ICT Security Policy

Incident Management Plan and Process Guide

Ministry of JUSTICE | ICT

Document Information

Master Location	:	
File Name	:	ICT Security Policy – Incident Management Plan and Process Guide
Distribution	:	
Author(s)	:	Ravi Boodhram, Andrew Shephard

Version Control

Issue	Date	Author	Details
0-01	19/01/2012	MoJ ICT IA	Initial draft
1-00	01/08/2013	MoJ ICT IA	Release Version

Glossary and Abbreviation

Term	Definition
DSO	Departmental Security Officer
HMG	Her Majesty's Government
IA	Information Assurance
ICT	Information & Communication Technology
IT	Information Technology
ITSIM	IT Security Incident Management
RMADS	Risk Management and Accreditation Document Set
ITSO	Information Technology Security Officer
MoJ	Ministry of Justice
OST	Operational Security Team
SAL	Security Aspects Letter

SPF	Security Policy Framework
SIRO	Senior Information Risk Owner

References

ID	Title	Version / Issue
1	ICT Security Policy	V
2	ICT Security - ICT Incident Management Policy	V1-00
3	ICT Security - Forensic Readiness Policy	V1-00
4	ICT Security - Acceptable Use Policy	V1-00
5	HMG Security Policy Framework	v.10.0 April 2013
6	CESG Good Practice Guide No. 24 - Security Incident Management	Issue 1.1 November 2012

1

Contents

2

About this document

This document is the MoJ IT Security – Incident Management Plan and Process Guide. It is designed to help protect the information assets of the MoJ through the formal documentation of procedures surrounding the management of IT security incidents.

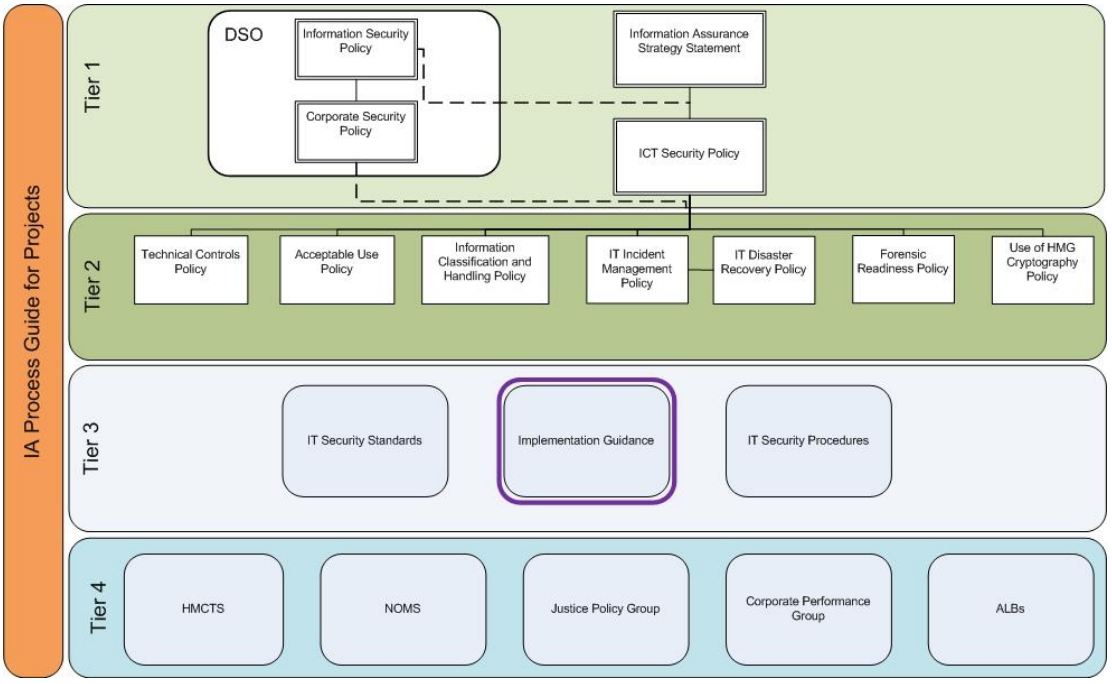

Figure 1 - IT Security Policy Framework

2.1 How to use this document

This document provides guidance on implementing the MoJ IT Security – Incident Management Policy [Ref, 2]. It should be used to guide the development of a MoJ business group level IT Security Incident Management Plan whose scope covers all IT systems used to support that business group.

