Major Incident Management

Author:	Peter Edwards
Approved by:	See Document Control section
Process:	Major Incident Management
Revision Date:	August 2019
Version Number:	1.0
Publication Date:	August 2018
Review Cycle:	Annualy

Version history

Version	Date	Author	Action
1.0	August 2018	Peter Edwards	Published
0.2	July 2018	Peter Edwards / Adam Webb	Reviewed & Updated
0.1	April 2018	Peter Edwards	First Draft

Document control

Document Name:	Governance of Incident Management	**Security Marking:**	NOT PROTECTIVELY MARKED
Document Description:	Process	**Company Marking:**	UNCLASSIFIED
Retention Requirement:	Permanent	**Export Controlled:**	NO

Approvals

Author:	Peter Edwards	Major Incident/Problem Manager
Authorised By:	Omer Zaman	Netcompany Service Manager
Owner:	Tony Staniforth	HE Head Of Service Management

1 Introduction 4

2 Purpose 4

3 Scope 4
3.1 In Scope 4
3.2 Out of Scope 4

4 Major Incident Definition 4

5 Major Incident Management Process 5
5.1 Detect & Record Incident 5
5.1.1 Incident Detection 5
5.1.2 Incident Reporting 5
5.1.3 Reporting Incidents via the Service Desk 5
5.1.4 Service Supplier 6
5.1.5 Potential Priority One and Priority Two (Out of Hours). 6
5.2 Incident Classification & Initial Support 6
5.2.1 Incident Classification 6
5.2.2 Incident Initial Support 7
5.2.3 Incident Initial Administration 7
5.2.4 Initial Major Incident Communications 7
5.2.4.1 Initial Communications 7
5.2.4.2 Ongoing Incident Communications 7
5.3 Investigate & Diagnose Incident 8
5.4 Resolve & Recover Incident 8
5.4.1 Emergency Change 9
5.5 Incident Resolved 9
5.6 Incident Closure 10
5.7 Managing Security Incidents 10
5.7.1 Incident Assessment 10
5.7.2 Service Desk Analysis Steps: 10
5.7.3 See Priority Assessment instruction below. 10
5.8 Major Incident Report 11
5.9 General Incident Communications 11

6 Major Incident Management Process Flow 12

Appendices 13
Appendix A – Key Roles & Responsibilities 13
Appendix B – RACI Matrix 14
Appendix C – Priority Matrix 15
Appendix D – Priority Definitions 16

1 Introduction

All Highways England staff and Service Supplier's involved with the operations and delivery of Highways England information technology and systems must understand and comply with this process document.

This document defines the Highways England IT Major Incident Management process that must be adhered to when managing major Incidents assigned to the Highways England IT support functions. It replaces any previous version of a Highways England IT centric Major Incident Management Process.

The structure of this document describes the Major Incident Management process followed by a detailed description of each major stage in that process.

This document shows the end-to-end process to be followed from first identification and recording of an Incident. Additionally it documents the concept of ownership along with the importance of monitoring, tracking, communication and restoration

Major Incident Management is a fundamental component of good and responsible practice for managing operation IT services.

2 Purpose

The purpose of the documented process is to outline the Highways England Major Incident Management process and provide the IT organisation with structured guidelines to effectively manage the end-to-end lifecycle of a Major incident.

3 Scope

3.1 In Scope

The scope of this documented process is to outline and document the end to end process for managing high priority incidents. These are classified as a Priority one or two Incidents.

3.2 Out of Scope

The management of lower priority incidents. These are classified as Priority three or four Incidents.

