

# Incident Response Procedure

For account compromise

Version 1.2 2004





## Table of contents

1.0	Introduction.....	1-1
1.1	Audience.....	1-1
2.0	Executive summary .....	2-1
3.0	Incident definition .....	3-1
3.1	Incident classification.....	3-2
3.2	Incident severity level .....	3-5
4.0	Incident response framework .....	4-1
4.1	Preparation .....	4-2
4.2	Identification .....	4-6
4.3	Assessment .....	4-8
4.4	Containment .....	4-8
4.5	Eradication.....	4-9
4.6	Recovery .....	4-9
4.7	Follow-up .....	4-10
	Appendix A: Incident Response Contact List.....	A-1
	Appendix B: Incident Response Checklist .....	B-1
	Appendix C: Incident Reporting Form .....	C-1
	Appendix D: Visa Incident Escalation Form .....	D-1
	Appendix E: Incident Response Framework Flow-chart .....	E-1



## 1.0 Introduction

This document has been developed for all entities (e.g. merchants, processors etc.) that process, store or transmit Visa account and transaction information. It provides all the relevant information and steps required to develop and implement effective security response procedures, to be executed in the event of a security incident relating to Visa account and transaction information.

The risk of theft or data compromise continues to increase. As 100% security cannot be guaranteed, it is necessary to have an incident response plan in place that is tailored to your business environment to minimise disruption or losses to business operations in the event of an incident.

Whilst this document defines the steps needed to develop and implement effective security response procedures, adhering to the appropriate security standards as defined in Visa's *Account Information Security (AIS) Program*<sup>\*</sup>, the risk of security incidents occurring should be minimised.

### 1.1 Audience

The document is intended for all entities that handle Account and Transaction Information, and includes:

- (a) Third-party service providers
- (b) Merchants: face to face (retail), Mail Order/ Telephone Order (MOTO) and e-Commerce
- (c) Internet Payment Service Providers (IPSP's) or payment gateway providers.

---

<sup>\*</sup> Visa's AIS Program encompasses all aspects of data security related to the protection of Visa cardholder account and transaction information. The AIS Standards define minimum requirements for protecting such information. All entities that handle Visa account and transaction information must ensure they meet the AIS Standards. Contact your Acquirer or visit [www.visa-asia.com/secured](http://www.visa-asia.com/secured) for more information on the AIS Program.



## 2.0 Executive summary

In today's fast-moving technological world, having security features on internal networks is no longer sufficient to protect or shield your company from intrusion attempts, either internal or external. It is essential for your organisation to have a well-defined and systematic procedure to respond to security-related incidents. This ensures you are adequately prepared to respond and recover from incidents that may potentially disrupt critical business processes.

This document explains the importance of developing an incident response plan through a well-defined incident response framework. The framework comprises seven phases that ensure a consistent and systematic approach in handling such incidents. The details for each of the seven phases is summarised below:

### Phase 1 – Preparation

In any incident response plan, it is essential to form an Incident Response Team ("IRT") prior to other tasks. The role of the team is to promptly handle an incident so that it will have minimal impact to the business operation. The team is formed of members from various functional roles in your organisation. The process of setting up the team is explained in section 4.1.

### Phase 2 – Identification

The occurrence of an incident is unpredictable. An anomaly in the system behaviour may indicate an incident or configuration errors. Hence, identifying an incident amidst routine daily operations is not an easy task. In section 4.2, some guidelines are provided to facilitate the process of positively identifying an intrusion incident.

### Phase 3 – Assessment

After the identification phase, an initial assessment should be performed to confirm the existence of the incident. The assessment should include determining the scope, the impact of the incident, and the extent of the damage caused by the incident.

### Phase 4 – Containment

Containment of the incident is necessary to minimise and isolate the damage incurred by your Company. In section 4.4, some guidelines are provided to help determine the appropriate course of action for limiting the extent of the incident.

### Phase 5 – Eradication

In order to successfully eliminate the incident, the IRT need to determine the cause of the incident that resulted in the compromise of the system. The implementation of the eradication process is explained in section 4.5.



### **Phase 6 – Recovery**

The recovery phase restores operations of the compromised system to facilitate the resumption of normal business operations. Prior to the resumption process, a validation check should be performed to ensure that the system is secured against any repeated incidents. Furthermore, the system should be placed under surveillance to ensure that if the perpetrator returns, unauthorised attempts may be detected early.

### **Phase 7 – Follow-up**

As a follow-up, you should perform a post-mortem analysis of the compromised system to understand the weaknesses that resulted in the incident and other potential vulnerable areas. In the event that the Company is considering legal action against the perpetrator, it is recommended that forensic specialists and/or law enforcement agencies should be engaged to ensure that digital evidence are accumulated and preserved in a manner that is consistent with the legislative requirements.

In addition to this, for “Extreme” and “High” severity incidents (as defined in section 3.1.2), an onsite review must be performed by a Visa qualified security assessor. This review is required to validate your company’s compliance with Visa’s *Account Information Security (AIS) Standards* (as defined above).



### 3.0 Incident definition

Before any discussion on the incident response framework, it is important to establish the definition for a security incident. According to CERT/CC\*, a security incident can have the following definitions:

- (a) violation of an explicit or implied security policy
- (b) attempts to gain unauthorised access
- (c) unwanted denial of resources
- (d) unauthorised use of electronic resources
- (e) modification without the owner's knowledge, instruction, or consent.

In the context of this document, the term "security policy" in the first definition refers to the security policies in place to protect account and transaction information. These security policies, should be in-line with the 15 standards that comprise Visa's *Account Information Security (AIS) Standards*. All Visa Members, Member agents, and merchants must adhere to these standards to effectively protect account and transaction information.

