

MAJOR INCIDENT MANAGEMENT PROCESS

Version: 0.1

Owner:

Date:

DOCUMENT CHANGE HISTORY

Version	Date	Editor	Description of Change
0.1		Rhys Williams	Initial outline document

CONTRIBUTORS

Name	Role	Author / Review / Approve

TABLE OF CONTENTS

1	PROCESS OVERVIEW	4
1.1	Description	4
1.2	Objectives	4
1.3	Critical Success Factors	4
2	PROCESS FLOWCHART	5
3	PROCESS DESCRIPTION	6
4	ROLES AND RESPONSIBILITIES	13
5	SUPPORTING DOCUMENTS	15
6	GLOSSARY	16

1 PROCESS OVERVIEW

1.1 Description

Major Incident Management is the process that handles incidents(s) where the impact of the incident has the potential to lead to a loss or disruption of a business critical service.

Major Incident Management is invoked when shorter timescales and the need for greater urgency is required to deal with incidents which have the potential to cause major business, financial or reputational impact.

MIM provides a distinct process for the IT organisation to resolve major incidents in a consistent and controlled manner. It includes:

- Provision of timely and meaningful information to business and IT stakeholders on business impacting issues on a best endeavour basis;
- Provision of management communication and escalation on major incidents, where required;
- Coordination and facilitation of the resolution of major incidents, where cross-delivery engagement is necessary or resolution is not pending within a reasonable and agreed timeframe.

The stages within the MIM lifecycle are:

1. Major Incident Review and Acceptance
2. Major Incident Investigation and Diagnosis
3. Major Incident Review and Closure
4. Major Incident Monitoring

1.2 Objectives

The key objectives of Major Incident Management are to:

- Return the service to the user as quickly as possible.
- Effectively coordinate service providers and the organisation in the resolution of major incidents.
- Provide effective communication and visibility to the organisation and senior IT executives into the progress of the major incident.
- Manage all major incidents through the lifecycle.