4 Major Incident Definition

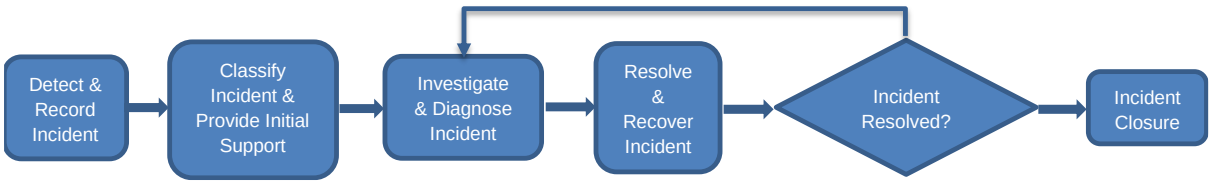
A Major Incident is defined as an incident that has, or is likely to have, a major impact on the ability of the business to maintain services during agreed operational hours. An outage or complete loss of functionality of a critical or key application or service.

The incident could result in:

- An emergency situation.
- Security risks or threat.
- Highways England reputation (HSSE) could be adversely affected.
- Multiple locations/businesses or significant user impacted.

5 Major Incident Management Process

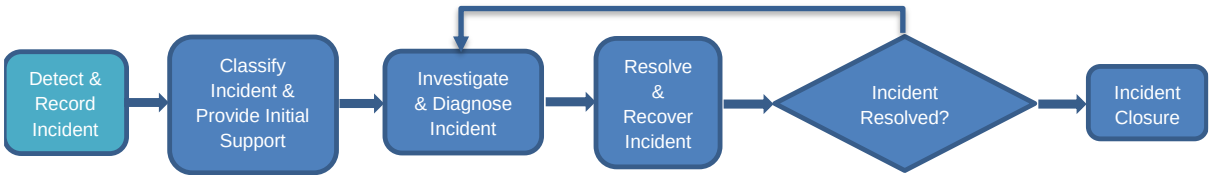
Major Incidents will go through the same high-level process steps as an Incident, the details of the Incident process can be found in the Incident Management Process document. This document will only look at specifics related to the management of Major Incident.



Incidents must be recorded in the ITSM tool by the ICT Service Desk and by means of using best practice guidelines to capture the required level of detail to assist with timely triage to accurately classify the incident.

Record of the events is important to ensure the effective understanding of the decision making and resolution process. This information will also support the effective trend analysis of the Incidents during the Problem Management Process to assist in the identification of the Root Cause and subsequent prevention of any further incidents.

5.1 Detect & Record Incident



5.1.1 Incident Detection

The Incident Reporter will have detected the incident as a part of the Incident Management Process.

5.1.2 Incident Reporting

There are a number of entry points to log a Major Incident onto the Incident Mangement toolset and to engage with the Major Incident Management team.

5.1.3 Reporting Incidents via the Service Desk

When reporting a potential Priority One or Priority Two Incident via the ICT Service Desk, the ICT Service Desk must capture as a minimum the following data and log the incident on the Service Management Tool.

- Best Contact number for the users reporting the issue and/or the affected user:
- Alternative contact numbers for others affected:
- Information on the business service that is affected:
- Availability of those affected:
- Number of reported users affected at the point of logging the incident:
- Site(s) that is/are affected:
- Screen shots of the error, or type in exact error codes etc:

- Understanding of business impact, wide affecting, localised etc:

5.1.4 Service Supplier

If a Service Supplier becomes aware of a potenitial Priority One or Priority Two Incident type situation they will contact the ICT Service Desk by telephone who will create, triage the incident and contact the Major Incident Manager directly by teletphone to inform them of the potential Major Incident.

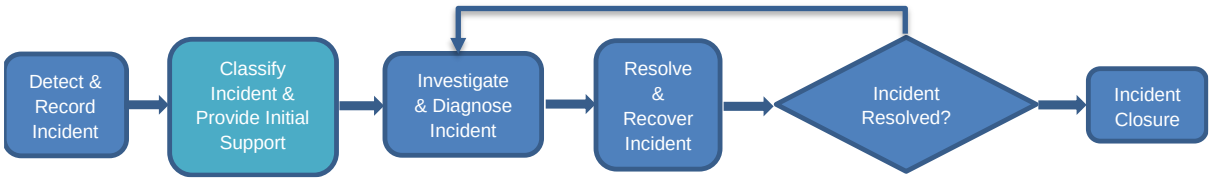
5.1.5 Potential Priority One and Priority Two (Out of Hours).