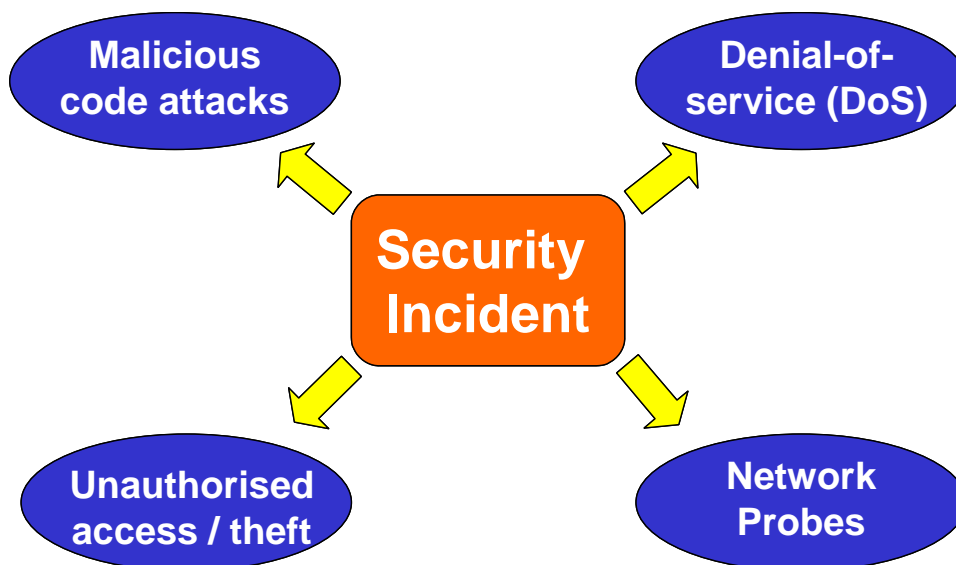
As an illustration, one of the security requirements in the AIS is to ensure that all vendor-supplied default system passwords should be changed. There are many websites that publish default passwords for many vendor products. One of the websites is <http://www.astalavista.com>. If an intruder compromises a router using its default password obtained from the above website, an incident has occurred. Using the compromised device, further exploits may be launched against other systems or network devices in the IT infrastructure.

---

\* The CERT Coordination Centre (CERT/CC) at <http://www.cert.org>

### 3.1 Incident classification

A security incident can be classified under the following categories as shown in figure 1 below.



**Figure 1: Categories of security incident**

#### Malicious code attacks

Malicious codes can be programs such as viruses, worms, Trojan application, and scripts used by intruders to gain privileged access, capture passwords or other confidential information e.g. user account information. Malicious codes attacks are usually difficult to detect as certain viruses can be designed to modify their own signatures after inflicting a system and before spreading to another. Some can also modify audit logs in order to hide unauthorised activities.

The following are some examples of malicious code attacks:

- (a) Worms or viruses rapidly spreading through emails (e.g. I Love You, Melissa Virus)
- (b) Spying codes (e.g. Caligula Virus, Marker Virus, Groov Virus)
- (c) Remotely controlled codes (e.g. Back Orifice, NetBus), and
- (d) Coordinated attack codes (e.g. Trinoo, Tribe Flood Network (TFN)).



### **Denial-of-Service (“DoS”)**

DoS attacks refer to the use of specific tools by intruders to cause networks and/or computers to cease operating effectively or to erase critical programs running on the system. Currently, distributed DoS attacks are becoming prominent where a team of intruders located in various geographical locations launch simultaneous attacks on a victim host. It is generally difficult to trace the source of distributed DoS attacks as perpetrators could launch the attack through multiple different gateways before reaching the victim host. In a DoS attack, DNS, web, and mail servers are the most likely targets.

A DoS attack may not be a direct cause of account compromise however may be a warning signal for future attacks.

Some examples of DoS attacks are:

- (a) Email related DoS (e.g. mail SPAM, mail bombs)
- (b) Service related DoS (e.g. Slammer Worm, Chargen DoS), and
- (c) Network jamming DoS (e.g. SYN flood DoS, 'Ping of Death' DoS, Smurf DoS).

### **Unauthorised access / theft**

Unauthorised access ranges from the unauthorised usage of logon credentials to the tampering of files and directories stored on a system or storage media. It could also entail access to additional computer systems by planting an unauthorised “sniffer” program or device to capture confidential information traversing the network. Most e-Commerce merchants use Secure Socket Layer (SSL) to protect web transactions over the Internet. SSL provides server authentication, data encryption and message integrity. Without SSL, most web transactions, including credit card transactions, would travel across the internet in the clear, which is susceptible to network sniffing i.e. the information could be copied, modified or deleted.

Internal compromise continues to be the most common and most damaging method of stealing sensitive information. Organised crime groups now actively recruit employees of organisations that process high volumes of account information to steal account and transaction information.

The following list is some examples of unauthorised access:





- (a) Employees stealing confidential information
- (b) System access by using user IDs belonging to ex-employees
- (c) Unauthorised access by using user IDs that have administrative access rights
- (d) System access by using special purpose IDs that are no longer required or use weak passwords, and
- (e) Unauthorised access by exploiting vulnerability in the company's information systems, routers or firewalls.

#### **Network reconnaissance probes**

The objective of performing reconnaissance probes against a Company is to gather information on its network infrastructure. A probe can consist of two natures - host discovery and service ports discovery. Host discovery will determine all active systems in a network, which includes performing Operating System ("OS") fingerprinting while port discovery will gather information on the services running on the systems.

A network probe attack may not result in an account compromise however may be a warning signal for future attacks.

There are many tools available on the Internet for performing these probes such the following examples:

- (a) Host discovery (e.g. Ping sweep, directed broadcast pings, SYN-FIN scans), and
- (b) Service port discovery (e.g. TCP port scan, UDP port scan).

### 3.2 Incident severity level

Once classification of the incident has occurred, the severity level of the incident can be determined. The severity level of the incident will dictate the course of actions that should be performed to resolve the incident. The following five severity levels may be assigned to the incident:

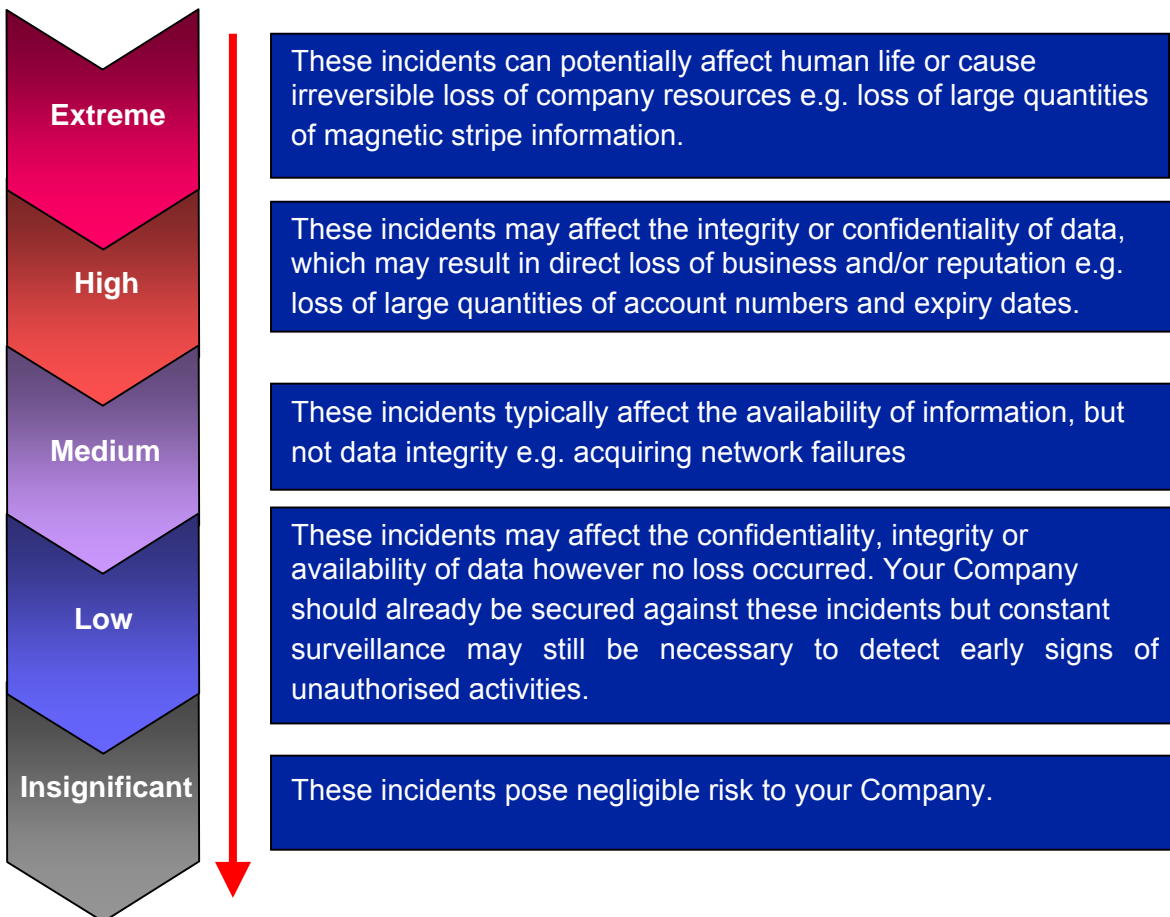


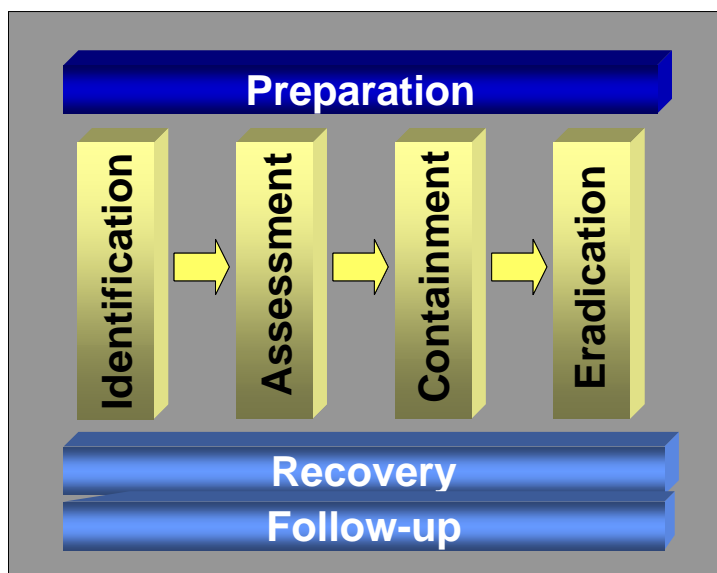
Figure 2: Severity levels of an incident

**Your Acquirer and Visa MUST be advised of any “Extreme” or “High” severity incidents.**

## 4.0 Incident response framework

The objective of an incident response framework (illustrated in Figure 3) is to provide a systematic approach in developing an incident response plan. A well-defined incident response plan will enable you to handle any incident efficiently and effectively with minimal impact to the business operations. When developing these plans, efforts must be made to anticipate scenarios before they happen, and to make the following decisions in advance:

- (a) Where did the incident happen?
- (b) Which areas of the business processes are affected?
- (c) Who should be notified?
- (d) What are the procedures/actions to be taken?
- (e) How should the procedures/actions be performed?



**Figure 3: Incident Response Framework**



## 4.1 Preparation

### 4.1.1 Incident Response Team

In any organisation, an Incident Response Team (“IRT”) should be made up of senior management and experienced people. The role of the IRT is to promptly handle an incident so that containment, investigation and recovery can quickly occur. The IRT should be empowered by the top management to have decision-making authority for facilitating the incident response process. The needs and resources of the company also play a part in the selection of the team members. The table below shows a list of members who should be included in the IRT and their roles in the team.

**Table 1: Team members in IRT**

No.	IRT Member	Role in IRT
1.	Senior Management	Apart from providing the team the authority for operation, the management has to make business-related decisions based on input from the other members of the team.
2.	Information Security	Assess the extent of the damage incurred and perform containment, basic forensics, and recovery.
3.	IT/MIS	Minimise the impact to system end users, and to assist the Information Security team with technical issues.
4.	IT Auditor	Understand the cause of the incident, ensure procedures are complied with, and work with IT/Security to eradicate the incident.
5.	Security	Assess physical damage incurred, investigate physical evidence, and guard evidence during a forensics investigation to maintain a chain of evidence.
6.	Legal	Ensure the usability of any evidence collected during an investigation if the company chooses to take legal action. The role also includes providing advice regarding liability issues in the event that an incident affects customers, vendors, and/or the general public.
7.	Human Resource	Provide advice in situations involving employees. HR will only be involved in handling the incident if an employee is found to be responsible for the intrusion.
8.	Public Relations	Communicate with team leaders to have an accurate understanding of the issue and the company’s status before communicating with the press and/or informing the stockholders of the current situation.
9.	Financial Auditor	Assess the damage incurred in terms of monetary value, which is frequently required for insurance companies or if the company intends to press charges against the perpetrator.

For small and medium sized merchants/processors one person may assume one or more of these responsibilities. An external party/consultant may also assume one e.g. public relations.