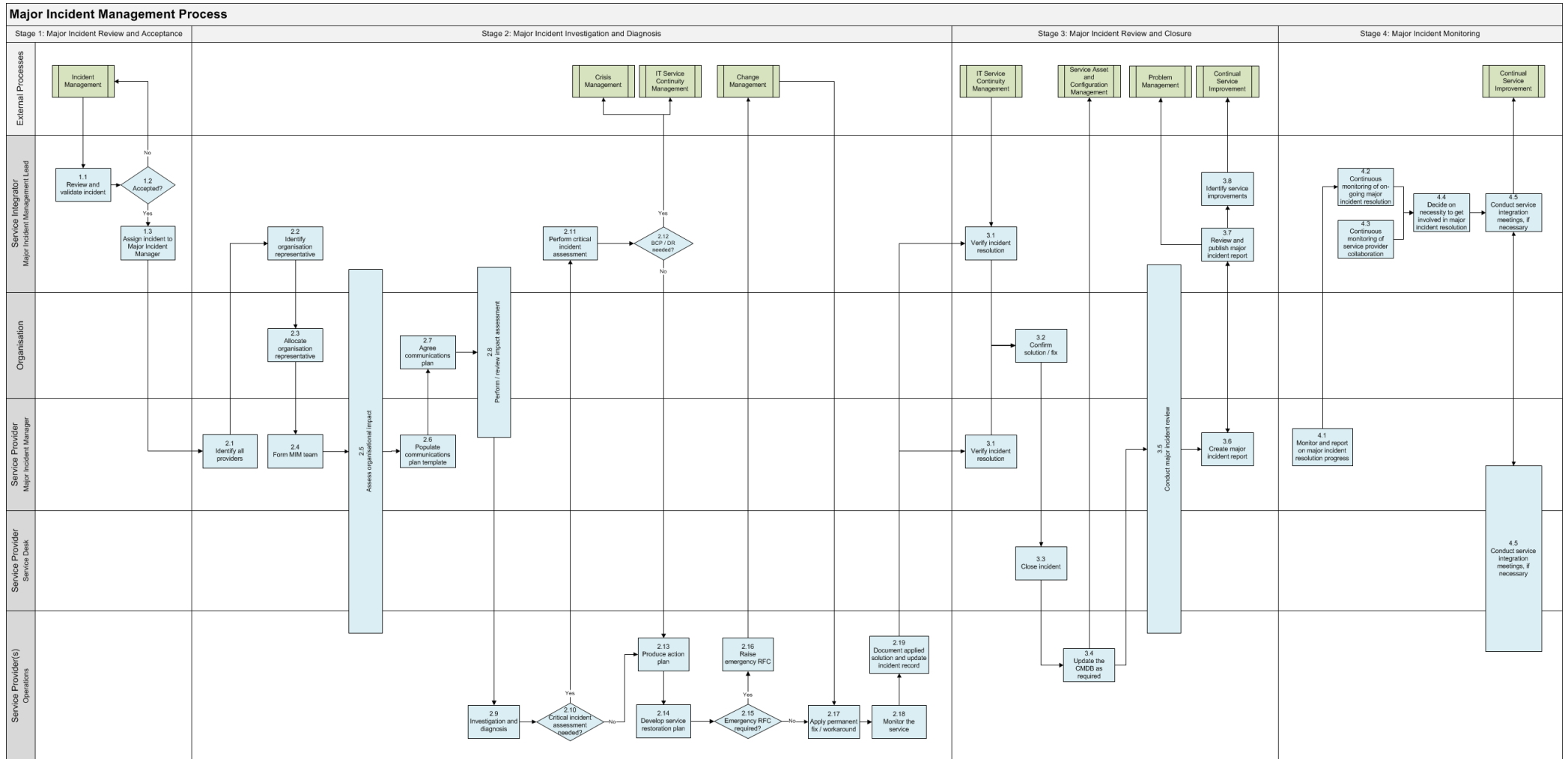
1.3 Critical Success Factors

The critical success factors for Major Incident Management are:

- Business impact is minimised through the prompt resolution of major incidents.
- Incident resolution priorities are aligned with business priorities.
- Standardised methods and procedures are applied to major incidents, improving resolution times.
- Service improvements are identified and actioned to prevent reoccurrence of major incidents.