For the purposes of this document, the following term will be used:

- **IT Security Incident Management** will be referred to as **ITSIM**.

3

Overview

3.1 Introduction

The ability of the Ministry of Justice (MoJ) to react quickly to IT security incidents will ensure that losses are minimised and the business will be able to resume or continue operations as quickly as possible.

Incident management is the ability to react to security incidents in a controlled, pre-planned manner. Preparation and planning are key factors to successful incident management and all MoJ systems will rely upon the development and implementation of an IT Security Incident Management (ITSIM) plan as described in this guide.

The HMG Security Policy Framework [Ref, 5] mandatory requirements 4 states that:

"Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business."

The policy on IT Security Incident Management is covered in IT Security Policy - IT Incident Management Policy [Ref, 3] while this document set outs the MoJ guidance for creating an ITSIM plan. This guide must be read in conjunction with CESG GPG No. 24 – Security Incident Management [Ref, 6].

3.2 Aim of this guide

The aim of this guide is to ensure all MoJ business groups develop, implement and maintain an ITSIM plan.

This guide is split up into four sections:

- An overview of principles of IT security management, its lifecycle and stakeholders;
- Planning and preparation;
- Managing an IT security incident and;
- Capturing lessons learnt.

A template ITSIM plan is provided in Appendix A, this is not designed to be a rigid template and can be flexed to meet the needs of the business.

3.3 Demonstration of Compliance

The CESG Information Assurance Maturity Model (IAMM) sets out the minimum maturity level Government departments should attain. ICT asset disposal is captured as a basic requirement in Level 1 where the MoJ will need to demonstrate compliance.

4

Principles of IT Security Incident Management

ITSIM is a combination of people, plans and predefined processes which enables the MoJ to deal with the consequences of an IT security incident. ITSIM at the MoJ follows the following principles:

- Consistency

The use of dependable, documented methods ensures that incidents, and the reaction to them, are dealt with systematically and cost-effectively.

- Business Continuity

It is essential that the business is able to resume or continue operations as soon as possible after a security incident.

- Ownership and Responsibility

IT security incidents can be very distressing times but reacting on impulse often does more damage than the initial incident itself. The purpose of incident management is to ensure that people with the right level of expertise and experience are consulted and take responsibility for decisions made.

- Escalation

IT security incidents may require coordination with external agencies such as law enforcement or computer forensic capabilities. Internally, different functions within the MoJ may need to be involved in incident management. ITSIM ensures that communication channels are predefined and appropriate for the categorisation of an incident.

- Preservation of MoJ's reputation

Information breaches or IT security incidents are extremely sensitive; both politically and how they viewed by the media and public. When major incidents do occur, as well as escalation within MoJ, there is a public relations requirement to manage how information and questions are dealt with. A good ITSIM should minimise the reputation damage to the MoJ were an incident to occur.

4.1 ITSIM Stakeholders

Stakeholder	Role
All MoJ staff (including contractors and agency	All MoJ staff (including contractors and agency staff) play a

staff)	role in identifying and reporting IT security incidents. All staff must report any concerns especially when the IT security policy is not being adhered to, or where suspicious activity may indicate a security incident is being (or highly likely to be) committed. Moreover, if there is a strong likelihood that a security incident may occur, this must also be reported.
MoJ Senior Managers	MoJ Senior Managers hold a position of responsibility and can form part of the decision making process during the management of a live IT security incident. MoJ Senior Managers must ensure that all IT security incidents or personal data breaches are taken seriously and sufficiently investigated, and where necessary, corrective, disciplinary and or legal proceedings are actively pursued.
Senior Information Risk Owner (SIRO)	MoJ Business Group SIROs are responsible for implementing and managing information risk in their respective business groups and, reviewing the application of policy and guidance regularly thereafter to ensure it remains appropriate to their business objectives and risk environment. In the context of ITSIM, the SIRO forms part of the escalation path where incidents which are categorised as having a high impact or involve personal data (see section 6.3) are reported to the SIRO as a matter of course. They are also responsible for ensuring that their business group has an ITSIM plan.
Information Asset Owner (IAO)	IAOs are senior individuals involved in running business units. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. MoJ IAOs must understand and address risks to the information, and ensure that information is fully used within the relevant laws, and provide written input and assurance to the SIRO annually on the security and use of their asset. They will be informed of any security incidents which compromise any information assets under their ownership.
MoJ IT Security Officer (ITSO)	The MoJ ITSO is responsible for IT security across the MoJ and is the first point of escalation. The ITSO performs two functions with regards to ITSIM; Firstly, a source of advice and guidance on MoJ IT security policy and secondly, forms