Out of Hours, the Major Incident Manager can be contacted directly by agreed nominees.

The Major Incident Manager will then assess the validity of the call-out and will check that the incident has been logged in the IT Service Management Toolset.

Only designated nominees can raise Major Incidents OOH.

5.2 Incident Classification & Initial Support



In order to ensure that the Major Incident is recorded correctly the ICT Service Desk Analyst must gather all the relevant incident data paying particular attention to business impact, urgency, potential workarounds and any recovery estimates.

All this information will assist in correctly prioritising the incident, using the Priority Matrix (Appendix C).

The ICT Service Desk Analyst should gather the following information: -

- How many users are affected by this issue and is this isolated or widespread?
- Is the application the user is using a critical application as defined in the 'HA Application List'. (Note these are categorised as Gold, Silver, Bronze).
- Is there an outage or complete loss of a critical or key application or service?
- Is there a business workaround available?
- Does an emergency situation or security risk potentially exist?
- Will Highways England reputation be adversely affected?
- Is there a Financial Risk involved?

5.2.1 Incident Classification

If the reported incident meets the ICT Service Desks criteria for a potential Major Incident they must then verbally engage with the Major Incident Manager to inform them of the potential Major Incident, this must then be followed by an email notification to the Major Incident Managers group mail inbox, ICTIncidentManagement@highwaysengland.co.uk.

The Major Incident Manager will respond to the ICT Service Desk to provide confirmation and agreement that this is Major Incident. They will review the details of the Major Incident with the ICT Service Desk Analyst to ensure that there is a clear understanding of the following: -

- Business impact, including:
    - Application / Service affected.
    - Number of users affected.
    - Location(s) impacted.
    - What will the business be unable to do? Implications? Urgency.
    - Possible workarounds.
- If it is agreed that it is not a Major Incident it should be reported as a Priority three or four Incident and follow the normal Incident Management Process.

If the Incident is agreed as a Priority One or Two Incident, then the Major Incident process applies and the steps documented within the process should be followed.

5.2.2 Incident Initial Support

The initial Support incorporates ensuring that the all initial considerations and activities for management of the Major Incident have been set up to enable correct management of the Incident. The Major Incident Manager will have overall control of the Major Incident.

5.2.3 Incident Initial Administration

The Major Incident Manager will: -

- Publish the initial Major Incident Communications.
- Provide the initial SMS alert.
- Organise the conference bridges (Technical and Management).
- Ensure the correct Service Supplier is assigned to assume ownership of the Major Incident and manage it through to resolution.
- Confirm that an incident ticket has been raised in the Service Management Tool;
    - If no ticket has been logged, then engage with the ICT Service Desk to create a ticket in the Service Management Tool ticketing system.
    - The Major Incident Manager should inform the Highways England Service Delivery Management team for all Priority One Incidents.
- Elevate the Priority of the Incident within the ITSM tool.

5.2.4 Initial Major Incident Communications

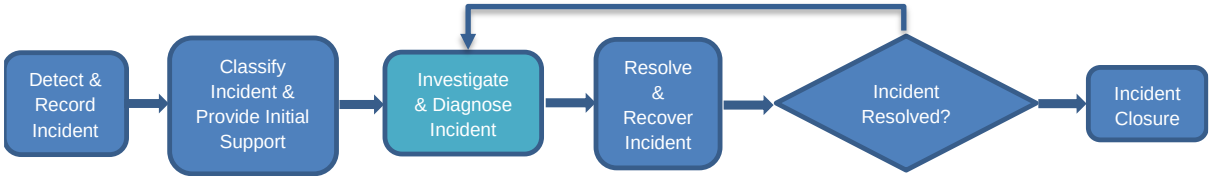
5.2.4.1 Initial Communications

The Major Incident Manager will compile and issue the SMS and initial ICT Incident Communications email using the relevant Distribution Lists. This communication will be sent within 30 minutes of the Major Incident Manager formally accepting the Incident as a Major Incident.