Major Incident Management Process

2 PROCESS FLOWCHART



3 PROCESS DESCRIPTION

No.	Activity	Description	Inputs	Outputs	Responsible
Stage 1: Major Incident Review and Acceptance					
1.1	Review and validate incident	<p>The SI Major Incident Management Lead evaluates incidents / potential major incidents against the major incident qualifying criteria. An initial impact assessment is performed to understand the potential scale of the incident. Not all the facts may be available, but high-level detail is required.</p> <p>Upon validation / assessment, a decision is taken to follow the Major Incident Management process or pass the incident back to the Incident Management process.</p> <p>If the incident is accepted as a major incident, an automated alert is sent out to all relevant stakeholders.</p>	<ul style="list-style-type: none"> Incident Management Process (S1) Incident Record (S2) Major Incident Qualifying Criteria (S3) 	<ul style="list-style-type: none"> Incident Management Process (S1) Incident Record (S2) - passed back <p>OR</p> <ul style="list-style-type: none"> Incident Record (S2) - accepted as Major Incident 	<ul style="list-style-type: none"> SI Major Incident Management Lead
1.2	Accepted?	<p>If the incident is accepted as a major incident, go to activity 1.3. If not, the incident is passed back into the Incident Management Process.</p>	n/a	n/a	n/a
1.3	Assign incident to major incident manager	The SI Major Incident Management Lead assigns the major incident to the relevant Service Provider Major Incident Manager (MIM).	<ul style="list-style-type: none"> Incident Record (S2) - accepted as Major Incident 	<ul style="list-style-type: none"> Incident Record (S2) - assigned to Major Incident Manager 	<ul style="list-style-type: none"> SI Major Incident Management Lead
Stage 2: Major Incident Investigation and Diagnosis					
2.1	Identify all providers	The Service Provider Major Incident Manager identifies all Service Providers that will be required to support the investigation, diagnosis and resolution of the major incident.	<ul style="list-style-type: none"> Incident Record (S2) - assigned to Major Incident Manager 	<ul style="list-style-type: none"> Service Providers identified 	<ul style="list-style-type: none"> Service Provider (MIM)
2.2	Identify organisation representative	The SI Major Incident Management Lead identifies who in the Organisation will be the best point of contact as part of the Major Incident Management team.	<ul style="list-style-type: none"> Incident Record (S2) - assigned to Major Incident Manager 	<ul style="list-style-type: none"> Organisation representative identified 	<ul style="list-style-type: none"> SI Major Incident Management Lead
2.3	Allocate organisation representative	<p>The organisation allocates the most appropriate person to be part of the MIM team. This could be the organisation's service owner or a senior representative of the impacted business area.</p> <p>The organisation representative is more of a contact to update the organisation on progress. They will not attend meetings with the SI Major Incident Management Lead and Service Providers. They would be contacted outside these meetings, or separate meetings will be held.</p>	<ul style="list-style-type: none"> Organisation representative identified 	<ul style="list-style-type: none"> Organisation representative allocated 	<ul style="list-style-type: none"> Organisation

Major Incident Management Process

No.	Activity	Description	Inputs	Outputs	Responsible
2.4	Form MIM team	The Service Provider Major Incident Manager (in conjunction with the SI Major Incident Management Lead) informs all required resources from Service Providers and the Organisation that they are part of the MIM team.	<ul style="list-style-type: none"> Relevant resources identified 	<ul style="list-style-type: none"> Major Incident Management Team formed 	<ul style="list-style-type: none"> Service Provider (MIM)
2.5	Assess organisational impact	<p>All relevant members of the MIM team work together to formally assess the actual and potential impact that the major incident is having on the organisation.</p> <p>Note: This is a much more detailed assessment than the one performed in activity 1.1 and will be an on-going activity throughout the lifecycle of the major incident.</p>	<ul style="list-style-type: none"> Incident Record (S2) - assigned to Major Incident Manager Major Incident Management Team formed 	<ul style="list-style-type: none"> Organisational Impact Assessment (S4) 	<ul style="list-style-type: none"> All
2.6	Populate communications plan template	<p>The Service Provider Major Incident Manager, with input from the MIM team, defines the communication method, content, frequency and distribution in the form of a plan.</p> <p>All relevant people named in the communications plan will be responsible for communicating progress on the major incident resolution during the lifecycle of the incident. These communications will be on-going until incident resolution but are not shown as a separate activity in this process.</p> <p>The SI Major Incident Management Lead must approve this plan before it is sent to the organisation for their approval.</p> <p>Note: The MIM will be responsible for distributing all communications applicable to the major incident unless this has already been predefined by the organisation (e.g. Digital Delivery).</p>	<ul style="list-style-type: none"> Communication Plan Template (S5) 	<ul style="list-style-type: none"> Communication Plan (S6) - created 	<ul style="list-style-type: none"> Service Provider (MIM)
2.7	Agree communications plan	<p>The Organisation will be required to agree the communications plan.</p> <p>The Organisation will often use this plan to produce their own internal communications plan.</p>	<ul style="list-style-type: none"> Communication Plan (S6) - created 	<ul style="list-style-type: none"> Communication Plan (S6) - agreed 	<ul style="list-style-type: none"> Organisation
2.8	Perform / review impact assessment	<p>The SI Major Incident Management Lead, Service Provider Major Incident Manager and Organisation representative perform an impact assessment.</p> <p>A check of known errors is also completed to help understand if this is a known error, if it has a temporary workaround and whether Problem Management is progressing the investigation of a permanent solution.</p> <p>Continue to investigate and diagnose the major incident and seek any additional assistance as required to reinstate the service as quickly as possible.</p> <p>Note: The organisation will be dealt with separately by the SI Major Incident Management Lead when obtaining impact in most instances.</p>	<ul style="list-style-type: none"> Incident Record (S2) - assigned to Major Incident Manager Major Incident Management Team formed Organisational Impact Assessment (S4) Communication Plan (S6) - agreed Forward Schedule of Change (S7) List of Known Errors (S8) 	<ul style="list-style-type: none"> Impact Assessment performed 	<ul style="list-style-type: none"> SI Major Incident Management Lead Service Provider (MIM) Organisation