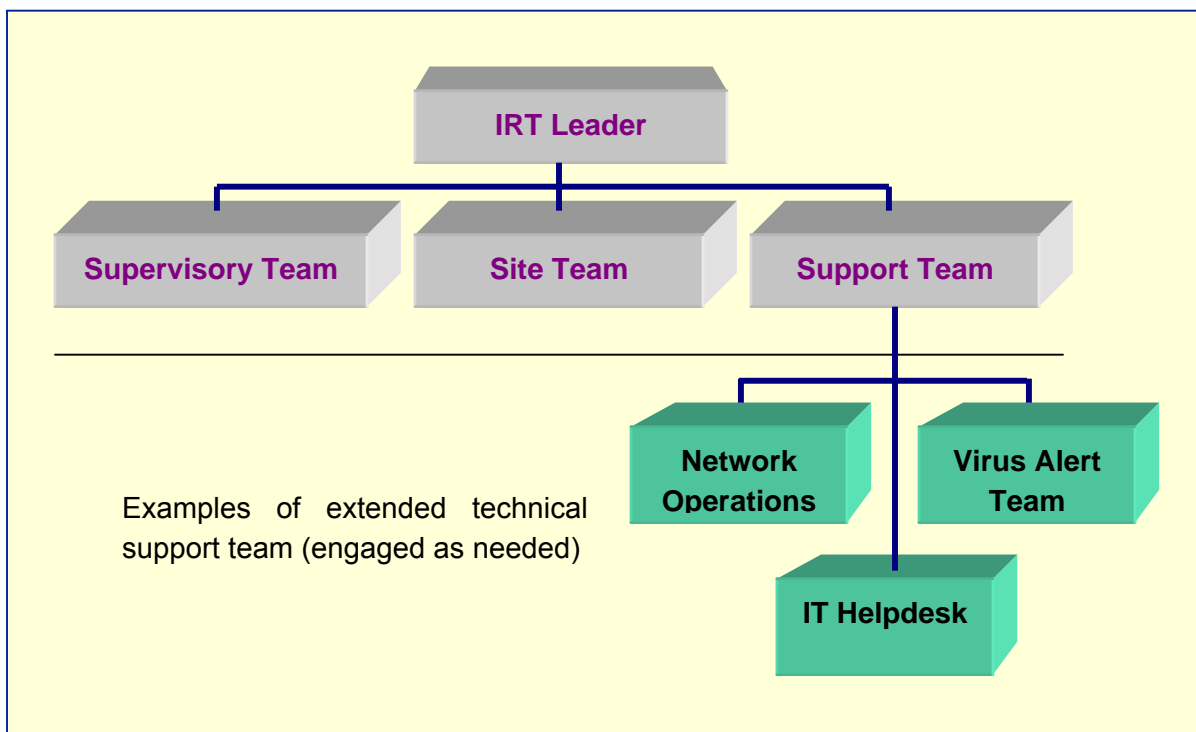
#### 4.1.2 IRT structure

Within the IRT, further division into three sub-teams: the Supervisory Team, the Site Team and the Support Team, may be formed based on the roles of the team members.

Table 2: Members in each IRT sub-team

Supervisory Team	Site Team	Support Team
Senior Management	IT/MIS	Human Resource
Information Security	Security	Public Relations
IT Auditor	IT Auditor	Legal
Financial Auditor		

The following diagram illustrates an overview of the team structure in IRT:



**Figure 4: Structure of the Incident Response Team**



The responsibility of the **Supervisory Team** includes:

- (a) making decisions on, and reviewing steps taken to rectify matters
- (b) communicating and translating technical information to senior management or board of directors
- (c) supervising and reviewing test results based on the tests conducted to verify the feasibility and effectiveness of the incident response procedures
- (d) cooperating with and supplying information to the support team so that their duties can be carried out
- (e) coordinating resources, e.g. software and hardware acquisition, if required
- (f) maintaining proper records of events and actions taken
- (g) attending, establishing and conducting training for relevant personnel
- (h) performing scenario planning and identifying corrective actions for each scenario; and
- (i) supervising and reviewing the update, including lessons learnt, on the Incident Response Procedures.

The responsibility of the **Site Team** includes:

- (a) surveying and securing the systems and environment
- (b) containing the incident
- (c) eradicating incident and performing recovery procedures
- (d) compiling "recovery kit", e.g. recovery procedures, contact list, boot disks, software, tools, hard disk, and so on
- (e) attending and conducting training for relevant personnel and
- (f) updating and maintaining the Incident Response Procedures.

The responsibility of the **Support Team** includes:

- (a) providing logistic and technical support to other IRT teams when required
- (b) updating public and relevant authorities via commercial press, web sites, telephone and others, and
- (c) coordinating communications for the company with various external parties, if required.

A leader will be appointed in the IRT as the point of contact in the event of an incident. When an incident is reported by the helpdesk, the leader will be responsible for



contacting the relevant sub-teams to handle the incident (refer to Appendix E for a detailed incident response work process).

A contact list for IRT members and external parties (for both office and non-office hours) should be developed and made available to the team (refer to Appendix A for the Incident Response Contact List).

When reporting the incident, communication should be made via the telephone and/or fax machine. This is to prevent interception of emails by the perpetrator if the computer used for sending the email has been compromised or by a "sniffer" program that has been planted on the network to capture information sent across the network. Should sensitive electronic media need to be passed to a third party (e.g. listings of account numbers that were leaked) this may be done via secure courier. However the media must be strongly encrypted.

Depending on situation, support from other technical teams in the Company (e.g. the network operations, anti-virus team or IT helpdesk) may be required to assist in the incident handling process.