	part of the decision making process during the investigation and resolution phase of an IT security incident.
MoJ Operational Security Team (OST)	The MoJ OST forms the core of the MoJ ITSIM response mechanism. They act as a co-ordinator managing all IT security incidents across the MoJ estate. The OST are responsible for: ● Incident ownership, monitoring, tracking and communication ● Sanctioning enhanced monitoring on IT systems where appropriate ● Updating the incident management database with details of all incidents, any investigation conducted and actions undertaken ● Carrying out analysis of security incidents as required ● Initiating a forensic investigation and commissioning forensic analysis (in accordance with IT Security – Forensic Readiness Policy [Ref, 3]) ● Providing progress reports on specific incidents to relevant parties.
IT Service Desk	The MoJ IT service desk act as the first point of contact for MoJ IT Users reporting an IT security event. Their function is to ensure that the details of the incident are captured and the OST are informed.

Table 1 - IT Security Incident Management Stakeholders

4.2 Lifecycle

ITSIM follows a typical risk management lifecycle (see Figure 2) based around:

- Preparation and planning;
- IT Security Incident Management;
- Lessons learnt and continuous improvement.

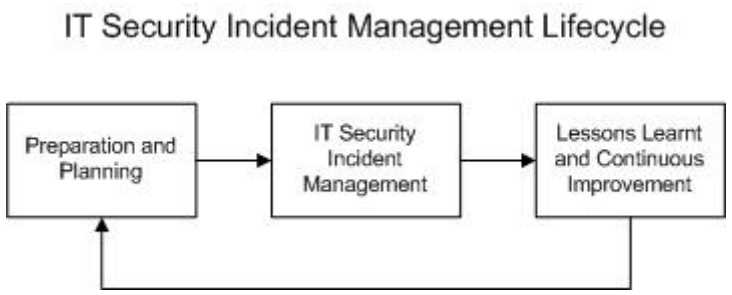

Figure 2 - IT Security Incident Management Lifecycle

The remainder of this guide explores each of these three components and provides guidance on what is required and the activity which must take place in order to create an ITSIM Plan which is fit for purpose.

5

Preparation and planning

The core of ITSIM is preparation and planning, the plan itself needs to be developed mindful of the environment an IT system operates in including the business context. Figure 3 below represents the flow required to develop and implement an ITSIM plan.

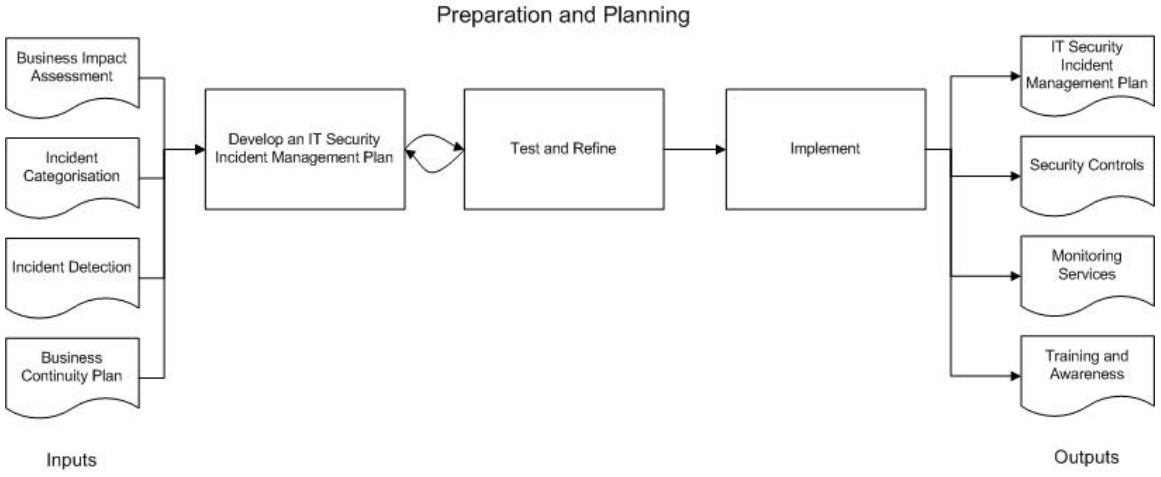

Figure 3 – Preparation and planning

5.1.1 Developing an ITSIM plan

A good ITSIM plan requires a good understanding of the business, the information assets and IT systems involved, the impacts to the business were an incident to occur and the overall business continuity requirement.

