INCIDENT MANAGEMENT PROCESS

Version: 1.0

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

1.1 Description

Incident Management is the process that handles all failures, faults or questions reported by users via the Service Desk or which are automatically detected and reported (by Event Management via monitoring tools) by the Service Providers. Incident Management utilises incident models that include the following steps within the incident management lifecycle:

1. Incident Identification
2. Incident Logging
3. Incident Triage
4. Incident Investigation
5. Incident Resolution
6. Incident Closure
7. Incident Monitoring

1.2 Objectives

The key objectives of Incident Management are to:

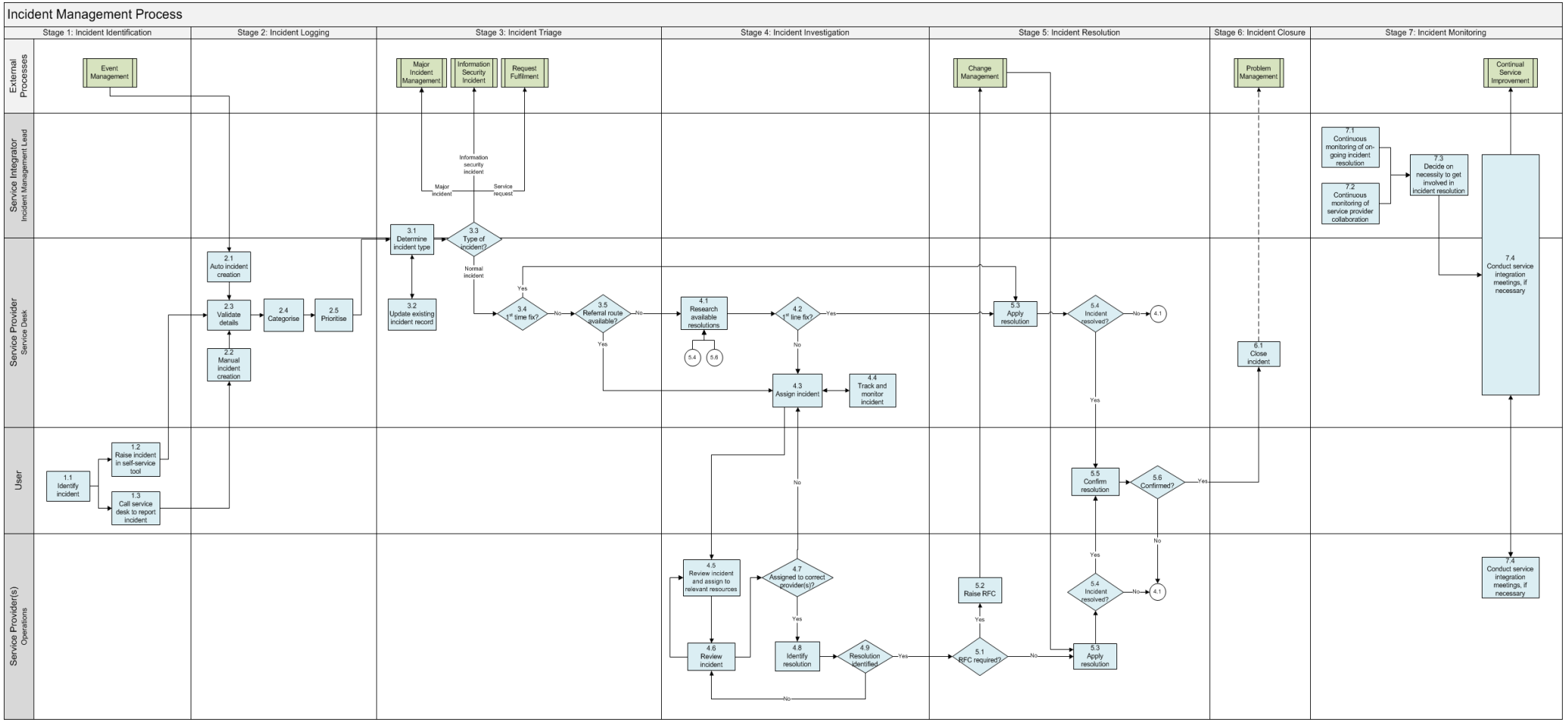
- Return the service to the user as quickly as possible.
- Effectively coordinate the inputs of the Service Providers in the resolution of cross-delivery incidents.
- Support effective communication and visibility for the business into the incident process.
- Manage all incidents through the incident management lifecycle.

1.3 Critical Success Factors

The critical success factors for Incident Management are:

- Minimise impacts to the business through the prompt resolution of incidents.
- Maintain user satisfaction through the prompt resolution of incidents.
- Ensure that incident resolution priorities are aligned with business priorities.
- Ensure that standardised methods and procedures are applied to incidents, improving incident resolution times.