## 4.2 Identification

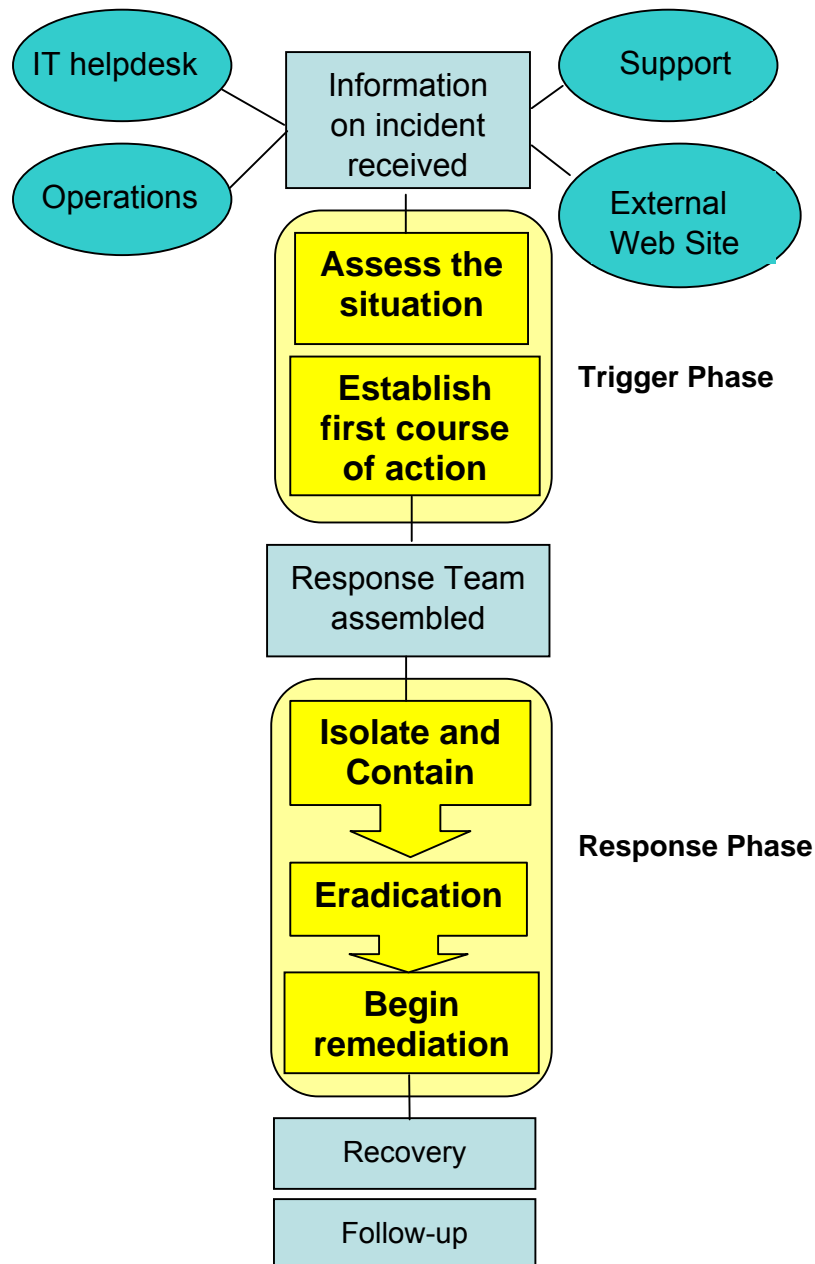
The cost of incident response and recovery can be high. When a staff member notices a suspicious anomaly in data, a system, or the network, the IRT has to perform investigation and verification, which is time and resource consuming. This activity in itself is at risk if the number of false reports exceeds the number of real incidents that occurred, as it diverts resources away from real incidents. To facilitate the task of identification, the following is a list of typical symptoms of security incidents, which include any or all of the following:

- (a) A system alarm or similar indication from an intrusion detection tool
- (b) Suspicious entries in system or network accounting (e.g. a UNIX user obtains root access without going through the normal sequence)
- (c) Accounting discrepancies (e.g. an eighteen-minute gap in the accounting log with no entries)
- (d) Repetitive unsuccessful logon attempts within a short time interval
- (e) Unexplained new user accounts
- (f) Unexplained new files or unfamiliar file names
- (g) Unexplained modifications to file lengths and/or dates, especially in system executable files
- (h) Unexplained attempts to write to system files or changes in system files
- (i) Unexplained modification or deletion of data
- (j) Denial/disruption of service or inability of one or more users to login to an account
- (k) System crashes
- (l) Poor system performance of dedicated servers
- (m) Operation of a program or sniffer device to capture network traffic
- (n) Unusual time of usage (e.g. users login during non-working hours)
- (o) An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user, and
- (p) Unusual usage patterns (e.g. programs are being compiled in the account of a Finance user with no programming background).

Although no single symptom conclusively shows that a security incident is taking place, observing one or more of these symptoms prompts the observer to investigate events more closely. System administrators who encounter one or more of these symptoms should work with the IRT to determine the cause of the incident. Using the



abovementioned categories of incidents as reference, the IRT should validate security incidents on a per case basis before proceeding with the other phases in the framework. All details in the Identification phase should be documented in the Incident Reporting Form in Appendix C. Figure 5 illustrates an overview of the process flow of the incident response plan. For more details on each process, refer to the Incident Response Framework Flow-chart in Appendix E.



**Figure 5: Overview of the incident response plan**

### 4.3 Assessment

The next step to be performed by the IRT is to assess the scope, the impact and the magnitude of the incident. **As a note of precaution, never power off or reboot a compromised system immediately as this may result in the loss of data, information or evidence required for forensic investigation later.** The following are some of the factors to consider during the assessment:

- (a) How many computers are affected by this incident?
- (b) Is sensitive information involved?
- (c) What is the entry point of the incident (e.g. network, phone dial)?
- (d) What is the potential damage caused by the incident?
- (e) What is the estimated time to recover from the incident?
- (f) What resources are required to manage the situation?
- (g) How should the assessment be performed effectively?

Depending on the severity of the situation, top management may have to be informed. Notification guidelines should be developed by the IRT during the preparation of the incident response plan. For “Extreme” and “High” risk incidents, the IRT should escalate them to Visa. The list of key contacts should be completed in the Incident Response Contact List in Appendix A. The Incident Reporting Form in Appendix C can be used to document the information gathered from the assessment.

### 4.4 Containment

The objective of the containment phase is for the IRT to regain control of the situation by limiting the extent of the damage. The IRT may consider isolating the compromised system from the rest of the network systems. However, this may disrupt the business operation if the compromised system is critical or many systems were affected by the incident, as in the example of a virus outbreak. Hence, the IRT must evaluate with the management on a per case basis the risk of continuing operations versus regaining control of the compromised system. All attempts to contain the threat must take into account every effort to minimise the impact to the business operations.

Furthermore, a backup should also be performed on the system to maintain the current state of the system to facilitate the post-mortem and forensic investigation later. The IRT may also consider changing the system passwords to prevent the possibility of Trojan programs being installed on the compromised system that allows the intruder from returning to the system via a backdoor.



## 4.5 Eradication

After the containment phase, further investigation should be performed to uncover the cause of the incident by analysing system logs of various devices (e.g. firewall, router, host logs). It is important that the IRT uses a separate set of administrative tools for the investigation and not those in the compromised system. In the event that the perpetrator has modified the system configuration, execution of any system tools may have dire consequences. For example, the intruder may have modified the DOS CMD.EXE application of the compromised system to delete all files in the system rather than to return a command shell.