Input	Role
Business Impact Assessment (BIA)	The BIA provides the core rational on how the business views the impact to their information assets and services from a loss of Confidentiality, Integrity or Availability. Where this is useful in the development of an ITSIM plan is that the BIA provides a steer on what types of incidents result in the highest impact to the business and how tolerant the business is to a loss of service provision.
Incident Categorisation	The IT Security – IT Incident Management Policy [Ref, 2] and this guide (see section 6.3) provides a generic incident categorisation schema. This generic scheme should be used to develop final schema contained within the ITSIM plan. The aim at this

	phase of developing the ITSIM plan is to: • Explore the different types of incidents which could or have occurred. For example a good starting point is a review of relevant system RMADS to identify possible incident types. • Compare the incident types identified with the information assets and services which could be impacted and broadly align each type to impact category (high impact, medium impact or low impact, see section 6.3 for further details on the response level for each category).
Incident Detection	It is unlikely that an ITSIM plan will be developed in isolation and the IT systems which fall under the scope of the plan will have security controls and procedures which directly or in-directly support incident detections, for example an anti-virus client or intrusion detection system (IDS).
Business Continuity Plan (BCP)	Though the ITSIM plan concentrates on the management of IT security related incidents, ITSIM sits within an overall BCP. It is vital that the relevant BCP is factored in the creation of the ITSIM plan and it is advised that both teams work together as both plans are closely linked and need to be aligned.

Table 2 – Inputs to the IT Security Incident Management plan

5.1.2 Test and refine

Before implementing an ITSIM plan, it is generally good practice to test out as many aspects of the plan as possible in-order to refine its processes and operations. This is likely to involve a number of iterations and include the testing of any automated detection tools.

5.1.3 Implementing the plan

Table 3 below provides a list of the main outputs required to implement an ITSIM plan.

Outputs	Role
IT Security Incident Management Plan	Though obvious, a final released version of the ITSIM plan is the primary output. It must be approved by the business group SIRO and ITSO. It must be released to all Users and stakeholders

	identified in the plan.
Security Controls	The development of an ITSIM plan may lead to the requirement for further security controls to be introduced. For example the ability to collate anti-virus detections centrally.
Monitoring Services	For an ITSIM plan to be effective, a consummate incident detection and monitoring service must be in place and active. For most MoJ ITSIM plans, this will involve the MoJ Operations Security Team (OST) acting as the centralised monitoring and management service where incident reports are fed to them, for example, from automated security controls (such as virus detection alerts from an anti-virus client) or manually by a User reporting the loss of a MoJ laptop to the IT service desk.
Training and Awareness	All Users must be provided with awareness training which covers the ITSIM plan and their role in incident detection, reporting and management. For those who perform specific roles within the plan such as a Senior Manager, they should undertake additional training to ensure they are prepared to fill their aspects of the plan.

Table 3 – Outputs from implementing the IT Security Incident Management plan

6

IT Security Incident Management

Incident management requires a variety of decisions to be made, drawing on expertise from a variety of backgrounds, including technical, administrative and managerial depending on the nature of the incident. The incident management process supports the decision making process and subsequent courses of action taken to resolve an incident.

