1



| Phase | Description |
|---|---|
| Preparation | The preparation phase is where preventative measures such as security policies and threat models are established. A 'response kit' is built, featuring tools that will be used to assist during an incident, such as USB jump drives, laptops, software, stationary and cabling. |
| Identification | Identification procedures are engaged, determining whether an incident exists. The incident should be validated, the scope and potential impact determined and how the incident occurred. |
| Containment | Containment prevents incidents from worsening. Two key objectives are the prevention of further contamination of the system and the preservation of evidence for potential future legal proceedings. |
| Eradication | Eradication activities clean up after the incident for example removing attack vectors from , systems. |
| Recovery | Recovery restores the system back into regular organisational use, though with monitoring and involvement from business heads to ensure that the system operates smoothly. |
| Follow-Up | The incident response team will validate and improve the incident handling process. This will involve the completion of incident reports, presentation of these reports to management, improvement of the incident response process from technical and managerial perspectives and to define a strategy and plan for implementing these changes. |

Table 2.1: Incident Response Phases (Northcutt, 1998)

## 2.8. Related works

Researches has been done by scholars from abroad regarding assessment of information security incident management practice in different organization using ISO/IEC standard and guideline. Some of them are discussed in the following table 2.2.

| Author | Objective | Methodology | Key finding | Observed gaps |
|---|---|---|---|---|
| Hove and Tarnes ,2013 | Assessing current practice of information security incident management practice | Interviews<br>Document study<br>Survey | Employees in our survey seem to have an overall positive attitude towards awareness campaigns<br>Findings from Organization A showed that their information classification is not satisfactory | Although the researchers focused in all five phases of information security management guidelines which is provided by ISO, they did not make in depth study for each of the phases equally |
| Maria B. Line and EirikAlbrechtsen | To examining the suitability of industrial safety management approaches for information security incident management | Interview | Training for information security incidents is not prioritized<br>Post-incident evaluations are not performed | They only focused 0n plans, compliance, and situational adaptation; training; and learning from incidents |
| Maria B. Line,2014 | To survey current practice for information security incident management. | interview | Detection mechanisms are insufficiently applied<br>The absence of | |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  | major incidents limits preparatory activities<br>Outsourcing reduces preparatory activities.<br>Training for information security incidents is not prioritized |  |
| Maria B. Line,2015 | To survey current practice for information security incident management. | Interview | Detection mechanisms are insufficiently applied<br>The absence of major incidents limits preparatory activities<br>Outsourcing reduces preparatory Training for<br>information security incidents is not prioritized activities<br>Post-incident | These researchers also didn't focus in all five phases of ISO guideline. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  | evaluations are not performed |  |
| Maria B. Line and Nils Brede Moe,2015 | To understand challenges met during preparedness exercises for information security incidents in order to provide recommendations for future exercises. | observation | Outsourcing reduces preparatory activities<br>Post-incident evaluations are not performed | They didn’t focus in all five phases of ISO guideline. |
| Grispos,et.al | To present the security incident response criteria. | Interview | Security incident response criteria | Their focus was only in preparing security incident response criteria. |
| Shedden, et.al, 2011 | To explore organizational learning concepts. | Focus group | Response to incidents is largely informal.<br>A need for a new incident response model that incorporates informal learning practice. | The focus of these researchers were also only on the single phase of incident management. |

| | | | | |
|---|---|---|---|---|
| | | | | |
| Welinger ,et.al. 2007 | To determine what skills,tools and strategies were required to manage and handle security incidents. | Interview | Practitioners often used pattern recognition and hypothesis generation during the analysis of security incidents. | This research also didn’t cover all phase of incident management practice. |

Table2.2. Related works.

As it is shown in the above table2.2, researchers have tried to assess current practice ofinformation security incidents in different organizations and they have identified gaps in relation with international standard.

Hove and Tarnes (2013)has studied the three Norwegian companies and they identified that all had incident management plans in some form. This included plans and guidelines for handling (specific types of) security incidents, established routines, incident management handbooks for the incident response team, and plans for communication during incidents. They also emphasized that, for organizations with distributed organizational structures there are many sources of information hence knowing how much information to share can be difficult more over they have identified that in cases where IT operations are outsourced, collaboration during incident management is even more challenging. Even minor incidents can be problematic if all assume the incident to be someone else's responsibility. Although the researchers focused in all five phases of information security management guidelines which is provided by ISO, they did not make in depth study for each of the phases equally on top of that their study bases the organizational culture of those three Norwegian companies under their study. These calls for further study in the area, hence generalization is impossible. Maria B.Line and EirikAlbrechtsen have tried to examining the suitability of industrial safety management approaches for information security incident management, but they only focused 0n plans, compliance, and situational adaptation; training; and learning from incidents.

Line and Nils (2015) has also researched challenges met during preparedness exercises for information security incidents in six power industries. They have used observation as a data collection instrument and they have identified that outsourcing reduces preparatory activities and post incident evaluations are not performed. These researchers also didn't focus in all five phases of ISO guideline.

Security incident response criteria were researched by Grispos et.al. They have used an empirical research with a data collection method interview. Their focus was only in preparing security incident response criteria. These researchers pointed that there are fundamental problems with existing security incident response process solutions.

Other researchers, Shedden, et.al.(2011), conducted a research to explore organizational learning concepts. They have used a focus group method to find out that response to incident is largely informal. They have highlighted that the need of a new incident model that incorporates informal learning practice.The focus of these researchers were also only on the single phase of incident management.

An exploratory study that investigated the security incident activities of practitioners was conducted by Welinger, et.al.(2007). They have used interview as a method of data collection. The objective of their study was to determine what skills, tools and strategies were required to manage and handle security incidents. The result showed that practitioners often used pattern recognition and hypothesis generation during the analysis of security incidents. This research also didn't cover all phase of incident management practice.

Hove.G.&Tarnes.M(2013), also mentioned that, even though, few studies of current practices in information security incident management have been conducted, generalization is not possible for all organizations. Hence, it is vital to study information security incident management practice in different organizations. As per the knowledge of the researcher, information security incident management practice is not studied locally in financial industries like banks. This research is intended to investigate the current information security incident management practice at bank x of Ethiopia

## 2.9 Chapter Summary

The fundamental concepts related to information security incident management practices, has been discussed thoroughly in this chapter. Guidelines and international standards to assess information security incident management practice also presented. It is noticeable that, scholars are paying attention for the issue of assessing information security incident management practice in literature. On top of that this chapter highlighted that,among internationally accepted guidelines and standards for assessing information security incident management practice, ISO/IEC 27035 appeared being powerful as it is developed extensively by experts from different corner of the world ISO. Due to this reason most of the researchers in literature applied it to assess the current practice of information security incident management of different companies and indeed this research relies on it as well.

The next chapter deals about the methodology and design of theresearch.