A clean operating system should be reloaded into the compromised server after the investigation. Many off-the shelf operating systems are not developed with security in mind. Hence, to increase the security defence of the system, it must undergo a hardening process, which should include:

- (a) Applying all the latest patches
- (b) Disabling any unnecessary services
- (c) Installing anti-virus software, and
- (d) Applying the Company's security policy to the system.

## 4.6 Recovery

Prior to restoring the system from a clean backup, it is recommended that the IRT validate that the eradication procedures have been properly performed. After installing the backup, the system should be monitored in a test environment to determine if it is functioning normally before it can be restored into the business operation.

Furthermore, a network surveillance tool should be implemented to detect any unauthorised attempts such as additional scans or probes that may signal the return of the intruder.

## 4.7 Follow-up

### 4.7.1 Post mortem

The objective of a post-mortem analysis is to perform a detailed investigation of the incident to identify the extent of the incident and potential impact prevention mechanisms. There are three options for performing a post-mortem analysis as shown in Table 2. The IRT should select the option based on the severity of the incident, the damage incurred by the Company and the need for legal actions to be taken against the perpetrator.

**Table 3: Comparison of options for post-mortem investigations**

	<b>In-house investigation</b>	<b>Law enforcement</b>	<b>Private forensic specialist</b>
<b>Cost</b>	Least expensive	Expensive	Most expensive
<b>Time response</b>	Quick response time	Resources not always available, could cause slow response time	Quick response time
<b>Competency of investigators</b>	May not have the relevant skills	Dependent on the local law enforcement	Skilled staff often with law enforcement background
<b>Presentation of evidence</b>	Does not ensure evidence integrity	Preserve evidence integrity and present evidence that is acceptable in court	Preserve evidence integrity and present evidence that is acceptable in court
<b>Reputation impacts</b>	Minimal effect as no outside intervention is required for potentially reputation damaging incidents	Potential loss of reputation if certain incidents reach the public arena	Potential loss of reputation if certain incidents reach the public arena



#### 4.7.2 Documentation

All details related to the incident response process should be documented and filed for easy reference. This provides valuable information to unravel the course of events and can serve as evidence if prosecution of intruders is necessary. It is recommended that the following items be maintained:

- (a) All system events (audit records)
- (b) All actions taken (including the time that an action is performed), and
- (c) All external conversations (including person with whom the discussion was held, the date and time and the content of the conversation).

Furthermore, an incident report documenting the following should be written by the IRT at the end of the exercise:

- (a) A description of the exact sequence of events
- (b) The method of discovery
- (c) Preventive measure put in place, and
- (d) Assessment to determine if the recovery step taken is sufficient and what other recommendations need to be considered.

The objective of the report is to identify potential areas of improvement in the incident handling and reporting procedures. Hence, the review of the report by management should be documented, together with the lessons learnt, to improve on the identified areas and used as reference for future incidents.

#### 4.7.3 Public media handling

In the event of an incident prioritised as “High” or “Extreme”, it is important to consult your Acquiring bank and Visa prior to any public releases or responses to media enquiries being made. Public or media statements must be carefully managed to ensure that any investigation and/or legal proceedings are not jeopardised. Any disclosure of information should be projected in a clear and concise manner by the Public Relations personnel in the IRT and approved by your Acquiring bank and Visa. Any responses to questions from the media should reflect the stand agreed upon by your Acquiring bank and Visa.

#### 4.7.4 Visa Account Information Security Standards

Where an “Extreme” or “High” incident has taken place, an onsite review must be performed to validate your organisation’s compliance to Visa’s *Account Information*



*Security Standards.* The onsite review must be performed by a Visa qualified security assessor.



## Appendix A: Incident Response Contact List

The following table is a template for the IRT to document the contact information of the relevant (internal and external) parties involved in the incident respond plan. The external section of the table has been completed with relevant contact information. This table must be prepared and issued to all the relevant parties together with the Incident Response Checklist (refer to Appendix B).

<b>Prepared by:</b>		<b>Date Updated:</b>		
<b>Internal Contact List</b>				
Department	Designation	Name	Phone	Fax
<b>External Contact List</b>				
Company	Designation	Name	Phone	Fax
Acquiring Bank				
Law Enforcement Agency				
Visa (local office)				
Legal Counsel				
Forensic Investigator				
Information Security Consultant				



## Appendix B: Incident Response Checklist

No.	Description	Remarks
	<b>Preparation Phase</b>	
1.	Prepare contact list for both internal and external parties and disseminate to other relevant parties	
	<b>Identification</b>	
2.	Fill in Sections 1 to 4 of the Incident Reporting Form	
	<b>Assessment</b>	
3.	Fill in Sections 5 to 8 of the Incident Reporting Form	
4.	Notify senior management, Acquirer and Visa (refer to Incident Response Contact List) for "High" and "Extreme" risk-level incidents	
	<b>Containment</b>	
5.	Perform system backup to maintain the current state of the system	
6.	Change system password for affected system(s) to secure the system against any Trojan programs	
	<b>Eradication</b>	
7.	Do not use the system administrative tools. Use separate administrative tool sets for investigation	
8.	Re-install a clean operating system	
9.	Harden the operating system (e.g. apply patches, disable unnecessary services, install anti-virus software, etc.)	
	<b>Recovery</b>	
10.	Validate that the system has been hardened	
11.	Restore system with clean backup	
12.	Put the affected system(s) under network surveillance for future unauthorised attempts	
	<b>Follow-up</b>	
13.	Perform post-mortem analysis on affected system(s) to identify (potential) vulnerable areas	
14.	Engage law enforcement agency/forensic specialists for forensic investigation	





No.	Description	Remarks
15.	Engage a Visa approved qualified security assessor to perform an onsite review, for incidents involving data compromise ("High" and "Extreme" risk-level incidents)	
16.	Submit an Incident Response Report for management review	
17.	File all documentation on the incident response process for future reference	
18.	Seek consultation from Acquiring bank and Visa before releasing any information to the public media	