5.2.4.2 Ongoing Incident Communications

The Major Incident Manager will issue Major Incident Update communications throughout the lifecycle of the Incident. As a general guide, the communications for a Priority One will be at a minimum of every one hour and a Priority Two a minimum of every two hours.

5.3 Investigate & Diagnose Incident

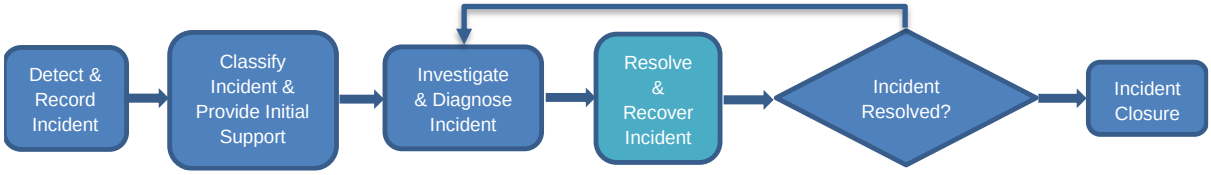


The Service Supplier will carry out the initial investigation & diagnostics of the Incident. All aspects of this investigation will be recorded on the Incident ticket in the ITSM Tool by the relevant members of the resolution team. Key Incident information such as Error Messages, Systems Logs, changes causing the incident, changes to resolve the incident etc. are critical to ensuring that the Problem Management process can correctly identify the Root Cause of the Problem.

The Service Supplier will provide progress updates to the Major Incident Manager throughout the major incident.

The Major Incident Manager will keep a timeline of the events that occur during the lifecycle of the Major Incident. This will be recorded in the Major Incident Report (MIR). The MIR report forms the foundation of the Root Cause Analysis document (RCA).

5.4 Resolve & Recover Incident



Once the Incident has been confirmed to be resolved , the Service Supplier will then complete an informal Root Cause Analysis (RCA) report which is delivered to the Major Incident Manager. This report details all the activities required to restore service, including any emergency change requirements. This is then incorporated into the Major Incident Report (MIR) report which once combined generates the formal RCA report.

The Service Supplier will coordinate the activities of the resolution team as the resolution and recovery plan is implemented. The Service Supplier carries out the activities defined in the resolution and recovery plan, they are also responsible for updating the Incident Ticket in the ITSM Tool, in real time, with information relating to any decision points, investigation, diagnostic and change activities performed, regardless if the activities were successful or not. It is the responsibility of the Service Supplier to ensure that there is a full log of all events and activities carried out during the incident.

During the Resolution and Recovery activities : -

- Ensure the Service Supplier team adheres to any Fatigue Management that may be in place by establishing a shift work pattern.
- Major Incident Manager is kept informed of current status and any problems, concerns, roadblocks and obstacles.
- The Service Supplier continually evaluates the current resolution teams to determine if they are the correct teams to continue to work on the solution.
- Resolution and recovery is potentially an iterative process, and if service is not restored after resolution activities are completed, further investigation & diagnostic activities are undertaken

and a new plan developed and implemented.

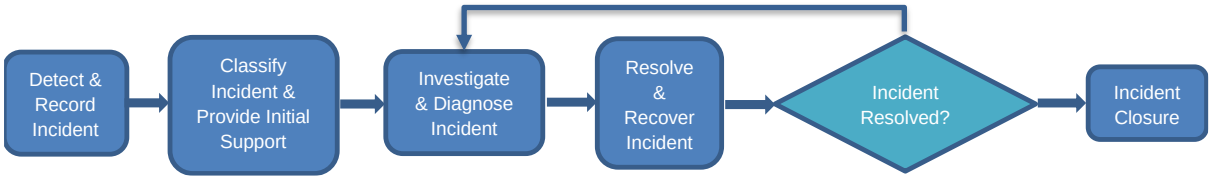
5.4.1 Emergency Change

A Change may be required in order to restore the Service; this will be managed using the emergency change process.