Major Incident Management Process

No.	Activity	Description	Inputs	Outputs	Responsible
2.9	Investigation and diagnosis	The Service Provider(s) continue to investigate and diagnose the major incident and seek any additional assistance as required to reinstate the service as quickly as possible. This investigation may highlight that a critical incident assessment is required (i.e. there is a possibility that a disaster has happened or is about to happen).	<ul style="list-style-type: none"> Impact Assessment performed Incident Record (S2) 	<ul style="list-style-type: none"> Incident Record (S2) - investigated and diagnosed 	<ul style="list-style-type: none"> Service Provider (Operations)
2.10	Critical incident assessment needed?	If a critical incident assessment is required, go to activity 2.11. If not, go to activity 2.13.	n/a	n/a	n/a
2.11	Perform critical incident assessment	Based on the Service Provider(s) recommendation, the SI Major Incident Management Lead will examine all the information available and make a decision on whether the Crisis Management and IT Service Continuity Management processes should be invoked.	<ul style="list-style-type: none"> Incident Record (S2) - investigated and diagnosed 	<ul style="list-style-type: none"> Critical incident assessment performed AND <ul style="list-style-type: none"> Crisis Management Process (S22) invoked IT Service Continuity Management Process (S9) invoked OR <ul style="list-style-type: none"> BCP / DR - not needed 	<ul style="list-style-type: none"> SI Major Incident Management Lead
2.12	BCP / DR needed?	If BCP / DR is needed, the IT Service Continuity Management and Crisis Management processes should be invoked. If not, go to activity 2.13.	n/a	n/a	n/a
2.13	Produce action plan	The Service Provider(s) agrees roles, responsibilities and actions to aid fault resolution and investigate potential solutions. Specifically, identify any relevant existing workarounds (considering continuity / recovery plans) that can be used to reinstate the service as quickly as possible, where appropriate.	<ul style="list-style-type: none"> Incident Record (S2) - investigated and diagnosed BCP / DR - not needed 	<ul style="list-style-type: none"> Major Incident Action Plan (S11) 	<ul style="list-style-type: none"> Service Provider (Operations)
2.14	Develop service restoration plan	The Service Provider (Operations) develops a service restoration plan to provide a fix and ensure the execution of actions, in-line with the defined service management processes. Each team / role will undertake the required investigation for their area of responsibility. The actions to be completed are clearly stated in this plan. All action owners are responsible for completing any ancillary or subsidiary actions required.	<ul style="list-style-type: none"> Major Incident Action Plan (S11) Incident Record (S2) - investigated and diagnosed 	<ul style="list-style-type: none"> Service Restoration Plan (S12) AND <ul style="list-style-type: none"> Emergency RFC (S15) required to apply permanent fix / workaround OR <ul style="list-style-type: none"> Emergency RFC not required to apply permanent fix / workaround 	<ul style="list-style-type: none"> Service Provider (Operations)