## Appendix C: Incident Reporting Form

INCIDENT RESPONSE REPORTING FORM			
Date Updated:		Incident no.:	
<b>1. Contact information for this Incident</b>			
Name:		Organisation:	Title:
Address:			
Office/Cell Phone:		Email:	Fax no.:
<b>2. Physical location of affected computer/network:</b>			
(Include building number, room number, and barcode information, if available):			
<b>3. Date and Time Incident occurred:</b>			
Date (mm/dd/yy):		Time (hh:mm:ss am/pm/Time Zone):	
<b>4. Type of Incident (check all that apply):</b>			
<input type="checkbox"/> Malicious code/Virus/Worms/Trojans			
<input type="checkbox"/> Denial-of-Service			
<input type="checkbox"/> Unauthorised access			
<input type="checkbox"/> Network reconnaissance probes			
<input type="checkbox"/> Others (Specify):			
4a. If a Virus/Worm/Trojans,			
Provide the name(s) of the Virus/Worm/Trojans:			
Provide any URL with information specific to this Virus/Worms/Trojans:			
Provide a synopsis of the incident:			
Actions taken to disinfect and prevent further infection:			
<b>5. Information on Affected System:</b>			
IP Address:	Computer/Host Name:	Operating System (incl. release number)	Other Applications:



<b>6. Number of host(s) affected:</b>			
<input type="checkbox"/> 1 to 50	<input type="checkbox"/> 50 to 100	<input type="checkbox"/> 100 to 1000	More than 1000
<b>7. IP Address of apparent or suspected source:</b>			
Source IP address:	Other information available:		
<b>8. Incident Assessment:</b>			
What is the impact of the incident? Please elaborate:			
Sensitivity of the data residing on system:			
Damage or observations resulting from incident:			
<b>9. Information Sharing:</b>			
Has the Public Information Officer been notified? Yes ف No ف		If yes, provide name and date of notification:	
Consider with whom this information may be shared outside of the IRT (do not leave blank and check all that apply):			
<input type="checkbox"/> Acquiring Bank			
<input type="checkbox"/> Visa			
<input type="checkbox"/> Law Enforcement Agency			
<input type="checkbox"/> Forensic Specialists			
<input type="checkbox"/> Others (Specify):			
<input type="checkbox"/> No Sharing is Authorised			
<b>10. Additional Information:</b>			
If this incident is related to a previously reported incident, include any previously assigned incident number for reference:			



## Appendix D: Visa Incident Escalation Form

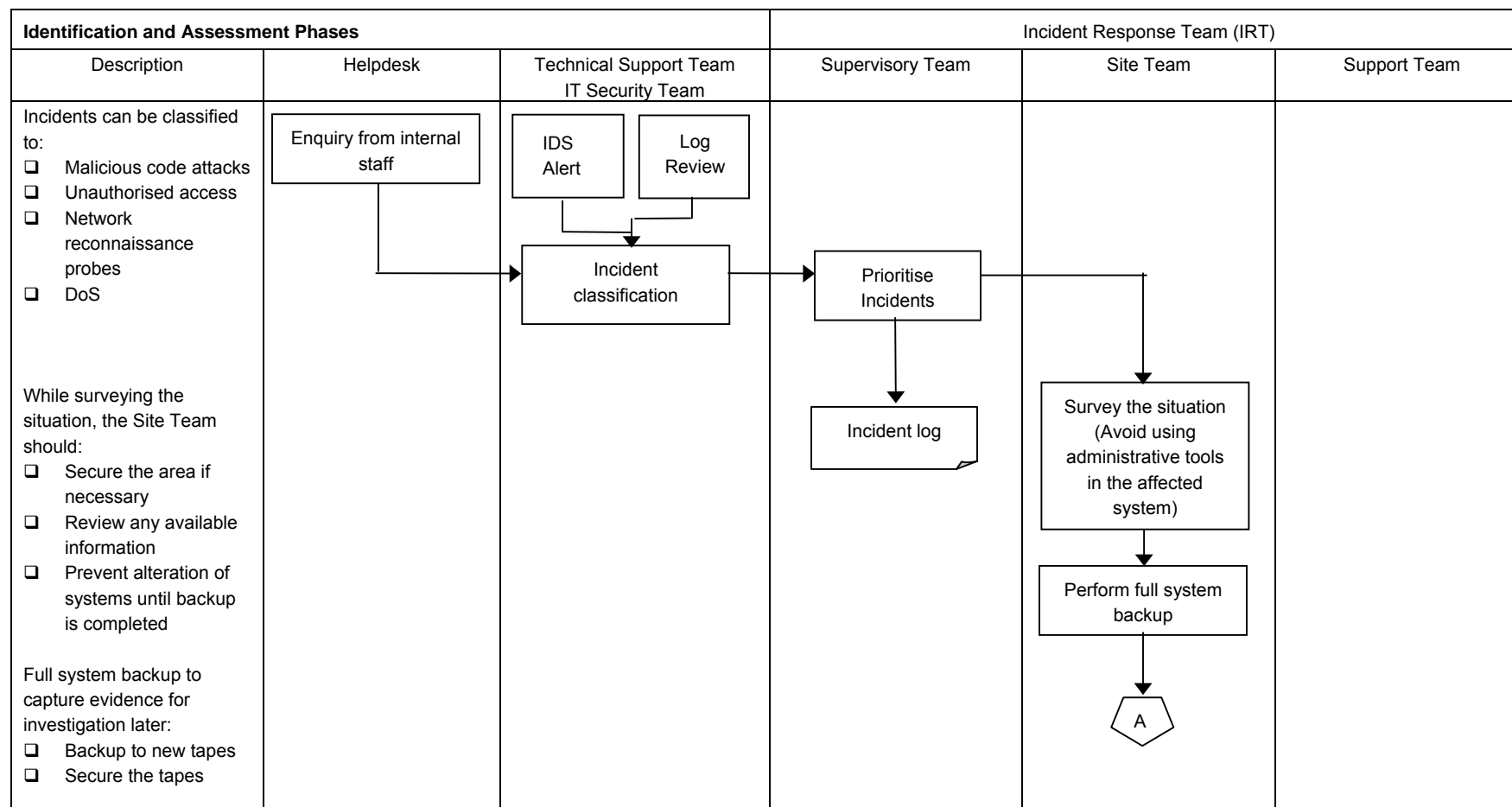
INCIDENT ESCALATION FORM		
Date Updated:		Incident no.:
<b>1. Contact information for this Incident</b>		
Name:	Organisation:	Title:
Address:		
Office/Cell Phone:	Email:	Fax no.:
<b>2. Physical location of affected computer/network:</b>		
(Include building number, shop number, and barcode information, if available):		
<b>3. Period that Incident occurred:</b>		
From (mm/dd/yy):	Till (mm/dd/yy):	
Time (hh:mm:ss am/pm/Time Zone):	Time (hh:mm:ss am/pm/Time Zone):	
<b>4. Incident Assessment:</b>		
Describe the incident.		
How was the incident discovered? Please elaborate:		
Damage or observations resulting from incident.		
Are there any actions taken to control the incident? Please elaborate.		