Where multiple applications or infrastructure are impacted it is the responsibility of the Service Supplier to ensure that any required Change Approvals are in place, the implications understood and that the change activities are documented. The retrospective emergency change process is used to formally document the change and approval once the incident is resolved.

A Retrospective Change may be needed where a single application or infrastructure is impacted. The Service Supplier is responsible for raising a retrospective 'Request For Change' (RFC) once service has been restored.

5.5 Incident Resolved



The Major Incident Manager will confer with the Service Supplier to confirm if the service has been restored and is acceptable.

The Major Incident Manager will confirm with the Incident Reporter and/or any Key Business Owner/Representive that all the impacted services have been restored. Confirmation will also be given to the ICT Service Desk.

If services **were not** satisfactorily restored:

- Collect all details and information regarding the current status.
- Evaluate the current resolution teams to determine if they are the correct team to continue to work on the solution. Engage with additional Resolution Teams as appropriate.
- Re-work the Resolution and Recovery plan.

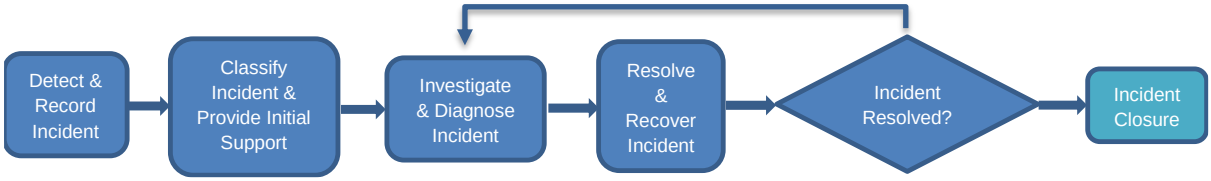
If services were restored, then the incident can be moved to a status of 'Resolved' on the ITSM tool. The Major Incident Manager will manage all the appropriate Major Incident Resolution communications.

If service has not been fully restored, but a work-around or acceptable improvement in Service has been implemented as a result of Resolution and Recovery actions, which mean that the Major Incident implications have now reduced, the Major Incident should be resolved, not downgraded and resolution communication issued accordingly.

Note: Incidents that have correctly been prioritised as a Major Incident should not be downgraded when the impacted service has been partialy improved. A High Priority incident will always be recorded at the most severe impact during it's lifecycle.

If additional Service Restoration activities are still required to address any (lower priority) outstanding impacting service issues, then a problem record should be created and the outstanding actions governed by the Problem Management Team. This should form the basis of handover of outstanding actions/tasks to Problem Management team for the overall management of resolved high priority incidents with ongoing actions incliuding root cause analysis.

5.6 Incident Closure



When the services are restored, the Incident Ticket can be closed.

The Major Incident Manager will manage all the appropriate Major Incident Resolution communications.

If there are outstanding activities to be carried out, but are not impacting the service, then these actions should be recorded in the Root Cause Analysis document (RCA) and managed as actions within the Problem Management Process.

5.7 Managing Security Incidents

5.7.1 Incident Assessment

As part of the virus outbreak process, an analysis must be completed to:

- Identify if it really is a virus; and if so which one it is and
- Obtain any info on the source and cause of the outbreak.

5.7.2 Service Desk Analysis Steps:

- What unusual behaviour is being or has been observed, e.g.
  - Pop-Ups / Browser Redirects to unwanted sites / Unexpected Messages / Ransomware demand / Anti-Virus shotware warning of virus detection
- When was this first noticed (date and time)
- Was there anything odd that happened prior to the issue, e.g.
  - Opening an odd email or attachment,
  - A prompt to install software or an update
- How many people have noticed or been affected by this.