# CHAPTER THREE

## RESEARCH DESIGN AND METHODOLOGY

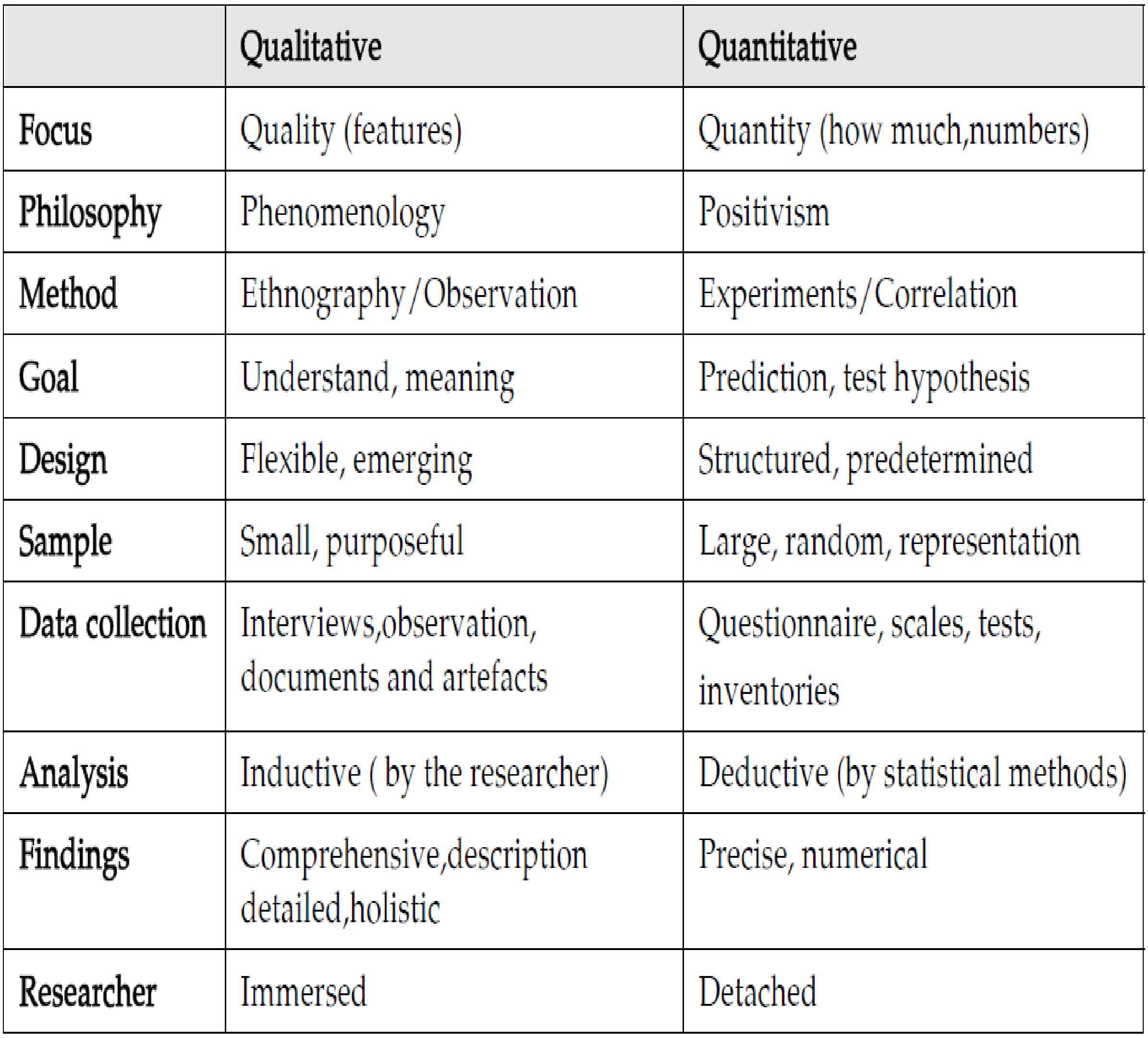
This chapter describesthe research design and methodology which is intended to meet the objectives of this research. Thus, the chapter discusses the research design and techniques used toanswer the research questions. It covers the research methodology, data collection methods, and data source, validity and reliability anddata analysisisissues.

### 3.1 Research Design

A research design is a plan used as a guide in collecting and analyzing research data for the studyto be conducted. It describes the methods used to collect and analyze the data that helps toanswer the research question. Hence this research is qualitative and exploratory in nature which intended to assess the current practice of information technology incident management at bank x of Ethiopia, it usescase study

### 3.1.1 Qualitative Research

In order to satisfy the objective of this research, a qualitative research was held. The main characteristic of qualitative research is that it is mostly appropriate for small samples, while its outcome is not measurable and quantifiable. Its basic advantage, which also constitutes its basic difference with quantitative research, is that it offers a complete description and analysis of a research subject, without limiting the scope of the research and the nature of participant’s responses (Collis and hussy, 2003).There are some differences between quantitative and qualitative approach inresearch methodology.



| | Qualitative | Quantitative |
|---|---|---|
| Focus | Quality (features) | Quantity (how much,numbers) |
| Philosophy | Phenomenology | Positivism |
| Method | Ethnography/Observation | Experiments/Correlation |
| Goal | Understand, meaning | Prediction, test hypothesis |
| Design | Flexible, emerging | Structured, predetermined |
| Sample | Small, purposeful | Large, random, representation |
| Data collection | Interviews,observation,<br>documents and artefacts | Questionnaire, scales, tests,<br>inventories |
| Analysis | Inductive ( by the researcher) | Deductive (by statistical methods) |
| Findings | Comprehensive,description<br>detailed,holistic | Precise, numerical |
| Researcher | Immersed | Detached |

Table 3.1: Differences between qualitative and quantitative research
(Adapted from Potter, 1996)

In ICT, both methods play a significant role in facilitatingthe entire research process and leading to desirable results or outcomes.A researcher is always the main in data collection and analysis in qualitative approach, compared to questionnaire or tests in case of quantitative approach. Qualitative method also involves field work where a researcher must participate in the setting especially for observation and interviews with respondents of the research topic. Qualitative research adopts the inductive approach. Such a method is conducted due to lack of theory related to the research topic that is unable to explain a phenomenon convincingly. A qualitative approach also focuses on process and understanding based on rich description of body of knowledge.However the effectiveness of qualitative research is heavily based on the skills and abilities of researchers, while the outcomes may not be perceived as reliable, because they mostly come from researcher’s personal judgments and interpretations. Because it is more appropriate for small samples, it is also risky for the results of qualitative research to be perceived as reflecting the opinions of a wider population (Bell, 2005).

### 3.1.1.2 Case Study

A case study is an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context. It relies on multiple sources of evidence and benefits from the prior development of theoretical propositions to guide data collection and analysis. Case studies are well suited for development of detailed, intensive knowledge about a single case, or of a small number of related cases moreover it focuses in contemporary events and it is applicable to real-world organizations (Robert.K.Yin, 2009),which is where the focus of this study is. Yin described that the applicability of case study to research questions in a form of How & Why and were thus chosen as the preferred research strategy.

### 3.1.1.3 Analytic Frame ISO/IEC 27035

ISO/IEC 27035 describes information security incident management process. According to ISO/IEC 27035 “Information security incident management” (ISO, 2011), information security incident management process comprises of five phases.The first phase runs continuously, as opposed to the next four, which are triggered by the occurrence of an incident. Plan and prepare includes activities such as establishing a dedicated response team, defining roles and responsibilities, documenting procedures, and training of personnel and awareness raising activities regarding incident management throughout the organization. Detection and reporting is the first operational phase of incident managementand involves detection of what might be an incident and reporting into an incident tracking system. Deciding what kind of response is needed to cope with the registered event belongs to the Assessment and decision phase. The Responses phase then describes the actions taken to cope with the incident and prevent further consequences, restore systems, collect electronic evidence, and possibly escalate to crisis handling. The final phase, Lessons learned, is when the team analyzes whether the incident management scheme worked satisfactorily and considers whether any improvements are needed on any level: the scheme, policies, procedures, security mechanisms, or similar. The improvements are then implemented as part of the continuously running phase of Plan and prepare. Similar recommendations are described by NIST and ITIL, as well. Existing standards and recommendations in the area of incident management provide a useful baseline for organizations about to implement their own scheme or looking for inspiration for improvements. The ISO/IEC 27035 standard stands out as the most recognized, as it is developed by international consensus by experts worldwide(Anne.I et al,2014).Hence ISO/IEC 27035is the most comprehensive guideline for information security incident management, it used as a basis in this research, to investigate the current practice of information security incident  management at bank x.

## 3.2Research Approach

The research approach that was followed for the purpose of this research was the inductive one. This approach let the researcher to begin with specific observation, which is used to produce generalized theories and conclusion drawn from the research. The reason for accepting inductive approach was that it takes into account the context where research effort is active, while it is also most appropriate for small samples that produce qualitative data. However, the main weakness of the inductive approach is that it produces generalized theories and conclusions based only on a small number of observations, thereby the reliability of research results being under question (Denzin and Lincoln, 2005)

## 3.3 Data Collection Method

Among the qualitative data collection methods face to face semi-structured interview E-mail interview were used., in order that the information is richer and has a deeper insight about the subject of this research more over interview is seen as being one of the most important sources of information in a case study (Robert.K.Yin, 2009). A reasonable number of interview questions were open-ended so that respondents can have a chance to provide additional and detail information. Interview questions were adapted from an international information security incident management standard and guideline, ISO/IEC 27035.After conducting interviews internal documentation requested from participant that would assist the researcher in collecting synthesizing and cross- referencing responses (Shwaz&Hirschhein, 2003).Because of bank x's security policy and confidentiality reason the researcher couldn't access those documents.

### 3.3.1. Qualitative Interviews

Qualitative interviews are a well-known and powerful tool for information collection in qualitative research (Myers.D& Newman.M, 2007). They allow for the researchers to view the phenomenon from the interviewees' perspective and understand why and how they got that particular perspective (Cassell.C&Symon.G, 2004). To meet this objective, qualitative interviews were driven by open questions, a low degree of structure, and a focus on specific situations and experiences made by the interviewee.

## 3.4 Data Source

The method of purposive sampling was used to identify the data source of this research. Purposive sampling belongs to the category of non-probability sampling techniques, sample members were selected on the basis of their knowledge, relationships and expertise regarding a research subject (Freedman et al, 2007).The target population of this research was IT staffs who were working at bank x's head office. But for this specific research, the researcher identified the participants based on their current role, which was related to the issue of this research. Hence, the participants of this research for in person interview were 4 managers from different IT departments: information system security manager, infrastructure and application manager, ATM and e-payment manager and the security operation center team leader. Participants for e-mail interview were: 9 cyber-attack analysts who work at security operation center of bank x.