Major Incident Management Process

No.	Activity	Description	Inputs	Outputs	Responsible
2.15	Emergency RFC required?	If an emergency change is required, go to activity 2.16. If an emergency change is not required, go to activity 2.17.	n/a	n/a	n/a
2.16	Raise emergency RFC	The Service Provider (Operations) raises an emergency RFC, if required, to implement the permanent fix or workaround. <u>Note 1:</u> The fix / workaround may need to be implemented prior to all approvals being gained within the Change Management Process. In this instance the Change Management process may need to be invoked retrospectively. <u>Note 2:</u> There may also be situations where an RFC can be raised (rather than an emergency change) where there is already a workaround that enables a change to be raised in the normal manner (with business agreement).	<ul style="list-style-type: none"> Emergency RFC (S15) required to apply permanent fix / workaround RFC Template (S14) Incident Record (S2) - investigated and diagnosed Service Restoration Plan (S12) 	<ul style="list-style-type: none"> Emergency RFC (S15) raised to apply permanent fix / workaround Change Management Process (S16) 	<ul style="list-style-type: none"> Service Provider (Operations)
2.17	Apply permanent fix / workaround	The Service Provider (Operations) implements the permanent fix / workaround identified within the service restoration plan.	<ul style="list-style-type: none"> Change not required Incident Record (S2) Service Restoration Plan (S12) Emergency RFC (S15) - approved Change Management Process (S16) 	<ul style="list-style-type: none"> Permanent Fix / Workaround applied 	<ul style="list-style-type: none"> Service Provider (Operations)
2.18	Monitor the service	The Service Provider (Operations) monitors the service for the agreed time and documents any findings, particularly noting timings that will be required when reviewing the Service Level Agreement (SLA).	<ul style="list-style-type: none"> Permanent Fix / Workaround applied Service Level Agreement (S17) 	<ul style="list-style-type: none"> Service monitored Documented findings 	<ul style="list-style-type: none"> Service Provider (Operations)
2.19	Document applied solution and update incident record	The Service Provider (Operations) documents the applied resolution activities in the incident record and captures any remediation actions taken. The SI Incident Management Lead will then verify with the organisation that the applied resolution has restored service Based on these activities and the findings documented during monitoring, the incident record is updated appropriately.	<ul style="list-style-type: none"> Permanent Fix / Workaround applied Service monitored Documented findings Incident Record (S2) 	<ul style="list-style-type: none"> Incident Record (S2) - updated with actions taken and resolution details 	<ul style="list-style-type: none"> Service Provider (Operations)