Should the caller report any of the above, or if you feel there is a risk of infection even if they do not, then ask they disconnect from the Network (either by removing the network cable from their EUC or turning off their Wi-fi, and run a virus scan (instructions TBC).

5.7.3 See Priority Assessment instruction below.

Ask for the users EUC Asset Number (white tag), the make and model of the device, a contact number and their likely location for the next 48 hours, record these into the incident ticket with the answers analysis above. The user will be issued an INC number, The ICT Service Desk will send an activity to the IT security advice team and an activity to the HELITS team and make your Team Leader aware, this will help assess the Priority Assessment below if the ICT Service Desk starts to gain more calls.

5.8 Major Incident Report

A Major Incident Report (MIR) will be created for all Major Incidents by the Major Incident Manager with input from the Service Supplier(s). The MIR will be completed within two days of the Major Incident Resolution. A Major Incident Review meeting should be called for all Priority one Incidents, with all the appropriate representation from resources involved in the incident, to review and finalise the draft Major Incident Report. This meeting may also be the initial meeting for the RCA process, if the Problem Manager is invited and agrees.

The MIR will detail a full timeline of the incident, from initial logging of the incident through to final Resolution. All decision points and actions taken to resolve the incident need to be included in the report, including details of any:-

- Log Files and Error messages.
- Initial Root Cause indicators.
- Details of any Changes that may have caused the outage.
- Details of Emergency Changes carried out to restore the Service, and also who is responsible for retrospectively raising a 'Request For Change', (RFC).
- The Recovery Plan.
- Details of Work-around(s) implemented.
- Outstanding Actions from the Incident.
- List of observations which will result in the create of tasks, which will fall under the Problem Mangement process.

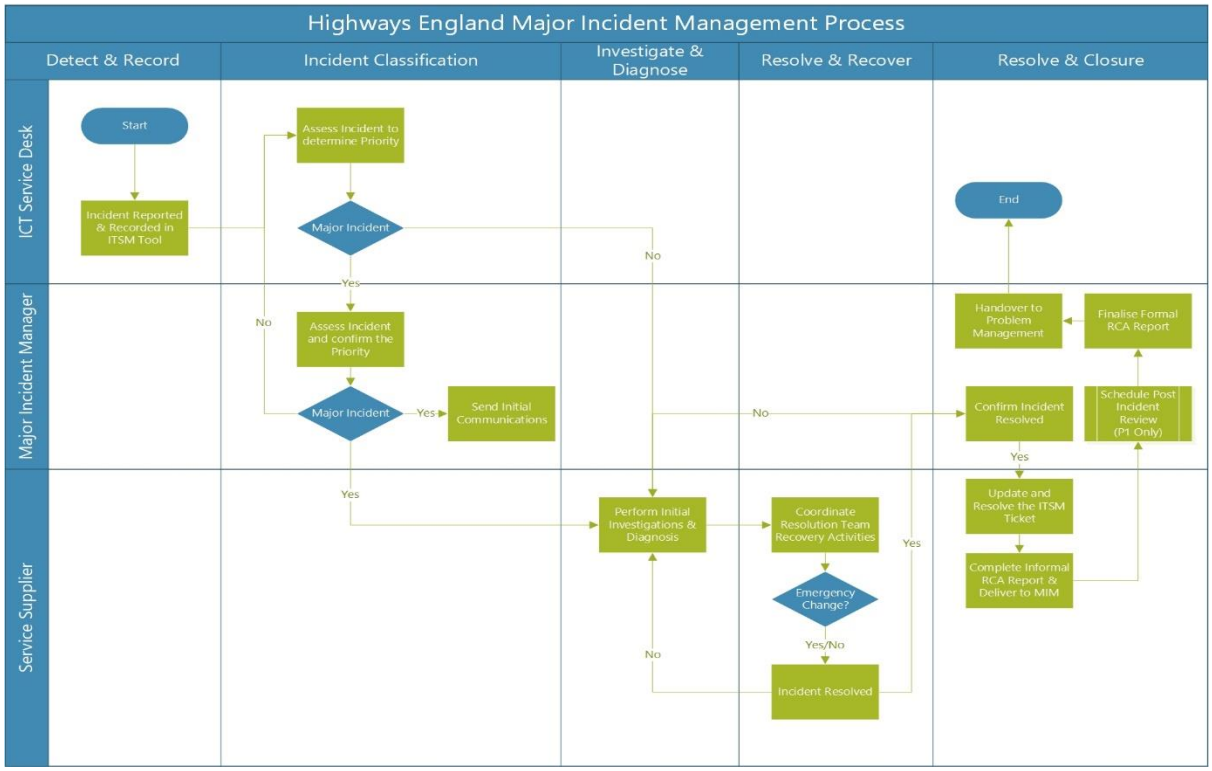
This MIR report will form the basis of the Problem Management Root Cause Analysis (RCA). Initial Actions for inclusion in the RCA should be defined in this report if identified during the Major Incident & they remain outstanding on Resolution.