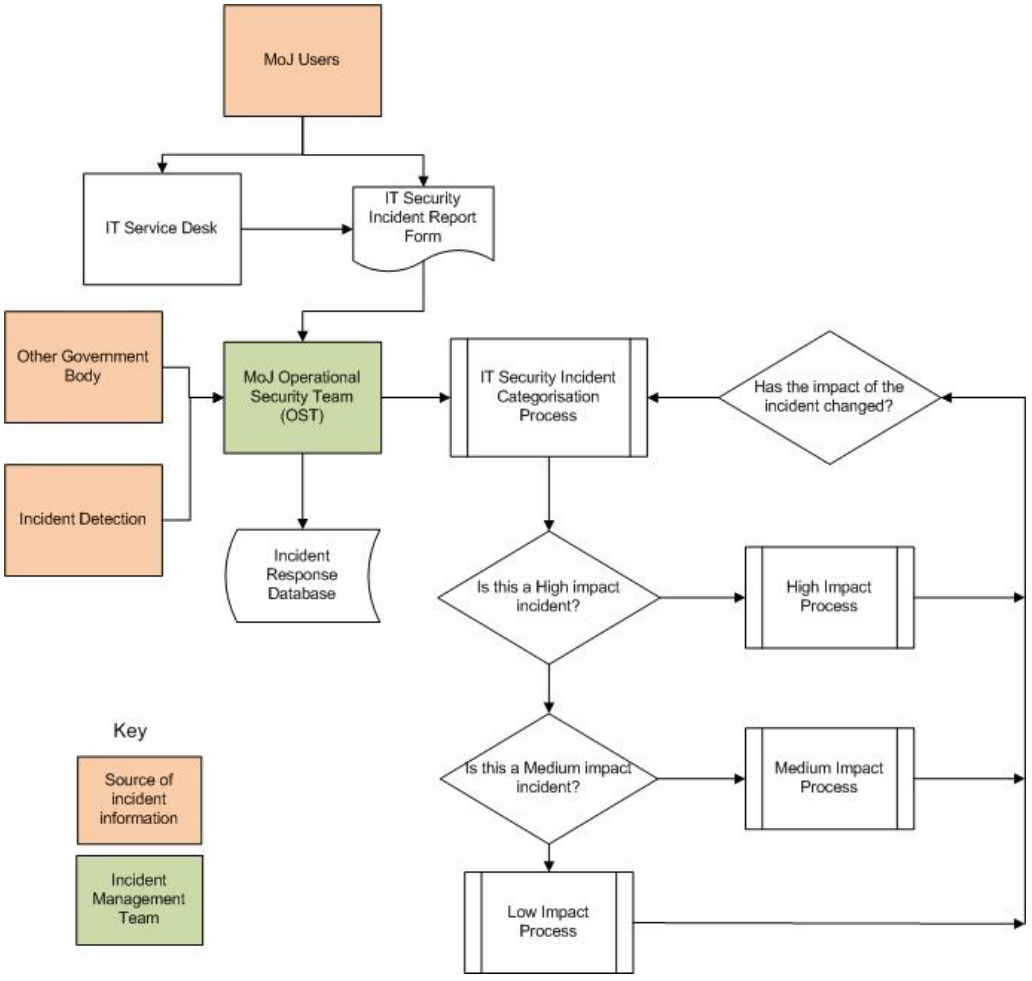

Figure 4 – IT Security Incident Management flow

The ITSIM process essentially consists of three elements:

- Incident reporting – This is shown as a source of incident information on Figure 4. Generally there are three sources, MoJ Users reporting incidents using an IT Security Incident Report Form, alerts from other government bodies such as GovCERT and incident detection controls such as an IT supplier reporting the release of an emergency critical

patch or an automated alert from an Intrusion Detection System (IDS).

- Incident management – This is a function perform by the MoJ Operational Security Team (OST), it involves conducting an initial assessment of the incident, incident categorisation and management of the incident escalating where appropriate. Note that the process continually examines the categorisation of an incident as it is being investigated. An incident may move up or down the impact scale as more information is discovered.

- Incident resolution – Where an incident has been through the management process and resolved.

6.1 What constitutes an 'incident'?

For the purpose of this document, an incident is defined as any event or action that results in an actual and/or potential compromise of personal and sensitive personal data, MoJ information assets and/or the MoJ IT infrastructure.

6.1.1 Types of Incidents

The list of incident types provided in this section is not exhaustive and mirrors the list provided in the IT Security – IT Incident Management Policy [Ref, 2]. Each ITSIM plan must contain a definition of what constitutes an incident which results in the plan being activated, this definition can solely refer to the list provided in the policy, however there may be incident types which are specific to a particular business area which need to capture. The list of incident types includes (but is not limited to):

- Breaches of the IT Security - Acceptable Use Policy [Ref, 4];

- Detection of malicious code (e.g. a piece of malware);

- Network attacks or Denial of Service (DOS) attacks;

- Scanning and probing of a network (where significant network resources are consumed);

- Inappropriate use of MoJ ICT assets as defined in the IT Security – Acceptable Use Policy [Ref, 4];

- The discovery of a new network vulnerability or release of a patch or software update which is considered critical or an emergency;

- The results of a penetration test on a live operational IT system that reveals critical vulnerabilities;

- Unauthorised access to an IT system;

- Accidental loss of personal or other information assets;
- Deliberate release of personal or other information assets;
- Compromise of integrity;
- Any alerts or suspicious activity report generated by an IT system that proves to be a real security alert.