2 PROCESS FLOWCHART



3 PROCESS DESCRIPTION

No.	Activity	Description	Inputs	Outputs	Responsible
Stage 1: Incident Identification					
1.1	Identify incident	If any user encounters a disruption to standard operation, they will contact the Service Desk via the portal or by phone to report the incident. Note: 'User' refers to any person who uses the IT service on a day-to-day basis - this can be anyone within the Organisation, a member of the SIAM function or any member of service provider staff.	• User impact	• Incident identified	• User
1.2	Raise incident in self-service tool	The user raises an incident in the self-service portal. Where contact is made by portal, verification of users' authenticity is intrinsic to the process (i.e. they must provide login details in order to be able to access the portal).	• Incident identified	• Incident Record (S2)	• User
1.3	Call service desk to report incident	The user calls the Service Desk to report an incident. Where a user makes contact by phone, the contacting user will be verified as an authorised user.	• Incident identified	• Incident reported	• User
Stage 2: Incident Logging					
2.1	Auto incident creation	The incident is automatically generated in the service management tool from details created by an event monitoring tool and is assigned to the Service Desk to be validated, categorised and prioritised.	• Event Management Process (S1) • Incident identified	• Incident Record (S2)	• Service Provider (Service Desk)
2.2	Manual incident creation	The Service Desk analyst manually generates an incident from the details provided by the user and provides the initial support.	• Incident reported	• Incident Record (S2)	• Service Provider (Service Desk)
2.3	Validate details	Details of all incidents are verified by the Service Desk to ensure that sufficient detail has been provided to aid investigation and resolution. If more details are required, the Service Desk will contact the user and update the incident record based on the additional information gathered.	• Incident Record (S2)	• Incident Record (S2) - validated	• Service Provider (Service Desk)
2.4	Categorise	The incident is categorised based on pre-defined rules within the service management tool.	• Incident Record (S2)	• Incident Record (S2) - categorised	• Service Provider (Service Desk)
2.5	Prioritise	The incident is prioritised based on pre-defined rules within the service management tool.	• Incident Record (S2)	• Incident Record (S2) - prioritised	• Service Provider (Service Desk)

No.	Activity	Description	Inputs	Outputs	Responsible
Stage 3: Incident Triage					
3.1	Determine incident type	The type of incident is determined based on all information gathered to date. In most cases, the reported incident will be exactly that - an incident. However, some reported incidents are better dealt with by other processes, i.e. • Normal incidents - dealt with by this process. • Major incidents - dealt with via the Major Incident Management process. The priority of the incident will be updated. • Information security incidents - dealt with via the Information Security Incident process. The priority of the incident will be updated. • Service requests - dealt with via the Request Fulfilment process. The incident record will be closed and the user told to raise the call as a service request. The Service Desk normally performs this activity, but the SI Incident Management Lead will also be involved in any cases where the type of incident is unclear, especially if the incident has the potential to be classed as a major incident. If the incident raised can be resolved by the Service Desk without the need for a change or additional investigation by searching for workarounds from the SKMS, the call can be managed / recorded as a 1st time fix. Also, if a clear and defined incident routing option is identified, this should be used to allocate the incident.	• Incident Record (S2) - prioritised / categorised • Service Knowledge Management System • Call Routing Information (S6)	• Major Incident Management Process (S3) OR • Request Fulfilment Process (S4) • Incident Record (S2) - closed OR • Information Security Incident Process (S5) OR • Incident Record (S2) - 1st time fix available OR • Incident Record (S2) - referral route available OR • Incident Record (S2) - referral route not available	• Service Provider (Service Desk) • SI Incident Management Lead
3.2	Update existing incident	The Service Desk updates the incident record with new information based on the determination of the incident type and any relevant additional information. Any other related tickets will also be linked. The added details should be clear, concise and accurate.	• Incident Record (S2)	• Incident Record (S2) - updated	• Service Provider (Service Desk)
3.3	Type of incident?	• Normal incidents - go to activity 3.4. • Major incidents - invoke the Major Incident Management process. • Information security incidents - invoke the Information Security Incident process • Service requests - invoke the Request Fulfilment process.	n/a	n/a	n/a
3.4	1st time fix?	If the incident raised can be resolved by the Service Desk as a 1st time fix, go to activity 5.3. If a 1st time fix is not available, go to activity 3.5.	n/a	n/a	n/a