5.9 General Incident Communications

There are various types of communications that occur during an incident. The Major Incident Manager is responsible for the ICT SMS and Email communications. All ICT Communications will be published following the agreed standard templates.

As a general guide, the timeframe for a Priority One will be at a minimum of every one hour and a Priority Two a minimum of every two hours.

6 Major Incident Management Process Flow



Appendices

Appendix A – Key Roles & Responsibilities

Role	Description
Service Desk Analyst	The Major Incident Management process will be initiated by the Service Desk Analyst in the Service Desk. The Service Desk Analyst will inform the Service Desk shift manager about the Major Incident and the Service Desk shift manager will run the initial stage of the Major Incident Management process.
Service Desk Shift Manager	Manages the operations of the Service Desk and has accountability for the Management of all incidents.
Major Incident Manager	Identifies and notifies the relevant Service Supplier support teams when a Priority One or Two call is logged. In addition, the Major Incident Manager should follow this process to escalate all high Priority faults and to ensure Service Supplier restores service. Takes the role of Change Manager where an emergency change is required to restore service. Produces Draft Major Incident Reports (Root Cause Analysis Document). Raises Problem Record in ServiceNow. Produces all Major Incident Communications.
Service Supplier Lead(s)	Take appropriate action to restore service in compliance with this process and will inform Major Incident Management of any changes to the escalation and notification contact lists.
Communications Lead	Ensures the lead Customer staff is updated with progress towards a resolution in line with customer policy. This role may also be carried out by the Major Incident Manager.
Service Delivery Manager	Works with the customer to ensure that topical escalation and notification lists are maintained for each service. Will also agree communication content and frequency, service continuity and restoration plans. They will also approve emergency changes.
IT Service Continuity & Disaster Recovery Co-ordinator	Where a funded Business Continuity Service exists then the IT Service Continuity Manager will take this role. Alternatively Service Recovery will be managed by the Major Incident Manager.
Change Manager	Manages the operational change process and chairs the CAB.
Problem Manager	Manages the problem management process and co-ordinates root cause analysis.

Appendix B – RACI Matrix

The RACI Matrix demonstrates who is **R**esponsible, **A**ccountable, **C**onsulted and **I**nformed for each step of the process.