Major Incident Management Process

No.	Activity	Description	Inputs	Outputs	Responsible
Stage 3: Major Incident Review and Closure					
3.1	Verify incident resolution	The SI Major Incident Management Lead and Service Provider Major Incident Manager verify that the major incident is resolved and service is fully restored. They will review the incident record and ensure notes are complete.	<ul style="list-style-type: none"> IT Service Continuity Management Process OR Incident Record (S2) - updated with actions taken and resolution details 	<ul style="list-style-type: none"> Incident Record (S2) - verified 	<ul style="list-style-type: none"> SI Major Incident Management Lead Service Provider (MIM)
3.2	Confirm solution / fix	The Organisation representative confirms that the incident has now been resolved and the service restored.	<ul style="list-style-type: none"> Incident Record (S2) - verified 	<ul style="list-style-type: none"> Incident Record (S2) - resolution confirmed 	<ul style="list-style-type: none"> Organisation
3.3	Close incident	Based on the Organisation's confirmation of resolution, the Service Desk closes the incident record.	<ul style="list-style-type: none"> Incident Record (S2) - resolution confirmed 	<ul style="list-style-type: none"> Incident Record (S2) - closed 	<ul style="list-style-type: none"> Service Provider (Service Desk)
3.4	Update the CMDB as required	<p>The Service Provider (Operations) updates the Configuration Management Database (CMDB) if the remediation actions mandate a change to the CMDB.</p> <p>This action is performed under the jurisdiction of the Service Asset and Configuration Management Process.</p>	<ul style="list-style-type: none"> Incident Record (S2) - updated with actions taken 	<ul style="list-style-type: none"> CMDB updated Service Asset and Configuration Management Process (S18) 	<ul style="list-style-type: none"> Service Provider (Operations)
3.5	Conduct major incident review	<p>A major incident review takes place after a major incident has occurred. It will cover:</p> <ul style="list-style-type: none"> Whether the incident should have been dealt with as a major incident. Capturing the incident's underlying causes if known. If not known, what actions were performed to restore the service and resolve the major incident? Capturing the complete resolution history. Identification of opportunities to improve the handling of future major incidents. A review of the MIM team initiation, monitoring and reporting. A review of Service Providers' collaboration. A review of breaches / impact to SLAs. <p>During this meeting, the Service Provider Major Incident Manager will be assigned the responsibility of producing the major incident report.</p>	<ul style="list-style-type: none"> Incident Record (S2) - closed Major Incident Management Team 	<ul style="list-style-type: none"> Major Incident reviewed 	<ul style="list-style-type: none"> All Organisation (when requested)
3.6	Create major incident report	The Service Provider Major Incident Manager creates the major incident report, documenting the findings from the review. Opportunities are identified for improving the handling of future major incidents. The report is sent to the SI Major Incident Management Lead.	<ul style="list-style-type: none"> Major Incident reviewed 	<ul style="list-style-type: none"> Major Incident Review Report (S19) 	<ul style="list-style-type: none"> Service Provider (MIM)

Major Incident Management Process

No.	Activity	Description	Inputs	Outputs	Responsible
3.7	Review and publish major incident report	The SI Major Incident Management Lead reviews the major incident report, publishes it in the service knowledge management system and requests a problem investigation to identify the root cause of the major incident (if required). If the review results in modifications being required, the Service Provider Major Incident Manager will be requested to update the report accordingly.	<ul style="list-style-type: none"> Major Incident Review Report (S19) 	<ul style="list-style-type: none"> Major Incident Review Report (S19) - published Problem Record (S20) - raised, if required Problem Management Process (S13) 	<ul style="list-style-type: none"> SI Major Incident Management Lead
3.8	Identify service improvement	The SI Major Incident Management Lead identifies any service improvements that will ensure that the incident does not reoccur and feeds into the Continual Service Improvement process.	<ul style="list-style-type: none"> Major Incident Review Report (S19) 	<ul style="list-style-type: none"> Identified service improvements Continual Service Improvement Process (S21) 	<ul style="list-style-type: none"> SI Major Incident Management Lead
Stage 4: Major Incident Monitoring					
4.1	Monitor and report on major incident resolution progress	On an on-going basis, the Service Provider Major Incident Manager will monitor progress of the major incident resolution and provide updates to the SI Major Incident Management Lead.	<ul style="list-style-type: none"> On-going monitoring of progress 	<ul style="list-style-type: none"> Progress updates 	<ul style="list-style-type: none"> Service Provider (MIM)
4.2	Continuous monitoring of on-going major incident resolution	Continuous monitoring of the on-going incident resolution is carried out by the SI Major Incident Management Lead using different approaches, for example: <ul style="list-style-type: none"> Receive progress updates from Service Provider Major Incident Manager. Evaluate impact of any unforeseen difficulties on major incident resolution. Regularly check if SLAs / OLAs are about to fail. Regularly check known error and workaround database. 	<ul style="list-style-type: none"> Incident Records (S2) SLA / OLAs (S11) KPIs Progress updates List of Known Errors (S8) Workarounds 	<ul style="list-style-type: none"> Performed monitoring Analysed major incident resolution 	<ul style="list-style-type: none"> SI Incident Management Lead
4.3	Continuous monitoring of provider collaboration	Continuous monitoring of on-going provider collaboration is performed by the SI Major Incident Management Lead using different approaches, for example: <ul style="list-style-type: none"> Receive progress updates from Service Provider Major Incident Manager. Check major incident records for re-assignment, re-prioritisation and verification of incident record. Evaluate impact of any unforeseen difficulties or problems which occurred during resolution activities. 	<ul style="list-style-type: none"> Incident Records (S2) Progress updates 	<ul style="list-style-type: none"> Performed monitoring Analysed provider collaboration 	<ul style="list-style-type: none"> SI Incident Management Lead