## 3.5 Validity and Reliability

Validityin research is concerned with the accuracy and truthfulness of scientific findings (LeComple and Goetz 1982: 32). Avalid study should demonstrate what actuallyexists and a valid instrument or measureshould actually measure what it is supposed tomeasure. There are many types of validity and many names have been used to define the different types of validity. Campbell and Stanley (1966) have defined two major forms of validity that encompass the many types. They refer to "internal" and "external" validity. Denzin (1970) used the distinction between internal and external validity and applied it to qualitative research. Internal validity is the term used to refer to the extent to which research findings are a truereflection or representation of reality rather than being the effects of extraneous variables. External validity addresses the degree or extent to which such representations or reflections of reality are legitimately applicable across groups.

Validity issues need to be considered when designing a research project and evaluated when analyzing the credibility of research results. Construct validity concerns whether a study measures what it sets out to measure (Robson.C,2011). Both interviewees and the researcher may be biased, either consciously or unconsciously (Diefenbach.T). Bias may be overcome by a number of strategies, such as triangulation and member checking. Data triangulation means using several methods for collecting evidence, such as interviews, document analysis, and observations. This allows for studying a phenomenon from different perspectives and increases data quality (R.K.Yin,2009).Member checking involves returning data material to the respondents for review and shows that their contributions are valued.

Reliability is concerned with the consistency, stabilityand repeatability of the informant's accounts as well as the investigators' ability to collect and record information accurately (Selltiz et al 1976:182). It refers to the ability of a research method to yield consistently the same results over repeated testing periods.

In order to reduce risks to validity and reliability of this research, the researcher performed the following tasks:

- So as to eliminate the researcher effects, Field and Morse recommended that researchers undergo extensive and rigorous training as interviewers and observers before undertaking qualitative study. The researcher of this study was exposed herself for several online and face to face trainings about the subject of this research. The researcher practical experience about the subject of this research was very helpful to move from untrusted stranger to a trusted and friendly person during the research process.
- To reduce sample bias, sample selection was based on the ability of the respondents to provide data relevant to the research questions. The researcher judgment based upon the best available evidence to choose interview participants who know enough was applied.
- The researcher clarified the nature of the research for the participant of the interview. There was a discussion between the researcher and each of the interviewee 2 days before the interview conducted. During the discussion participant were able to understand why the research conducted in their bank, how the data collected, and for what purpose it

used. Hence, it was possible to build a trust-relationship among the interviewees and the researcher.

- Because the subject of this research is sensitive, the interpersonal context under which the data gatheredwas taken in to consideration by the researcher. Particular attention to confidentiality had paid. Interview conducted at bank x offices after making sure that both the researcher and the interviewees were not exposed to be overheard by others in the environment.
- Analysis and findings of this research was sent via email for the face to face interview participant of this research. Three of them reviewed and returned it in time. The researcher took their review into consideration to validate the findings.
- Face to face interview and survey as e-mail interview was data collection tools and used as a means of triangulation.

## 3.6. Data Analysis

Data analysis allows linkage to be established between the research object and the outcomes regarding the original research questions (Parikh, 2002).

Content analysis was used to analyze the data which was gathered from face-to-face interview and survey. According to Moore and Mc Cabe(2005). This is the type of research whereby data gathered is categorized in themes and sub-themes, so as to be able to be comparable. Content analysis gives the ability to researchers to structurethe qualitative data collected in a way thatsatisfies the accomplishment of research objectives. However, human error is highly involved in content analysis, since there is the risk for researchers to misinterpret the data gathered ,thereby generating false and unreliable conclusions(Krippendorff and Bock,2008).

Tape recordings of interview were transcribed and it has passed through several phase of analysis. First, a preliminary analysis conducted in order to get a general sense of the data and reflect on its meaning. Next,a more detailed analysis were performed and data were divided into segments or units that reflect specific experiences, thought and knowledge of participants .at the end of this analysis a list of topics weregenerated and the topics was compiled into categories that labeled as key findings.

## 3.7. Chapter Summary

The research design and methodology has been discussed in this chapter. The chapter clarified that, qualitative research was the design of this study followed by inductive research approach. As a method for this research case study was employed. Among the qualitative research data collection instruments, face-to-face interview and E-mail interview was discussed in this chapter, as this instruments used to collect relevant and in depth data related to this study.Moreover, the chapter presented the analytic frame of this study which was ISO/IEC 27035.Steps that was performed to address Validity and reliability issues of this research has been also discussed in this chapter. Finally, the data analysis process of this research waspresented.

The next chapter will discusses about, data presentation, analysis and discussion of this research.

# CHAPTER FOUR

## DATA PRESENTATION, ANALYSIS AND DISCUSSION

## 4.1. INTRODUCTION

This chapter presents data as introduced from interviews, analysis and discussion of findings. In the discussion part links between the research questions and findings are established. The findings from face-to-face interview and E-mail interview described separately but the grouping of the information is based on the five phases of ISO/IEC 27035 standard and guideline.Inductive analysis performed as it described in section 3.6.

## 4.2. Respondent Information

- The respondents of the research include IT staffs who are engaged in managerial position and those who play significant role in information security incident management. The job title of these officials are information system security manager, infrastructure and application manager,ATM and E-payment manager, security operation center team leader and cyber-attack analysts at security operation center.
- It was the researcher impression to carry out face-to-face interview with the mobile and internet banking manager as well, but the manager was tied up in different commitment at bank x . Due to that reason interview was not able to conduct with the internet and mobile banking manager.
- The working environment of the security operation center was not convenient to conduct face-to-face interview. Hence, theresearcher has changed it in to survey. Out of 9 e-mail interview sent for all cyber-attack analysts 7 of them replied for it in time.

## 4.3. Challenges in Data Collection Process.

Cooperation letter from AAU to Bank x was submitted by the researcher at the end of February. HRM office of bank x accepted the letter and wrote inter departmental memorandumletter for information system security department to be cooperative with researcher without compromising the bank confidentiality. The researcher had to made several calls to arrange for the meeting with the security manager. After waiting for aweek, the first meeting held with the security manager to clarify the nature of the research. The challenge started at that point. The manager completely rejected the idea of conducting information security related research at bank x. he simply said that, “we are not going to allow you to conduct this research.” That was verydisappointing and bad news for the researcher. But the researcher went back again and again to the security manager office to get another chance to explain more so that the manager can be convinced. The good thing was the manager agreed to discussagain. The researcher was able to convince the manager and the data collection started by conducting the first interview with the security manager. Things seem went well at that time. But again in the middle of the data collection, another official from bank x refused the research and he reported to the top level management of bank x. the top level management decided to stop the research and that  decision told for the researcher on phone. It was a desperate situation for the researcher. But by the help and encouragement of the researcher’s advisor, the researcher convinced the officials to continue researching under two circumstances. By refraining from publishing the name of the bank and by avoiding any content of the research document the gives clue about which bank is. In general, it was a very disappointing andmajor challenging process that affected the researcher time management negatively.

## 4.4. Data Presentation

### 4.4.1. Data from Face-To –Face Interview

Under this part, the data presented as it is introduced by interviewees using face-to-face interview. The interviewees were: information system security manager, infrastructure and application manager, ATM and E-payment manager and the security operation center team leader.

**Plan and prepare**

Interviewees were asked about their understanding of information security incident.The security manager described that, information security incidents as events which compromise the confidentiality, availability and integrity of information assets.  For instance: trying to collect and harvest our email addresses, malicious software, high level access requests, ransom ware attack and many more. The infrastructure manager and ATM manager have almost same definition, they said, it is a security event that can affect or breach the normal transaction. According to the security operation center team leader, information security incident is un necessary information disclosure or unauthorized access of information assets, especially those which can cause negative impact in companies’reputation. His definition is actually grounded in the explanation given by the security manager

He said:

“…information security incidents are those security events that can cause financial loss and reputational damage.”

All interviewees mentioned that, Information security policy is the main governing document at Bank x moreover they prevailed that, they don’t have specific policy to address information security incident management. The security manager said that, bank x has grand information security policy that gained top level management commitment but it also includes some about information security incidents. He added that they actually had procedures for security incident handling but it is not approved by top level management. The infrastructure manager also said that, they don’t have detail policy that could be used for information security incident management but some issues about information security incidents are included in security policy. ATM manager and the security operation team leader highlighted that, their bank is on process to implement international frame work for information security management.

When interviewees were asked about incident response team: the security manager described that they have an incident response team that includes all security operation center cyber-attack analysts and some other IT staffs as a virtual team. He said that, because the cyber-attack analysts are the one responsible to monitor bank x’s cyber space 24/7, they all are member of the response team but those IT staffs out of the security operation center are participant when needed. The infrastructure manager mentioned that all senior IT staffs from each category have role to perform information security incident related tasks but they are not in one team. He added that, even though those cyber-attack analysts at security operation center arefocusing mostly on those incidents which are visible to them, they are considered as incident response team. The ATM manager and the security operation center team leader have agreed with the explanation of the infrastructure manger. The security operation center team leader said that:

“…in our security operation center, we monitor the cyber space 24/7 using security information event management system but security incidents cannot be addressed by control center workers only. It is advantageous to have a holistic team who can lead information security incident handlers in different departments.”