No.	Activity	Description	Inputs	Outputs	Responsible
3.5	Referral route available?	If a clear and defined incident routing option is identified, go to activity 4.3. If no clear referral route is available, go to activity 4.1.	n/a	n/a	n/a
Stage 4: Incident Investigation					
4.1	Research available resolutions	If, following further investigation and incident matching, the incident raised can be resolved by the Service Desk without the need for a change or additional investigation by searching for workarounds from the SKMS, the call can be managed / recorded as a 1st line fix. If no clear incident routing option is available when triaging the call, the incident will require further investigation and incident matching to identify the correct Service Provider to assign the incident to. This may involve discussions with the user to clarify incident details.	• Incident Record (S2) - referral route not available OR • Incident Record (S2) - not resolved • Service Knowledge Management System	• Incident Record (S2) - resolution identified OR • Incident Record (S2) - resolution not identified	• Service Provider (Service Desk)
4.2	1st line fix?	If the Service Desk can apply the resolution, go to activity 5.3. If the Service Desk cannot resolve the incident, go to activity 4.3.	n/a	n/a	n/a
4.3	Assign incident	If, following further investigation and incident matching, no simple resolution has been identified, the incident is assigned to the appropriate Service Provider(s) to complete additional detailed investigation.	• Incident Record (S2) - resolution not identified • Incident Record (S2) - referral route available • Call Routing information (S6)	• Incident Record (S2) - escalated to Service Provider(s)	• Service Provider (Service Desk)
4.4	Track and monitor incident	All incidents will be monitored and tracked to ensure they are handled in the correct manner and resolved within the agreed SLAs. The Service Desk will also keep the user who reported the incident informed of progress.	• Incident Record (S2) - escalated to Service Provider(s)	• Incident Record (S2) - tracked and monitored	• Service Provider (Service Desk)
4.5	Review incident and assign to relevant resources	The Service Provider (Operations) assesses the incident and determines the appropriate resources to resolve the incident (this may be a 3rd party supplier).	• Incident Record (S2) - escalated to Service Provider(s)	• Incident Record (S2) - escalated to relevant resource	• Service Provider(s) (Operations)
4.6	Review incident	The assigned resource begins additional investigation of the incident escalated to them. At this point the service provider may find that the incident has not been correctly routed or that other service providers are also required to help resolve the incident.	• Incident Record (S2) - escalated to relevant resource	• Incident Record (S2) - investigated	• Service Provider(s) (Operations)
4.7	Assigned to correct provider(s)?	If the incident has been correctly assigned, go to activity 4.8. If not, go back to activity 4.3.	n/a	n/a	n/a

No.	Activity	Description	Inputs	Outputs	Responsible
4.8	Identify resolution	The resolution of the incident is identified, documented and a decision is made on whether an RFC is required prior to the fix being applied. If a resolution is not identified, the incident will require further reviewing (as per activity 4.6). Identification of resolution (this activity) may be performed by a single service provider or multiple service providers (in the case of cross-functional incidents).	• Incident Record (S2) - investigated • Service Knowledge Management System	• Incident Record (S2) - resolution identified, RFC required OR • Incident Record (S2) - resolution identified, RFC not required OR • Incident Record (S2) - resolution not identified	• Service Provider(s) (Operations)
4.9	Resolution identified?	If a resolution is identified, go to activity 5.1. If not, go back to activity 4.6.	n/a	n/a	n/a
Stage 5: Incident Resolution					
5.1	RFC required?	If an RFC is required to resolve the incident, go to activity 5.2. If an RFC is not required, go to step 5.3.	n/a	n/a	n/a
5.2	Raise RFC	If a change is required to resolve the incident, the relevant service provider raises the RFC and invokes the Change Management Process.	• Incident Record (S2) - resolution identified, RFC required • RFC Template (S7)	• Change Management Process (S8) • RFC (S9)	• Service Provider(s) (Operations)
5.3	Apply resolution	The solution should be applied as documented in the incident record / RFC (if one was required). The incident record will then be updated with resolution details.	• Incident Record (S2) - resolution identified AND/OR • RFC (S9) - approved	• Incident Record (S2) - resolved OR • Incident Record (S2) - not resolved	• Service Provider(s) (Operations)
5.4	Incident resolved?	If the incident is resolved, go to activity 5.5. If not, go back to step 4.1.	n/a	n/a	n/a
5.5	Confirm resolution	The user confirms that the incident has been resolved, in discussion with the Service Desk.	• Incident Record (S2) - resolved	• Incident Record (S2) - resolution confirmed OR • Incident Record (S2) - confirmation that incident remains unresolved	• Service Provider (Service Desk)
5.6	Confirmed?	If the incident resolution is confirmed, go to step 6.1. If not, go back to step 4.1.	n/a	n/a	n/a