Business related IT security incidents include (but is not limited to):

- Harm to an individual as a result of the compromise of MoJ information assets;
- A significant loss of availability at the MoJ site at which processing and storage of MoJ information takes place;
- The theft or loss of MoJ information;
- The likelihood that a MoJ department or function will be brought into disrepute or might suffer reputational damage;
- A significant impact on the ability of the MoJ to perform its duties;
- A long recovery period either in terms of practical matters or reputation;
- An event that is of interest to local/national press;
- Evidence of espionage activities;
- Accidental loss of personal or sensitive personal information;
- Deliberate release of personal or sensitive personal information.

6.2 Incident Detection and Recording

Security incidents may come to light from a variety of sources, including through active system monitoring and the MoJ staff reporting suspicious activity or security incidents. All IT security incidents must be reported to the OST, who will conduct an initial assessment and manage the incident through to resolution.

Note – All incidents involving personal data must also be reported to the MoJ Data Access and Compliance Unit (DACU).

The MoJ IT Security Policy [Ref, 1] defines the requirements for capturing and recording security events and monitoring them for suspected malicious activity or breaches of security.

The MoJ Operational Security Team (OST) is responsible for maintaining a centralised database and view of all IT security incidents across all MoJ IT systems. This database contains information on:

- Security incident reports;
- An up to date status of all reported security incidents;
- An up to date status of any actions taken with respect to a particular security incident.

This database and the effective reporting of security incidents which populate it are important in managing the MoJ's overall risk exposure. This is both in the short term, to identify any major deficiencies with an IT system which requires immediate remedial action and in the long term, to capture lessons learnt to improve Information Assurance maturity and the ITSIM plan itself.

6.3 Categorisation of Incidents

Incidents need to be categorised to assess their impact and the required level of escalation and reporting. This is mainly done to manage resources and make investigations cost effective. The initial assessment for all IT security incidents will be made by the OST with support from the ITSO and the relevant system Accreditor as required. The assessment will be in terms of the potential impact of the incident with each incident categorised in terms of Low, Medium or High impact.

The three sub-sections below provides a description for each category, it is expected that the business group ITSIM plan will contain a tailored version of this description and confirm the escalation route which will be followed.

6.3.1 Low Impact Incident

These would typically be minor such as low level breaches in security through an accident or carelessness, or a minor loss of service from a service provider e.g. temporary loss of power or connectivity.

A low impact personal data incident would typically include an incident where no loss has occurred but a weakness in a system may potentially have led to a loss, and with a small amount of remedial action the weakness in a process can easily be addressed.

Incident categorised as low will be typically managed by the MoJ OST who will engage with the relevant parties within the business and IT supplier community to resolve the incident. Any escalation (see Figure 5) will be predominantly to the level of the MOJ ITSO and relevant system Accreditor.

6.3.2 Medium Impact Incident

Examples of medium impact incidents include (but not limited to):

- Deliberate disregard for the IT Security Policy [Ref, 1] leading to minor breach in security or the potential of data loss;
- Inappropriate use of MoJ ICT assets as defined in IT Security - Acceptable Use Policy [Ref, 3];
- Loss of data or ICT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Theft of data or ICT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Damage to any MoJ ICT asset;
- Connecting unauthorised equipment to an IT system (where there is no intent or suspicion of malicious activity);
- Prolonged or permanent failure of an IT system;
- Prolonged set of unsuccessful attempts to scan an IT network or instigate a denial of service attack;
- Any alert or reported suspicious activity on an IT system (note this may need to be escalated to High Impact upon investigation);
- Compromise of IT system integrity;
- The recognition of a new critical security vulnerability in an IT system (this may be the result of a penetration test);
- The release of a critical patch by an application or IT equipment vendor;
- Localised report of malicious code (e.g. the detection of a virus or malware of a desktop terminal);
- Serious case of equipment theft;
- The theft or loss of HMG cryptographic material.

Medium impact incidents require escalation to the MoJ ITSO who will determine whether the IAO and relevant system Accreditor also need to be informed. In the case of personal or sensitive personal data, the MoJ Data Access and Compliance Unit (DACU) also need to be informed. If deemed appropriate, a forensic investigation will be requested by the MoJ ITSO in line

with the IT Security – Forensic Readiness Policy [Ref, 3].