According to interviewees, Information security incident prevention is performed using globally well-known technologies in Bank x. the security manager stated that, there is a centralized antivirus that scans computing devices regularly. Vulnerability scanner tools, network edge defense like IPsec, encryption of data in transfer and storing depending up on their sensitivity, perimeter zone that filters traffic, fire walls and other globally well-known and recommended technologies are in place and in use to prevent information security incidents. The security operation center team leader has agreed with what the security manager said and he added that, they use awareness creation programs as incident prevention mechanism. Implementing security policy was deemed as information security incident prevention mechanisms by infrastructure manager. He highlighted that, one of their prevention method is implementing security policy. Security has priority and gained top level management commitment .creating awareness for employees, to understand what they are allowed to do and not is also part of security incident prevention. Moreover we use enterprise tools in which we control and see all devices. VPN is also among our incident prevention mechanisms. In addition to this we use central patch management tools to fix vulnerability holes. We have more than 35 thousands computing devices in distributed locations across the country due to this fact updating endpoint security is a bit challenging for us. We are working to stabilize its architecture so that end point security will be updated automatically to prevent our computing devices from viruses and other threats.

He said:

> "…Our bank doesn't compromise on security related issues."

Similarly, ATM and e-payment manager described incident prevention in his department by illustration. He said, Bank x gives emphasis for in advance prevention before the actual attack is coming. For instance, in order to secure card banking, triple data encryption standard is implemented, production and printing of cards are free from human intervention and hard ware security module calculate password for customers. There is also segregation of duty in this department; accordingly IT specialists have access to systems to accomplish specific tasks only. This contributes to prevent information security incidents.

Interviewees were also asked about relationship with other organizations. All of them agreed that Bank x established and preserve relationships and connection with appropriate internal and external organizations. INSA and federal Police are those who work closely with Bankxthey also work together with national CERT team.

All Interviewees mentioned that classification of incidents is performed at Bank x,they said that, information classification is basic for incident classification. Bank x classified information depending up on their sensitivity and accordingly,they classified information security incidents depending up on the damage they may cause on information assets. They are classified under the categories low, medium and high impact incidents.

Interviewees were asked about awareness and training: the security manager explained that awareness has been provided through all available means of communication in Bank x. via intranet, portal, company email, security magazines, in house developed knowledge management database. Those who have managerial roles and security operation center employees took part in most information security incident handling related trainings. But awareness creation program was available for almost all staffs in bank x. The security operation center team leader agreed with what the security manager said and he added that, cyber-attack analysts are trained in incident handling and most of them are certified.According to the infrastructure manager, training didn't include all IT staffs when it comes to specific security operations. He said that, It is not enough to train some group of IT staffs only, as prevention and handling of information security incidents can't be only responsibilities of security operation center workers. He also mentioned that, he is suspicious about that whether they are addressing awareness properly or not. The ATM and e-payment manager have agreed with what the infrastructure manager said.

Bank x never performed emergency preparedness exercise as it is explained by all of the interviewees. The security manager described that, they never did rehearsal to test incident management schema but they have done it before few years for disaster recovery.

He said:

"we have never done emergency preparedness exercise …no one pay attention for that and it is not a good practice to keep an incident handling procedure without testing it yet …we even don't know whether our security incident handling procedures works out or not. Because we have not yet identified our weakness and strength through rehearsal…it is a clear gap here that we need to work on it."

**Detecting and Reporting**

Available security incident detection mechanisms at bank x are mentioned by interviewees. The security manager stated that, they use different alternatives to detect security incidents. For initial detection; antivirus detect and report viruses and in some cases employees themselves report that their computing devices is not working or they are unable to log in to the system. He also mentioned that they use IDS, firewalls, UTM, antimalware software ,network flow analysis, log collectors ,security information event management system. Using SIEM log generated from hardware and software goes through analysis of correlated and consolidated patterns of possible cyber-attacks.

He said:

"We detect information security incidents in two ways: from those logs which captured direct from our systems and from user report."

The infrastructure manager also mentioned that Bank x performed multiple activities that aims to detect information security incidents. They used centralized antivirus software, network security devices like firewall, vulnerability scanner tools, and log monitoring tools. He also highlighted that, reports that came from users and third parties who work together with the bank are part of information security incident detection means for them. Having holistic view of the entire cyber space of bankx, their security operation center detects information security incidents in 24/ 7 monitoring. The ATM and e-payment manager described that, detection of information security incidents is managed in two ways at Bank x. manually and automatically. The security operation team leader highlighted that, identification of vulnerabilities allows Bank x to fix security holes before the real attack is coming. He mentioned that all traffics that comes in and out in the cyber space of Bank x are monitored by separate security operation center. He also listed currently available information security incident detection means which already mentioned by other interviewees.

He said:

"…our security operation center is our best practice we want others also to adopt it."

Interviewees explained that,reporting on the events (possibly information security incidents) may happen manually or automatically. Employees may report information security incidents via phone, company email or in some cases in person. Automatic detection tools also notify and report information security incidents.The security manager stated that they have a dedicated call center to accept information security incident reports from any of Bank x's employees. He also mentioned that users may report security events for their immediate IT support staffs, for security operation center workers or for the security manager. The security operation center team leader described that, those information security incidents which are detected using automatic tools especially using SIEM are registered in the incident tracking system under their pre-defined categories.

He said:

"…it is very important to register information security incidents and update incident tracking system data base in order to mitigate serious consequences. But we are not exhaustively and properly registering information security incidents which are detected and reported manually."

ATM and e-payment manager has agreed with what the security operation team leader said and he highlighted that, it is not a good practice not to maintain the quality of registering security of incidents which are identified and detected manually.

**Assessment and Decision**

According to the security manager and the security operation center team leader, using Bank x's agreed incident classification scale, cyber-attack analysts which are categorized in three tires. i.e tire1, tire 2 and tire 3, perform information security incident assessment.The security managerdescribed that there is an assessment of information security incidents mostly conducted by cyber-attack analysts who are responsible for real time monitoring activities at SOC. tier 1 cyber-attack analysts perform assessment on low level correlations, alerts or notification and they give immediate solutions. If the attack is complicated, tier 2 cyber-attack analysts will do further analysis and documentation. Senior cyber-attack analysts perform further detailed findings and they keep working on it until they bring policy and meaningful infrastructure change in order to avoid re occurrence of information security incidents. Moreover they determine whether the information security event should be classified as an information security incident or is in fact a false alarm. The infrastructure managerpointed that, the role of handling security incidents are dispersed in different IT departments at bank x. according to his explanation, they try to identify and assess incidents which are detected manually in their department. Those incidents which are detected using monitoring tools managed by cyber-attack analysts at SOC. it is their responsibility to assess and confirm on the decision as to whether security events are in fact security incidents.

He said:

"… hence monitoring teams focus mostly on those incidents detected automatically, we need to have IRT that will address assessment and decision of each security events including those detected manually."

The ATM and e-payment manager sees assessment and decision of information security events as a very important phase to respond successfully for security incidents. He said, they assess security events based on the location in which the security event detected manually. For example, reports which are forwarded to the call center about ATM and e-payment investigated and assessed by their department. He mentioned that, they work together with information system security department and other IT departments. According to the security operation center team leader, assessment of information security incidents may be conducted by the person who identified the security incidents at bank x. But sometimes this may require highly qualified personnel .They have limitation here,

He said:

"I can say there are almost no skilled cyber-attack analysts at tier 3 level with the necessary competence to assess and analyze sophisticated attacks in our local market."

**Response**

The security manager mentioned that, after they make sure about the occurrence of information security incidents, they notify by email, phone, and if necessary in person for all IT departments and for other concerned top level management. He also described that, cyber-attack analysts have the role to respond for information security incidents in collaboration with other IT department staff members. All interviewees explained that, those caseswhich are reported as a low impact incident used to be handled by IT technicians.

- The general incident response process handled by security operation center cyber-attack analysts which are derived from a description given during interview illustrated by figure 4.1 below.