Legend R (Responsibility) = Role executing work to achieve the task A (Accountable) = Role answerable for the completion of the task C (Consulted) = Role providing input and/or output (2way communication) I (Informed) = Role kept up-to-date on progress	Major Incident Manager	Service Supplier	Service Desk Analyst	Service Desk Shift Manager	Customer	ITSC & Disaster Recovery Co-ordinator	Problem Management	Communication Manager	Change Manager
RESPONSIBILITIES	ROLES								
Raise Major Incident									
Log Ticket on Incident System	C		R	A	I				
Obtain Details from Security Lead	C	I	R	A					
Liaise with Service Desk by Phone	R		C	A					
Liaise with MIM by Phone	C		R	A/R					
Manage Major Incident									
Triage and Assess Incident	A/R								
Update Communications System	A/R							R	
Investigate Incident	A	R	I	I					
Prepare for SRT	A/R	C	I	I					
Attend SRT – Discuss Resolution – Assign Actions	A/R	C	I	I					I
Ongoing Communication	A/R	C	I	I	I			R	
Management Bridge									
Prepare Management Bridge	A/R	C	I	I	C	I			
Set up Management Bridge	A/R	C	I	I	I	I			
Attend Management Bridge – Discuss Resolution – Assign Actions	A/R	C	I	I	C	I			
Liaise with Technical Bridge	A/R	C	I	I	I				
Closure									
Closure – Ensure Service has been restored.	A/R	R	I	C	C				
Closure – Incident Ticket – Brief Service Desk	A/R	I	C	C	I				
Closure – RCA & Problem Management Initiation	A/R	C	I	I	I	I	I		I

Appendix C – Priority Matrix

	Low	Medium	High	Critical
Critical	P3	P2	**P1**	**P1**
High	P3	P2	P2	**P1**
Medium	P4	P3	P2	P2
Low	P4	P4	P3	P3

Critical Impact	Complete loss of Tier 1 Service ○ At multiple sites ○ For multiple users (>10) Complete loss of access to a Tier 1 Service Degradation of multiple Tier 1 Services Complete loss of multiple Tier 2 Services across multiple sites Complete loss of resilience of Tier 1 Service Backup failure – 3rd occurrence Security Incident affecting more than 1 user >10% users offline	**Critical Urgency**	Response requires an immediate and sustained effort using any and/or all available resources as required until the Incident is resolved Hierarchical escalation is invoked, on-call procedures are activated, and vendor support invoked Generally customers are unable to work and no work around is available
High Impact	Complete loss of Tier 2 Service ○ At multiple sites ○ For multiple users (>10) Degradation of a Tier 1 Service Degradation of multiple Tier 2 Services Complete loss of access to a Tier 2 Service Complete loss of multiple Tier 3 & 4 Services across multiple sites Complete loss of resilience of Tier 2 Service Backup failure – 2nd occurrence Security Incident affecting 1 user but potential to lead to disruption <10% users offline	**High Urgency**	Assigned support team responds immediately, assesses the current situation and may interrupt other staff working lower priority Incidents / Service Requests to assist in timely restoration of services Users require expedited restoration of service, but can bear minimal delays Users may or may not have a work around available, or workaround may only provide partial relief
Medium Impact	Complete loss of Tier 3 / 4 Service ○ At multiple sites ○ For multiple users (>10)	**Medium Urgency**	Assigned support team are able to respond using standard procedures and operating within normal supervisory management structures. Users may or may not have a work around available or

	Degradation of a Tier 2 Service Degradation of multiple Tier 3 / 4 Services Complete loss of access to a Tier 3 / 4 Service Complete loss of resilience for a Tier 3 / 4 Service Backup failure – 1st occurrence Security Incident affecting 1 user – contained (inc password forgotten)		workaround may only provide partial relief
Low Impact	Single user unable to use a Service End user feature not working Warning with no impact to Service	**Low Urgency**	Users may be inconvenienced, but a suitable workaround is available to allow the customer to continue working, or a delay in resolution is considered acceptable

Appendix D – Priority Definitions

	OLA	Full Operational Services Period Service Level Target	Service Failure Threshold
Incident Resolution	OLA4	Severity 1 Incidents – 90% within 4hrs	90% of Severity 1 Incidents within 8 hours
	OLA5	Severity 2 Incidents – 90% within 8 hrs	90% of Severity 2 Incidents within 16 hours
	OLA6	Severity 3 Incidents – 90% within one Working Day	90% of Severity 3 Incidents within 2 Working Days