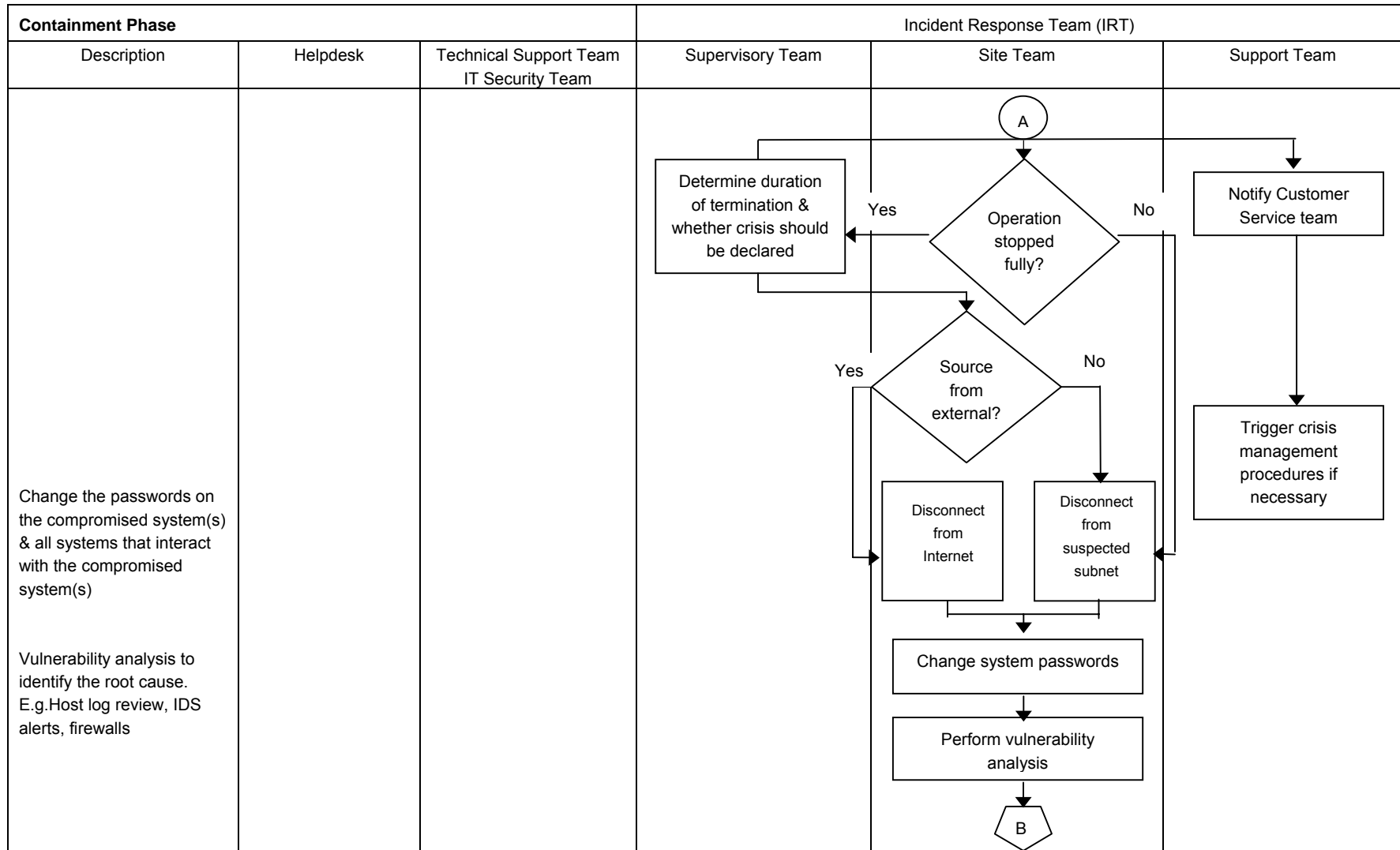


<b>5. Impact assessment:</b>	
How many credit accounts are compromised:	
Which banks/organisation issued the affected accounts?	
What account information is lost? Please elaborate on the sensitivity of the data lost.	
<b>6. Apparent or suspected source of compromise:</b>	
<b>7. Information Sharing:</b>	
Has the Public Information Officer been notified? Yes ڤ No ڤ	If yes, provide name and date of notification:
With whom this information has been shared outside of the Company (do not leave blank and check all that apply): <input type="checkbox"/> Acquiring Bank <input type="checkbox"/> Law Enforcement Agency <input type="checkbox"/> Forensic Specialists <input type="checkbox"/> Others (Specify): <input type="checkbox"/> No Sharing is Authorised	
<b>8. Additional Information:</b>	
If this incident is related to a previously reported incident, include any previously assigned incident number for reference:	

## Appendix E: Incident Response Framework Flow-chart

The flow chart below depicts in detail the process flow of the incident response framework:







Eradication and Recovery Phases			Incident Response Team (IRT)		
Description	Helpdesk	Technical Support Team IT Security Team	Supervisory Team	Site Team	Support Team
<p>Eradication may include:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Remove malicious code/virus</li> <li><input type="checkbox"/> Assess the impact for network probes</li> <li><input type="checkbox"/> Harden the operating system</li> <li><input type="checkbox"/> Remove dormant user IDs</li> <li><input type="checkbox"/> Tighten access rights</li> </ul> <p>Recover may include:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Shut down &amp; re-start systems/services for DoS</li> <li><input type="checkbox"/> Software/hardware configuration changes</li> <li><input type="checkbox"/> Restoration from previous backup</li> <li><input type="checkbox"/> Re-installation</li> </ul>				<pre> graph TD     B((B)) --&gt; A[Perform eradication actions]     A --&gt; D[Follow change management procedures if necessary]     D --&gt; E[Perform recovery procedures (depends on the types of incidents)]     E --&gt; F[System verification]     F --&gt; C{{C}}           </pre>	<pre> graph TD     G[Provide technical support when required] --&gt; H[Contact vendors if necessary]           </pre>