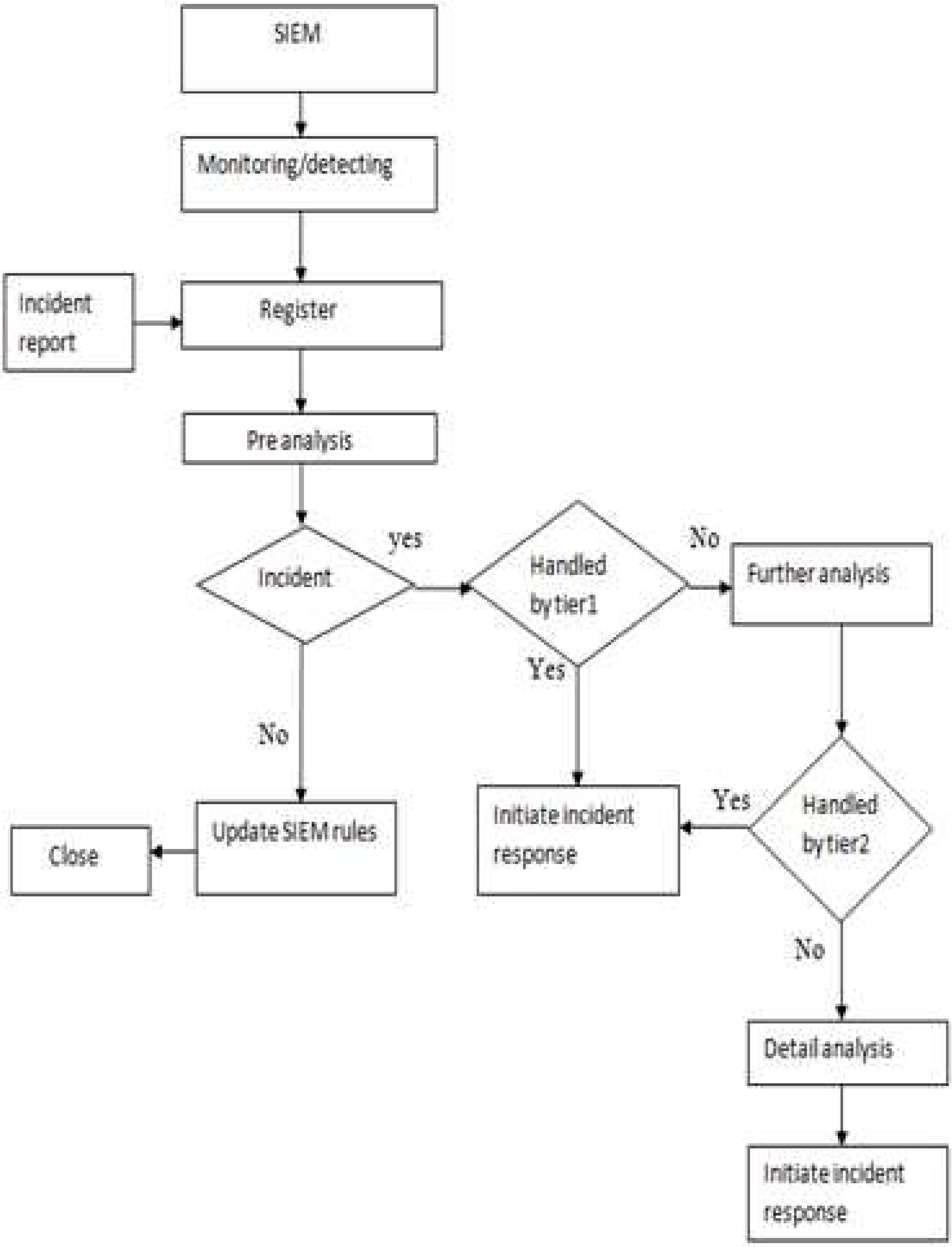


Figure 4.1 work flow for general incident response at SOC

Steps for general information security incident response at security operation center as represented by fig 4.1.

- Monitoring team monitor security events, detect incidents using SIEM in 24/7.
- Verify incident occurrence by collecting and analyzing security events.
- In case of incidents, register the case. Otherwise change the detection rule of the monitoring system.
- If incident can be handled by tier 1 cyber-attack analysts, then initiate specific incident response. If not send it to tier 2 cyber-attack analysts.
- Tier 2 cyber-attack analysts perform further investigation and analysis on incidents and if they are able to resolve it, they initiate specific incident response. Else, they send it to tier 3 cyber-attack analysts.

Interviewee were asked as to whether bank x experienced information security incidents recently. The security manager described that, Bank x has experienced information security incidents which are categorized as low, medium and high impact level. For instance: various infections or malicious software, high level access requests of services , temptation to harvest email addresses by accessing vulnerabilities and others. Recent information security incident they have experienced was ransom ware attack named by Wannacry. He said that, it is a network based attack which was very fast to propagate itself. They detected it earlier before the actual attack is coming using correlation from security information event management system and antimalware software. It took them few days to contain it. The vulnerability of those computing devices with Microsoft product operating system was exploited. Especially of those which were not patched.

He said:

"… The response was successful even though it has delayed to contain it."

He described that, in order to stop the attack, they have identified the port it was using to spread itself and they disabled it .moreover they fixed the security hole that was exploited by WannaCry. He highlighted that it was time and labor intensive to avoid and clean it from their system. The security operation center team leader has agreed with what the security manager said and he said:

"…WannaCry was not successful to ask ransom but it could stop our entire work…if we were not able to detect it early."

The ATM and e-payment manager pointed that, May 2017, worldwide attack WannaCry infected many computing devices including ATM in their bank. He stated that, a number of automated teller machines were out of service during the attack. He highlighted that two things were the reason for the attack. Antivirus was not enabled in some automated teller machines and in most cases their operating system was not patched. He stressed that it was time and labor intensive to get fixed their infected automated teller machines.

He said:

"It was a source of our customers complains until we fixed and clean all infected tailoring machines."

Electronic evidences preserved at bank x in case of need for future investigation. All interviewees mentioned that, department of IT audit uses automated tool to trace back and follow logins of employees which could be referred to it when it is necessary. If the security incident has an intention of fraud, bank x works in collaboration with police for further forensic investigation and legal evidences.

**Lesson learned**

The security manager stated that, they review incidents based on the report from security operation center in a weekly, monthly and quarterly meetings. They discuss about: how security incidents dealt, root cause to prevail, what gap they need to consider for future risk assessment and other additional issues about security incidents. The security operation center team leader also gave similar explanation. The infrastructure and application manager stated that they learn from past incidents to make sure re occurrence of security incidents avoided. Sometimes, they take part in the discussion with security department to share ideas about how they resolved security incidents and what challenge they have faced. He said, lack of awareness among employees is one of the challenges they identified after post incidents are facing. The ATM and e-payment manager has agreed with what the infrastructure manager described.

He said:

"It is very challenging to deal with users who are not information security sensitive."

Interviewees agreed that,Bank x share experience of handling information security incidents with the national CERT. All interviewees pointed that the need for other financial sectors and banks to give priority for managing information security incidents. They want to share their security operation center working environment as a good practice for other banks. The ATM and e-payment manager described that. Similar banks like ours should share experience of handling information security incidents to benefit from it for future security incident management. He said that, we might share ideas about preventing incidents. For example, there are some banks in which they enabled magnetic strip in using card banking. But magnetic strip can easily be copied and may lead them to face fraud in using card banking. This will be a cause for reputational damage. So it is advisable to stop enabling magnetic strip in card banking or they need to assess their risk appetite

He said:

"We need to share our challenges and success in managing security incidents with trusted community who works for the same purpose. Business competition can remain as it is but banks can benefit from common agenda to prevent security threats,"

### 4.4.2. Data from E-mail interview

Most of the survey participant agreed that bank x performed information security training in cooperation with local training centers and international companies. Among 7 of the participant 5 of them mentioned that, the security operation center cyber-attack analysts and other IT staff members take part in the training. One of the respondent said that the training which is conducted to address security issue should include business staffs as well. Respondents pointed that awareness program conducted using the bank intranet, portal and information security magazine. 4 of the survey participant mentioned that information security awareness among employees is not matured. One of the cyber-attack analysts mentioned that:

"Some employees are unhappy when you tell them not to use unknown USB sticks in working environment."

All of the respondents assured that bank x never performed emergency preparedness exercise to test information security incident management schema. One of the survey participants said that:

” we can’t think of rehearsal while we even don’t have working incident management plan which is recognized by all concerned staffs.”

Almost all of the survey participant described that, IDS ,IPS, antivirus, network flow analysis and security information event management system are currently in use as prevention and detection of information security incidents in their bank, three respondents mentioned that employees also detect information security incidents and ask support.

Several of the survey participants reserved from replying for the question that asked them to explain major and recent information security incidents their bank experienced. But two of them described that ransom ware attack WannaCry was a recent information security incident their bank experienced. One of the responses tells that there was a delay to respond properly for the attack and they both agreed that a number of computers were infected by WannaCry. Many of IT staffs were busy to resolve the problem.

The majority of the respondents explained that email and phone are means of communication which are in use widely at bank x for reporting information security incidents. 3 of the cyber-attack analysts mentioned that they are unsure about logging of all security incidents identified using different sources. But all of them agreed that those identified using monitoring tools logged properly in ticketing system.

When asked what major challenges their bank is facing in responding to information security incidents, they pointed to various issues. 4 of the participants mentioned that information gap among departments is a challenge and 3 of the respondents revealed that response delay and awareness of employees towards information security is another challenge for handling security incidents. Enhancement of new threats is also among the challenges they have noticed, which is described by 5 of the survey participant. One of the cyber-attack analysts said:

” because it needs various in-depth skills to analyze sophisticated new threats, it is challenging to respond for it. A zero day attack is also a challenge to respond for it right away.”