Major Incident Management Process

No.	Activity	Description	Inputs	Outputs	Responsible
4.4	Decide on necessity to get involved in major incident resolution	<p>The SI Major Incident Management Lead will make a decision on getting involved in the major incident resolution if, for example, incident resolution is likely to be delayed or is taking longer than planned, increasing number of requests re-assignment, re-prioritisation and verification of incident record, etc.</p> <p>If involvement is necessary, the SI Incident Management Lead will become involved in the relevant activity within the process.</p>	<ul style="list-style-type: none"> • Performed monitoring • Analysed major incident resolution • Analysed provider collaboration 	<ul style="list-style-type: none"> • Involvement in major incident resolution necessary <p>OR</p> <ul style="list-style-type: none"> • Involvement in incident resolutions not necessary 	<ul style="list-style-type: none"> • SI Incident Management Lead
4.5	Conduct service integration meetings, if necessary	<p>If there are any issues between various Service Providers that need to be handled via a service integration meeting, the meeting agenda is created, the meeting is scheduled with all required participants and the agenda is communicated accordingly.</p> <p>During the service integration meeting, the SI Incident Management Lead moderates the session, ensuring fair and productive feedback and a focus on issue resolution.</p> <p>The invited Service Provider(s) representatives actively participate in the service integration meeting providing options for issue resolution.</p> <p>The SI Incident Management Lead documents and communicates the decisions made in the meeting.</p> <p>If any service improvements are identified during this meeting, they will be fed into the Continual Service Improvement Process.</p>	<ul style="list-style-type: none"> • Service integration meeting required • Service integration meeting schedule and agenda (S12) 	<ul style="list-style-type: none"> • Service integration meeting minutes (S13) • Continual Service Improvement Process (S21) 	<ul style="list-style-type: none"> • SI Incident Management Lead • Service Provider (MIM) • Service Provider (Operations) • Service Provider (Service Desk)

4 ROLES AND RESPONSIBILITIES

Activity		Service Integrator Major Incident Management Lead	Organisation	Service Provider Major Incident Manager	Service Provider Service Desk	Service Provider(s) Operations
Stage 1: Major Incident Review and Acceptance						
1.1	Review and validate incident	R / A	C		C	C
1.3	Assign incident to major incident manager	R / A		I		I
Stage 2: Major Incident Investigation and Diagnosis						
2.1	Identify all providers	C		R / A	I	C / I
2.2	Identify organisation representative	R / A	C / I	I		
2.3	Allocate organisation representative	I	R / A	I		
2.4	Form MIM team	R / C	C	R / A	R	C
2.5	Assess organisational impact	R	R	R / A	R	R
2.6	Populate communications plan template	C	C	R / A	I	C
2.7	Agree communications plan	R / A	R	I		
2.8	Perform / review impact assessment	R	R	R / A		R
2.9	Investigation and diagnosis	C	C	A	I	R
2.11	Perform critical incident assessment	R / A	I	C / I	I	C / I
2.13	Produce action plan	C	C	A	I	R
2.14	Develop service restoration plan	C	C	A	I	R
2.16	Raise emergency RFC	I	I	A	I	R
2.17	Apply permanent fix / workaround	I	I	A	I	R
2.18	Monitor the service	I		A		R
2.19	Document applied solution and update incident record	I	I	A	I	R
Stage 3: Major Incident Review and Closure						
3.1	Verify incident resolution	R / A	C	R		C
3.2	Confirm solution / fix	I	R / A	I		I
3.3	Close incident	I	I	I	R / A	I