6.3.3 High Impact Incident

High level IT incidents require immediate escalation to the Senior Information Risk Owner (SIRO) and relevant Information Asset Owner/s. Examples of incidents requiring this level include (but are not limited to):

- Evidence of espionage activities;
- An incident that is of interest to local/national press;
- A significant impact on the ability of the MoJ to perform its duties;
- The likelihood that MoJ function will be brought into disrepute or might suffer reputational damage;
- Any successful network intrusion to MoJ ICT facilities;
- Widespread malicious code attacks;
- The release of an emergency patch released by a manufacturer used by the MoJ (as described in the Security Patch Management Policy);
- The loss of a MoJ, or suppliers, site at which processing and storage of MOJ information takes place for more than one working day;
- The theft or loss of MoJ protectively marked information which could include CONFIDENTIAL and above, or a significant quantity of RESTRICTED material.

It is highly likely that an incident of this magnitude would require the MoJ ITSO to instigate a forensic investigation and start collecting evidence.

6.4 Further Escalation Requirements

The decision to escalate an incident beyond the MoJ business group SIRO remains with that SIRO where advice will be provided by the MoJ ITSO. Incidents that require this type of escalation include (but are not limited to):

- Issues of national security;
- If the incident has received local or national press coverage;
- If the incident has caused or might cause harm to MoJ Staff;
- There is a high likelihood the MoJ will be brought into disrepute or might suffer reputational damage;

- If the incident involves (or is suspected to involve) FIS or Organised Crime;

- Where there is a HMG requirement to report to central incident management bodies, the OST will co-ordinate reporting for example, the reporting of network security incidents to GovCERT;

- Where there is a significant, actual or possible loss of personal data, the Information Commissioner's Office and the Cabinet Office Central Sponsor for Information Assurance need to be informed via the SIRO and ITSO

6.5 Investigation and Diagnosis Capability:

The MoJ Operational Security Team (OST) is responsible for organising the investigation of all IT security incidents. Where there is a need for evidence to be gathered for possible disciplinary or legal proceedings, a forensic investigation may be required. Each impact category should have its own associated management process which consists of the following activities:

- Investigating an incident as directed by the ITSO or SIRO;

- Proactively monitoring any IT system involved in the incident to capture suspicious behaviour;

- Where authorised by the MoJ SIRO, providing evidence to disciplinary hearings, industrial tribunals, civil courts and criminal courts when required;

- Maintaining files on investigations inappropriate security storage and in accordance to privacy laws;

- Conducting investigations into information security incidents at any of the MOJ locations;

- Recovering and securely store evidence when required;

The distinction between the management processes is the priority and level of resources assigned. For example, a low impact incident involving a MoJ user attempting to access a blocked website will be processed at a slower rate than a high impact incident where a confirm and active network intrusion has been detected.

It is important to ensure that a diagnosis of the events surrounding each incident is recorded and shared with the relevant stakeholders.

Where there has been a personal data incident or where possible disciplinary

or legal proceedings may be required, the following actions must be taken:

- The relevant MoJ Senior Manager must collect detailed information on the incident;
- Refer any possible disciplinary action to HR;
- Maintain records on the investigation appropriately preserving evidence.

6.6 Resolution, Recovery and Closure of Incidents

Based on the investigation and diagnosis of an incident the recovery and closure of the incident can involve many stakeholders. It is important that all stages of resolution are recovers and recorded before an incident is formally closed.

When an IT system has had a significant compromise, that system may require a review of its accreditation status in light of the circumstances of the incident. This is a decision normally made by the relevant system Accreditor.

7

Lessons learnt and continuous improvement

Adequate information relating to security incidents, such as types, volumes and costs must be recorded in order to identify recurring or high impact incidents or malfunctions. This may indicate the need for additional or enhanced security controls to limit the frequency, damage and cost of future occurrences or may indicate the need for a change in policy, the design of an IT system or implementation of SyOPs.

IT security incident statistics must be presented in conjunction with an assessment of top security risks and details of any significant compliance gaps on a monthly basis to the ITSO to assist risk management. Each ITSIM plan must be reviewed on a yearly basis and re-approved by the SIRO and ITSO.

Appendix A – IT Security Incident Management Plan - Template

IT Security Incident Management Plan		
Overview		
MoJ Business Group		[Enter the name of the MoJ Business Group.]
System Description and Scope		[This section must describe the scope of the ITSIM plan. Diagrams may prove useful where there is a complex interaction between systems and business processes covered by this plan.]
Escalation Path		[This section must describe the escalation path for an IT security incident (see Figure 5).]
Incident Categorisation		
Low Impact Incident	**Description**	[Provide a description of what a Low impact incident constitutes; see section 6.3.1 for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consultant the OST and ITSO when completing this section.]
Medium Impact Incident	**Description**	[Provide a description of what a Medium impact incident constitutes; see section 6.3.2 for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consultant the OST and ITSO when completing this section.]
High Impact Incident	**Description**	[Provide a description of what a High impact incident constitutes; see section 6.3.3 for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consultant the OST and ITSO when completing this section.]