## 4.5. DISCUSSION

### 4.5.1. HowDoes Bank X Of Ethiopia Perform Information Security Incident Management?

Several international standards pointed out that the importance of having an information security policy for an organization .ITIL, ISO and SAN stated that information security policy should be communicated throughout the organization and employees have to familiar with the policy. Bank x has developed an information security policy though it seems it is not well established across the entire branches of the bank. This is supported by the interviewees where the infrastructure and application manager stated that, it is very difficult to deal with those employees who are not information security sensitive.ATM and E-payment manager also agreed with that, some employees lacks knowledge about what they are allowed to do and not to do. Bank x is not compliant with ISO/IEC 27035 standard recommendation of having a specific policy for handling information security incident .All the interviewees agreed on that there is no separate policy and plan that only address information security incident management at Bank x.

Bank x classify information assets depending up on their sensitivity and value .supported by all interviewees. It is compliant with recommendation from the ISO/IEC 27002 standard that additionally emphasizes the relevance of information classification to ensure proper protection of information. The three company studies by Hove and Tarnes (2013) all classified information including classification of incidents based on the severity and damage they cause. Bank x also classify incidents for proper management depending up on their risk. Participant of the interview stressed on that classification of incidents is vital for proper incident handling process.

A finding from the study of Joatun et al (2009), Identified the need for a short and common plan for incident response. In the study of Hove and Tarnes(2013), all the three Norwegian companies had incident management plan in some form, This included plans and guidelines for handling specific types of security incidents, established routines, and plans for communication during incidents. This supports that the finding bank x has incident handling procedure though it is not approved by top level management. The security manager and security operation center team leader mentioned that, they have incident handing procedure in which they use it without gaining approval from management. This might indicate there is lack of common understanding among technical IT staffs and management staffs towards incident handling, we believe that it is an alarming finding as it tells bank x have no formal and clearly defined document that will guide incident handling process during incident occurrence.

The establishment of IRT is highlighted in standards and guidelines. NIST recommend that team members have to have diverse back grounds so that they can handle different incidents that occur. According to NIST, usually teams consist of highly technically skilled persons and teams should have at least one member with expertise in each major technological category. Participant of the interviewee at bank x assured that security operation center workers acts as an incident response team and they work in collaboration with  other IT staffs when it is needed, But ISO/IEC 27035 standard recommends having a permanent response team. Bank x don't comply with this recommendation as they don't have their own IRT but dedicated IT staffs and security operation center cyber-attack analysts for incident handling. This finding is similar with the finding of Ahmad et al (2012) at financial organization; the response to high impact incidents is coordinated by a high impact incident response coordination team, while other incidents are handled by a network incident response team more independently. Companies construct teams based on the incident and one of them has a specific team that is involved for major incidents.

Bank X conducted training and awareness creation program thataddresses various security issues. According to ISO/IEC 27035 standard, employees' awareness and participation in incident management procedures are important. Even though employees at bank x had attended courses or other awareness raising activities, there is still a room for improving security knowledge and awareness in order to create security positive environment. This observation is further supported by statement from infrastructure and application manager. He mentioned that it is very important to address the need of IT staffs and other employees to take part in security related training as information security incident handling process can't be only the responsibility of security operation center workers. This is similar with the finding from the study of the petroleum industry by Joatun et al (2009) that identified individual awareness related to information security should be improved.  Bank X never used rehearsals to identify areas of improvement yet. Conducting emergency preparedness exercise is however considered challenging; it ensures that participant train on the right things, that the scenario is realistic and useful for real situations. The security manager stated that it is difficult to conduct rehearsal and they never considered its importance. He stressed that it is not a good practice to keep incident handling procedure without checking its functionality. Bank x is not compliant with the recommendation of ISO/IEC 27035 standard to conduct rehearsal.

As it is recommended by most relevant standards and guidelines, bank x has implemented monitoring systems such as IDS/IPS, SIEM system, antivirus solutions, firewalls in which they have configured monitoring functionalities, DMZ, network flow analysis, mail monitoring tools and other security monitoring tools are in place and use, the tools currently in use however have their limitations. The security manager described the fact that high rate of false positive alerts from security information event management system is one of the challenges in using automated monitoring systems. Study by Werlinger et al (2010) also revealed that a lack of accuracy in tools, resulting in high false positive rates. Furthermore interviewees mentioned that the challenge to  hire senior cyber-attack analysts who can investigate and analyze sophisticated correlations makes a concern usability of tools. It is notable that efficient detection often requires intimate knowledge about the organization systems and services. Complexity and lack of properly trained security specialists may lead to rely on notifications to detect incidents. The finding from the study by Koivunen(2010) also showed that, of the incidents studied, none of the victims of the security breaches seemed to have discovered the incident on their own.

Notification of incident might be from users, IT employees or external third parties. Bank X uses email and phone to notify and report incidents which are detected manually. Even though bank x have ticketing or incident tracking system where incidents to be registered, the security operation center team leader stated that they were not exhaustively logging information security incidents which are reported manually. Commonly reporting channels mentioned at bank x were security manager, security operation center workers and immediate IT support staffs. Cyber-attack analysts who participated on the survey revealed that, there is no dedicated form for reporting information security incidents identified by users manually, so that the user can register what they have observed. Out of 7, 5 of the survey participant said this.ISO/IEC 27035 standardrecommends report that comes from any sources should be filled in a separate format and has to be approved by point of contact. Bank x doesn't comply this. Some studies report on challenges with having all incidents registered in the system.Cusick and Ma(2010), report that some issues are observed but not logged, typically when the case is considered to be non-critical. We believe that lack of proper communication might be the root cause of challenges with having all incidents registered. The case study by Hove and Tarnes(2013) included a survey of regular employees, it was found that few of the employees knew to whom  security incidents should be reported and that they were not sure which incidents to report.

According to ISO/IEC 27035 standard recommendation, the point of contact should conduct an assessment to determine whether the information security event should be classified as information security incident or is in fact a false alarm. Assessment may be also conducted by the person who identified the security incident, if he/she has the appropriate level of competence to determine whether the security event is an incident or false alarm. This is supported by from the statement of security manager and security operation team leader.

Though it is time taking for them to determine whether an alert is false positive or not, bank x'scyber-attack analysts perform assessment of security events using monitoring tools. This complies with ISO/IEC 27035 standard recommendation.

Bank x works in collaboration with third parties like INSA and national CERT in order to tackle some advanced attacks. It is in compliance with ISO/IEC 27035 recommendation. Another issue highlighted in the standard is forensic investigation; they work together with police if further forensic investigation is needed. This is supported by the study Hove and Tarens (2013), companies in some cases rely on third parties or the police for forensic investigation.

Post incident activities of bank x includes, conducting weekly, monthly and other additional meetings to review the cause of major incidents, The challenges they face and how it dealt with to respond for it. The security operation center technical staff team leader and security manager together with risk and program assessment staffs take part in the discussion. This is supported by participant of the survey and security manager. He stated that they have regular meeting to discuss on security incidents so as to incorporate the output from the discussion for further risk assessment tasks. It is similar finding as Werlinger et al(2010) reported the motivation for performing learning activities include keeping security practitioners updated on current threats, getting new ideas on how to resolve challenging incidents, discussing possible improvements of the incident management process. It complies ISO/IEC 27035 recommendation.

Experience sharing with trusted communities is a recommendation in most standards as post incident activity. It seems lesson learnt and other incident information is often available only to some selected few in Bank x. this is supported by survey conducted at bank x. among the 7 participant 4 of the cyber-attack analysts stated that, information gap among departments is one of the challenge for incident handling in their bank. We believe that sharing experience can make banks better prepared for incident handling. The ATM and E-payment manager noted that: it has to be clearly defined to which group they can share experience. He said that, I don't think that, it is necessary to make unavailable those important experiences, we identified in handling security incidents for trusted communities. This may imply that bank x is not benefiting from mutual sharing of experiences with other banking industries. So it is only partially compliant with ISO/ IEC 27035.

### 4.5.2. What challenges exist in information security incident management at bank x of Ethiopia?

Challenges for security incident management were mentioned by interviewee and the survey participant. Among these, limitation of having experienced incident handlers, lack of employees awareness, and too much false positive alerts are highlighted by all of them. cyber-attack analysts pointed out that, information gap among departments, response delay which also supported by statement from security manager, enhancement of new threats and network connection problem especially from internet service providerare challenges for incident management practice at bank x. a study by Kurowski and Fring (2011) reported that the professional experience of employees is most relevant for performing analysis of incident followed by documentation of past incidents.