Major Incident Management Process

Activity		Service Integrator Major Incident Management Lead	Organisation	Service Provider Major Incident Manager	Service Provider Service Desk	Service Provider(s) Operations
3.4	Update the CMDB as required	I			I	R / A
3.5	Conduct major incident review	R / A	C	R	R	R
3.6	Create major incident report	I		R / A		
3.7	Review and publish major incident report	R / A	I	I	I	I
3.8	Identify service improvement	R / A	I	C	C	C
Stage 4: Major Incident Monitoring						
4.1	Monitor and report on major incident resolution progress	I		R / A		
4.2	Continuous monitoring of on-going major incident resolution	R / A		C	C	C
4.3	Continuous monitoring of provider collaboration	R / A		C	C	C
4.4	Decide on necessity to get involved in major incident resolution	R / A		C		I
4.5	Conduct service integration meetings, if necessary	R / A		R	R	R

Key to RACI Chart:

- Responsible **(R)** : The person / group who has to perform the task
- Accountable **(A)** : The person / group who is accountable for the deliverables of the task
- Consulted **(C)** : Persons who must always be consulted before a decision / action is taken
- Informed **(I)** : Persons who must always be informed after a decision / action is taken

5 SUPPORTING DOCUMENTS

No.	Document Name	Owner	Location
S1	Incident Management Process	SI Incident Management Lead	Service Knowledge Management System
S2	Incident Record	SI Incident Management Lead	Service Management Tool
S3	Major Incident Qualifying Criteria	SI Major Incident Management Lead	Service Management Tool
S4	Organisational Impact Assessment	SI Major Incident Management Lead	Service Knowledge Management System
S5	Communication Plan Template	SI Major Incident Management Lead	Service Knowledge Management System
S6	Communication Plan	SI Major Incident Management Lead	Service Knowledge Management System
S7	Forward Schedule of Change	SI Change Management Lead	Service Management Tool
S8	List of Known Errors	SI Problem Management Lead	Service Management Tool
S9	IT Service Continuity Management Process	SI Service Continuity Management Lead	Service Knowledge Management System
S10	Service Continuity / Recovery Plans	SI Service Continuity Management Lead	Service Knowledge Management System
S11	Major Incident Action Plan	SI Major Incident Management Lead	Service Knowledge Management System
S12	Service Restoration Plan	SI Major Incident Management Lead	Service Knowledge Management System
S13	Problem Management Process	SI Problem Management Lead	Service Knowledge Management System
S14	RFC Template	SI Change Management Lead	Service Management Tool
S15	RFC	SI Change Management Lead	Service Management Tool
S16	Change Management Process	SI Change Management Lead	Service Knowledge Management System
S17	Service Level Agreement	SI Service Level Management Lead	Service Knowledge Management System
S18	Service Asset and Configuration Management Process	SI Service Asset and Configuration Management Lead	Service Knowledge Management System
S19	Major Incident Review Report	SI Major Incident Management Lead	Service Knowledge Management System
S20	Problem Record	SI Problem Management Lead	Service Management Tool
S21	Continual Service Improvement Process	SI Continual Service Improvement Management Lead	Service Knowledge Management System
S22	Crisis Management Process	Organisation	Service Knowledge Management System

6 GLOSSARY

BCP	Business Continuity Plan
CMDB	Configuration Management Database
DR	Disaster Recovery
ITIL	IT Infrastructure Library
KPI	Key Performance Indicator
Major Incident	“The highest category of impact for an incident. A major incident results in significant disruption to the business.” <i>(ITIL definition)</i>
MIM	Major Incident Manager
OLA	Operational Level Agreement
RFC	Request for Change
SI	Service Integrator
SKMS	Service Knowledge Management System
SLA	Service Level Agreement