Plan Approval	
Business Group SIRO	[Enter the name of the Business Group SIRO] [DATE OF APPROVAL]
IT Security Officer	[Enter the name of the ITSO] [DATE OF APPROVAL]

Completing this plan can form part of the Accreditation process and must be included and maintained as part of the relevant RMADS.

Appendix B – Escalation path

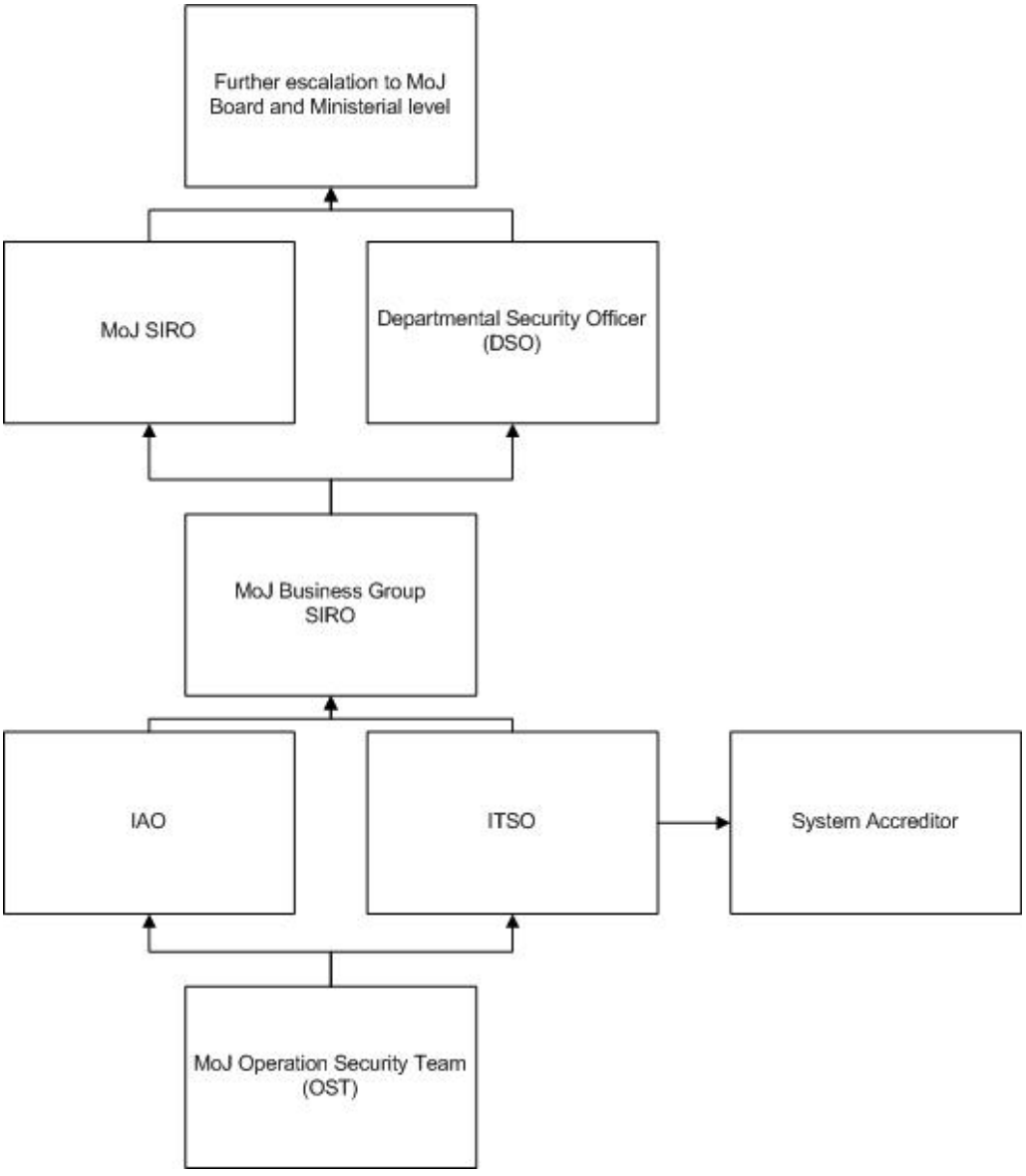

Figure 5 – ITSIM Escalation path