## 4.6. Chapter Summary

In the chapter, the data gathered from the participant of this study was presented and assessed using ISO/IEC 27035 information security incident management process guide. The data analyses and findings from this research discussed. The gaps and challenges for information security incident management practice at bank x also identified. The next chapter will present summery of key findings, conclusion, recommendation .limitation and future work of this research. .

# CHAPTER FIVE

## SUMMARY OF KEY FINDINGS, CONCLUSION RECOMMENDATIONS AND FUTURE WORKS

### 5.1. Summary of Key Findings

Systematic approaches to incident management activities contribute to respond successfully for an incident. As it is described in many of international standard and good practices, information security incident management policy, plan and procedures are part of an organization incident management capability. Bank x don’t have a separate information security incident management policy and plan that could help them to respond for incidents in an organized and better way from what it is practical currently.

The majority of this research participant revealed that the security operation center cyber-attack analysts are playing the role of an incident response team together with few focal persons in other IT departments. But cyber-attack analysts who participated in the survey pointed out that information gap among departments and response delay are notable challenges that affect incident management practice at bank x. this may indicate that the collaborative effort to respond for an incident is not satisfactory at bank x. it seems this finding call for establishment of well-organized and comprehensive incident response team.

Besides, an incident response is a highly collaborative activity, the skill and experience of incident responder and usability of security tools are an issue for the diagnosis work. Experience of incident handler can be achieved in two ways, through rehearsal and post incident learning activities. It is not a good practice to wait for an incident occurrence to learn from it, rather it is recommended to conduct scenario based rehearsal to enhance incident responder experience and to identify gaps to be managed beforehand. The finding of this research is indicating that bank x don’t perform rehearsal. This might have certain connection with the fact that bank x is suffering from lack of highly skilled and experienced incident responders.

In order to create security positive environment, it is believed that training and awareness creation program plays a vital role. Training is a common key factor for an organization to strengthen their response capabilities. The participant of this research indicated that bank x provide information security incident handling training for IT and control center workers. They also mentioned that their bank conduct information security awareness creation program for business staffs. On the other hand, most of the interviewee and the survey participant highlighted that lack of information security awareness among employees is a challenge for information security incident management practice at bank x. this may lead us to the conclusion bank x is not performing training and awareness program in an effective and efficient way to create security positive environment.

Apart from the limitation regarding usability and accuracy problem they have, automatic monitoring and detection systems are best suited for detecting known attacks. Manual detection mechanisms such as users, technical staffs and external notification supplement the limitation of automatic detection mechanisms such as, a problem of detecting new attacks which are specifically tailored and targeted. According to the participant of this research, Bank X widely implemented globally well-known and internationally recommended automatic incident detection mechanisms. We believe that, that deployment of a separate security operation center at bank x, which is first of its kind in the country indicates that undeniablecommitment of top level management to secure their IT infrastructure. This is supported by from the statement of almost all participants in the interviewee. Bank x also uses manual detection mechanisms to detect incidents but there is a grey area which indicates utilization of users as a sensor network for the bank is not sufficient. This is supported by the description of interviewees that pointed out, the absence of security incident registration form for users to use it, uncertainty about logging security incidents in the incident tracking system and lack of awareness.

Challenges of information security incident management at bank x identified in this research are:

- Accuracy of monitoring tools.
- Lack of skilled and experienced incident handlers.
- Lack of security awareness among employees.
- Information gap among departments and
- Enhancement of new threats.

## 5.2. CONCLUSION

The main objective of this research was to assess the current practice of information security incident management at bank x of Ethiopia, using international standard in identifying the gaps and proposing possible solution.

In this study, attempts were done to examine and compare the available international standards and guidelines to use it in comparing with the current practice.Qualitativein-depth study was used to assess practice of information security incident management at bank x.

The research pointed out that to what extent existing standards and guidelines are adopted in bankx's information security incident management process. We found that bank xhas not a predefined and separate information security incident management plan in which they follow it strictly. But, to some extent they are compliant with an international standards and guidelines recommendation like ITIL and ISO. Some procedures such as incident classifications and escalation of incidents seem to be well performed. Automatic means of detecting information security incidents is widely implemented. There are also procedures and activities don't seem sufficiently established. Such as, collaborative work, incident reporting process, training and awareness program, manual incident detection mechanisms, post-incident activities like sharing of experience. Moreover we highlighted that, an alarming finding that rehearsal never been practical and not gained anyone's attention at bank x.

Challenges in handling incidents at bank x were also reveled in this study .these challenges were related to employees awareness, lack of skilled incident handlers, communication and enhancement of new threats.

## 5.3. LIMITATIONS

- As the topic of the interviews was information security, which tends to business confidential information,some interviewee Participants may refuse to speak against their bank. Their conscious or unconscious desire to make their bank and themselves look good from the outside could cause a certain bias.
- Even though the researcher impression was to interview more business staff personnel and IT technical staffs from each categories, the sensitivity of the research topic, Time and resource constraints put a limitation on the number and selection of interviewees. A bigger sample would probably enhance the reliability of the research.

- Interviews and documentation were intended to provide two different views on incident management, confidentiality issues prevented bank x from sharing documentation. As information security researchers we should appreciate such caution regarding sharing of confidential documents, although it poses limitations to the data triangulation.

## 5.3. RECOMMENDATION

We believe that, having systems in place to prevent and detect as many breaches as possible may be a good starting point of incident response. Today's threat landscape also requires a detailed incident response strategy to detect and respond to a breach, along with the expertise to execute it .based on the identified current practice and challenges of information security incident management at bank x, we recommend the followings so as bank x and other organization may use it for a better way of managing information security incidents.

1. The management of bank x have to work together with IT department, so as sound and comprehensive standards or guidelines for information security incident management will be used recently.
2. As soon as possible, IT department together with the management, they have to produce information security incident management policy and plan in order to ensure that information security incidents are reported, assessed and their harmful effects are mitigated.
3. The management together with IT department have to establish an incident response team that consists representative from
    - Technical security specialists.
    - Information technology specialists from each category.
    - Relevant business staffs.
4. IT department have to produce operating and formal procedures for the information security incident response team.
5. IT department together with the management have to design and develop awareness and training programs:
    - The management has to provide role-based educational and training opportunities for Incident response team members and for IT staffs.

- IT department together with incident response team have to expose all employees regularly to information security incident management awareness. The awareness techniques may include periodic emails, posters.
- The management and IT department have to preserve communication with the academic institutions to address training gap

6. The Established incident response team has to conduct regular rehearsal to gain experience. Focus on challenging areas such as response delay, user report procedure, information gap. All IT department members, all Incident response team members, other business employees who have important roles have to take part in emergency preparedness exercise .
7. All IT department members and the management have to encourage an environment to share information about incidents that could involve colleagues.
8. Incident response team and all members of IT department have to make sure employees are fully utilized as means of detecting incidents.
9. The management and IT department have to produce formal policies on which means of information communication should be used and what should be disseminate and who should access it.
10. Incident response team have to enhance post incident activities:
    - Focus on the effectiveness of procedures, controls, training and awareness.
    - Share notable experiences with similar trusted financial industries and communities.

## 5.4. FUTURE WORK

In order to cope with the enhancement of new threats, we believe that, conducting more detail researches benefits banks and other organizations. The researcher recommends future studies in the following area:

- Conduct the same detailed study on a large scale with in financial industries and other organizations.
- How the identified challenges can be resolved.
- The need for tailored information security incident management frame work for different organizations.

- Prospects and challenges of academic institutions in minimizing the scarcity of highly qualified information security personnel.

# References

Asnake,T.(2016).*Tailoring IT governance framework for national bank of Ethiopia*.(unpublished master's thesis).Addis Ababa University, Addis Ababa,Ethiopia.

Ahmad,A.,Hadgkiss,J., and Ruighaver,AB.(2012).Incident response teams: challenges in supporting the organizational security function. Computer & security

Berhanu,N.(2017).*Assessment of IT Disaster Recovery Practice in Ethiopian Commercial Banks*.(unpublished master's thesis).Addis Ababa University, Addis Ababa,Ethiopia.

Beck,C.T.(2003).Initiation in to qualitative data analysis. *Journal of Nursing*

Campbell,D,T&Stanley,J.C(1963).Experimental and quasi-experimental designs for research. Chicago: Rand McNally.

Cassell,C. and Symon,G.(2004).Essential guide to qualitative methods in organizational research. sage publication Ltd.

Cusick,S.,MaG(2010)."creating an ITIL inspired incident management approach: roots, response, and results." In :Network Operations and Management Symposium Workshop(NOMS Wksps), IEEE/IFIP;2010.pp142-8.

Denzin,N.K.(1970).The research act: A theoretical introduction to sociological methods. Chicago: Aldine publishing co.

Diefenbach,T.(2009)" Are case study more than sophisticated story telling?: methodological problems of qualitative empirical research mainly based on semi-structured interview. vol.43,no.6,pp.875.

Endale,A.(2017) *Challenges In Relation to Business Continuity Management in*

*Commercial Bank of Ethiopia: Information System Security in Focus*.(unpublished master's thesis ).Addis Ababa University, Addis Ababa, Ethiopia.

ENISA.(2011).Good practice Guide for Incident Management.

ENISA .(2008).A basic collection of good practices for running a CSIRT.

Ernest,B.,Richard,G., Aidan,L.,andJohn,.S(2012). IT Service Management: A Guide for ITIL Foundation Exam Candidates. BCS, The Chartered Institute for IT, 2nd ed

George.G.,Willian.B.,Tim.S,(2014)"Rethinking Security Incident Response: The Integration of Agile principles," in twentieth Americas Conference on Information systems.Savammah.

George.G.,William.B.,David.B.,Tim.S.,Stacy.M,(2017). "Security Incident Recognition And Reporting: An Industrial perspective, "in: twenty-third American Conferences on Information Systems. Boston

Grispos,G., Bradley,G.W,Storer,T.,"Security Incident Response Criteria: A practitioner's perspective."

Hove.C.&Tarens.M(2013).Information Security Incident Management: An Empirical Study of Current Prac.

ISO/IEC 27000: 2012(E).Information technology-security techniques-information security management systems-overview and vocabulary. Second edition, International Organization for Standardization.

ISO/IEC 27035:2011(E). Information technology - Security techniques - Information security incident management - First edition. International Organization for Standardization.

ISO/IEC, \ISO/IEC 27000:2009 Information security management systems – Overview and vocabulary,".

Jaatun,MG., Albrechtsen,E.,Line,MB.,Tondel,IA.,Longua,OH.(2009). A framework for incident response management in the petroleum industry.Itjcritinfrastruch; 2:26-37.

Kaspersky.(2013)." Global Corporation It Security Risks:2013."

Kelver,J.(2002).Incident Response in a Global Environment. GSEC version 1.2b, SANS.

Koivunen ,E.(2010).” Why wasn’t I notified: Information Security Incident reporting demystified.” in 15th Nordic conference in secure IT systems(Nordsec 2010).

Kothari (2004). Research methodology methods and techniques (2nd edition ed.). New Delhi :new age international.

Kurowski,S.&Frings,S. computational documentation of IT incidents as support for forensic operations.

Le compte,M.D., and Schensul,J.J.(1999). Analyzing and interpreting ethnographic data. Walnut Creek,CA ;Altamira press.

Le Comple, M.D &Goetz,J.p.(1982).problems of reliability and validity in ethnographic research. Review of educational  Research 52(no1) 31-60

March,Sand.G.Smith(1995). Design and natural science research on information technology, Decision support systems 15,pp. 251-266.

Maria B, L.(2013). A Study of Resilience within Information Security in the Power Industry, IEEE Africon, Mauritius.

Maria,B,L., Inger,.A,Tndel,andMartin,.G, Jaatun(2014).” Information security incident management: Planning for failure,” in: 8th  International Conference on IT Security Incident Management and IT Forensics (IMF) ,Munster, Germany.

Maria B,L., and Nils,B(2015). “Understanding Collaborative Challenges in IT Security Preparedness Exercises,” International Conference on ICT Systems Security and Privacy Protection, IFIP SEC, Hamburg, Germany.

Maria B,L. and Eirik,A. Examining the suitability of industrial safety management approaches for information security incident management, forthcoming in International Journal of Information and Computer Security, ISSN 2056-4961

Maria B.L., Inger,A.,Tndel, and Martin G,J(2014).”Information security incident management: Planning for failure,” 8th  International Conference on IT Security

Incident Management and IT Forensics IMF, Munster, Germany, ISBN 978-1-4799-4330-2.

Michael E.&Herbert J.(2011),Principles of Information Security.

Myers,M.D.andNewman,M.(2007).”The qualitative interview in IS research: Examining the craft,” Information and organization, vol.17,no.1, pp2(26).

Northcutt,S.(1997). Computer Security Incident Handling, step-by-step. The SANS Institute.

Parileh, M.(2002). acquisition through case study development: a student researcher perspective. Communications the AIS 8(8): 360-379

Patrick,K.(2011).Incident Handler’s Handbook. SANS Institute of Information Security.

Paul,C.,Tom,M.,Tim,G.,andKaren,S.(2011). Computer security incident handling guide, NIST special publication 800-61,Revision 2.

Ponemon Institute.(2013a).”2013Global Cost of Data Breach.”

Ponemon(2016).”2016 Cost of Data Breach Study: Global Analysis”, ponemon Institute,p.32.

Pricewaterhousecooper(2014).”The Global State of Information Security Survey 2014.”

Robert K.Yin(2009),Cast Study Research Design and Methods, applied social research method series,5(4) Norwegian University of Science and Technology.

Robson,C.(2011).Real world research,3rded,John Wily & sons Ltd.

Schwarz.A&R.Hirschheim (2003).An extended plat form logic perspective of IT governance: Managing perceptions and activities of IT. *Journal of strategic Information systems* (12): 129-166.

Seltiz,C.&Wrightsman,L.C&Cook,W.S.(1976).Research methods in social relations. 3rded. New York: Holt Rinehart & Winston.

Shedden,P., Ahmad,A.,andRuighaver,A.(2011).”Informal Learning in Security Incident Response Teams.”ACIS 2011 proceedings.37.

Welinger,R., Botta,D.andBeznosou,K. (2007).”Detecting, Analyzing and Responding to Security Incidents: A qualitative analysis,” in :3$^{rd}$ symposium of usable privacy and security, ACM, pp.149-150.

Welinger,R.,Muldner,K.,Hawkey,K., Beznosov,K.(2010).” preparation, detection and analysis: the diagnostic work of IT security incident response.” Information management&   computer security (18), pp.26-42.

# APPENDICES

## Appendix A: Interview Guide

Interview guide (based on ISO/IEC 27035)

1. Which job title or role do you have?

2. For how many years you have worked in this position?

3. Can you explain your major responsibilities in your job?

**Plan and prepare**

4. what does it mean" information security incident" in your understanding?

5. Does your organization have existing plans for information security incident management? Yes/No

6. If yes, are the plans been practical? If not, why not?

7. Is there an already established incident response team in your organization? Yes/No
   If not, why not?

8. Does your organization perform incident management training?

9. If yes, does the training include emergency preparedness exercise?
   If yes, who take parts in such training and how is ICT represented in it?

10. Can you describe available means of incident prevention mechanism in your organization?

11. Can you mention the major types of ICT security incidents your organization experienced?

12. How frequent, information security incidents happen in your organization?

13. Is there any pre-defined down time that can be tolerated for your systems?
    If yes, can you mention?

14. Can you tell me your recent information security incident?
    Was it able to respond successfully to it?
    If yes, do you have any idea to tell about its process?
    If not, why not?

15. If you have never experienced information security incidents, what could be the reason for that?

16. Does your organization classify information security incidents? If yes, can you mention how?

17. Do you use only host-based (anti-viruses) or defense mechanisms that look at network
    Traffic too?

18. Do you encrypt critical data items while in transfer and stored?

19. Do you have network-edge defenses such as IPSec?

**Detection and reporting**

20. What sort of mechanisms you use to detect ICT security incidents?

(Anti-viruses?Intrusion detection systems?Firewalls?Users?Manual audit of logs?)

21. What means of reporting information security incidents are in use in your organization?

**Assessments and decision**

22. How does assessment of identified incident events take place in your organization?

23. Does your organization use predefined incident classification to decide on information security events?

**Response**

24. Who is participant in responding to information security incidents?

25. What sort of challenges you experienced in responding to incidents?

26. Can you describe additional works which are performed when regular operation
is restored?

**Lesson Learned**

27. How are ICT security incidents registered and reported afterwards?

28. Is information on incidents disseminated to end-users?

29.Does information security incidents go through further forensic analysis if required?

30. Are the experiences from ICT security incidents used as input to further risk assessments and improvements of procedures afterwards?

31. Do you have any success practices in relation to information security incident management that you would like to share to others?

32. Which are the most challenging parts of information security management in your organization?

And why?

## Appendix B: E-Interview Guide

1) Does your bank perform incident management training and awareness creation program?

a) If yes, who take part in such training and awareness program?

b) What means of awareness creation program your bank use?

C) if not, do you have any idea about the reason?

2) Does you bank perform emergency preparedness exercise for incident handling?

a) If yes, what are the strengths and gaps identified?

3) What sort of incident prevention and detection mechanisms your bank uses currently?

4) What are the major information security incidents your bank experienced?

5) Can you mention your recent information security incident?

a) Was it able to respond for it successfully?

b) If yes, do you have any idea to tell about its process?

6) What means of reporting information security incidents are in use in your bank?

7) Does your bank register security incidents at all the time?

a) If yes, can you mention who is responsible for that and how its process is?

8) What are the challenges your bank experienced in responding to information security incidents?

9) Do you have anything more to tell about information security incident management practice in your bank?