No.	Activity	Description	Inputs	Outputs	Responsible
Stage 6: Incident Closure					
6.1	Close incident	If the incident resolution has been confirmed, the Service Desk close the incident. The Service Desk will also inform the user who reported the incident that the incident has been closed. If the incident has occurred several times, a problem record may need to be opened to investigate the root cause. Note: If the incident proves subsequently not to have been fixed, a new incident will have to be raised.	• Incident Record (S2) - resolution confirmed	• Incident Record (S2) - closed • Problem Management Process (S10) • User informed of incident closure	• Service Provider (Service Desk)
Stage 7: Incident Monitoring					
7.1	Continuous monitoring of on-going incident resolution	The continuous monitoring of the on-going incident resolution is performed by the SI Incident Management Lead using different approaches, for example: • Check open incidents in periodic time slots to verify resolution status. • Check progress updates in service management tool. • Evaluate impact of any unforeseen difficulties on incident resolution. • Regularly check if counter-steering in incident resolution is necessary based on KPIs. • Regularly check if SLAs / OLAs are about to fail. • Regularly check known error and workaround database.	• Incident Records (S2) • Progress updates • Incident status information • SLA / OLAs (S11) • KPIs • Known errors • Workarounds	• Performed monitoring • Analysed incident resolution	• SI Incident Management Lead
7.2	Continuous monitoring of provider collaboration	The continuous monitoring of on-going provider collaboration is performed using different approaches, for example: • Check incident records on number of requests for re-assignment, re-prioritisation and verification of incident record. • Evaluate impact of any unforeseen difficulties or problems which occurred during resolution activities.	• Incident Records (S2)	• Performed monitoring • Analysed provider collaboration	• SI Incident Management Lead
7.3	Decide on necessity to get involved in incident resolution	Decide on getting involved in the 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. If involvement is necessary, the SI Incident Management Lead may become involved in the relevant activity within the process.	• Performed monitoring • Analysed incident resolution • Analysed provider collaboration	• Involvement in incident resolutions necessary OR • Involvement in incident resolutions not necessary	• SI Incident Management Lead

No.	Activity	Description	Inputs	Outputs	Responsible
7.4	Conduct service integration meetings, if necessary	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. During the service integration meeting, the SI Incident Management Lead moderates the session, ensuring fair and productive feedback and a focus on issue resolution. The invited Service Provider (Service Desk) and Service Provider (Operations) representatives actively participate in the service integration meeting providing options for issue resolution. The SI Incident Management Lead documents and communicates the decisions made in the meeting. If any service improvements are identified during this meeting, they will be fed into the Continual Service Improvement Process.	• Service integration meeting required • Service integration meeting schedule and agenda (S12)	• Service integration meeting minutes (S13) • Continual Service Improvement Process (S14)	• All

4 ROLES AND RESPONSIBILITIES

	Activity	**Service Integrator** Incident Management Lead	**Service Provider** Service Desk	**Service Provider(s)** Operations	**User**
	Stage 1: Incident Identification				
1.1	Identify incident				R / A
1.2	Raise incident in self-service tool		I		R / A
1.3	Call service desk to report incident		I		R / A
	Stage 2: Incident Logging				
2.1	Auto incident creation		R / A		
2.2	Manual incident creation		R / A		C
2.3	Validate details	C	R / A		C
2.4	Categorise	C	R / A		
2.5	Prioritise	C	R / A		
	Stage 3: Incident Triage				
3.1	Determine incident type	(R)	R / A		C
3.2	Update existing incident		R / A		I
	Stage 4: Incident Investigation				
4.1	Research available resolutions		R / A		C
4.3	Assign incident	C	R / A	C	
4.4	Track and monitor incident		R / A	C	I
4.5	Review incident and assign to relevant resources			R / A	
4.6	Review incident			R / A	C
4.8	Identify resolution		I	R / A	
	Stage 5: Incident Resolution				
5.2	Raise RFC	I	I	R / A	I
5.3	Apply resolution		I	R / A	I
5.5	Confirm resolution		C	I	R / A

	Activity	**Service Integrator** Incident Management Lead	**Service Provider** Service Desk	**Service Provider(s)** Operations	**User**
	Stage 6: Incident Closure				
6.1	Close incident		R / A	I	I
	Stage 7: Incident Monitoring				
7.1	Continuous monitoring of on-going incident resolution	R / A	C	C	
7.2	Continuous monitoring of provider collaboration	R / A	C	C	
7.3	Decide on necessity to get involved in incident resolution	R / A	C	C	
7.4	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	Event Management Process	SI Incident Management Lead	Service Knowledge Management System
S2	Incident Record	Service Desk	Service Management Tool
S3	Major Incident Management Process	SI Major Incident Management Lead	Service Knowledge Management System
S4	Request Fulfilment Process	Service Desk	Service Knowledge Management System
S5	Information Security Incident Process	SI Information Security Incident Management Lead	Service Knowledge Management System
S6	Call Routing Plan	Service Desk	Service Management Tool
S7	RFC Template	SI Change Management Lead	Service Management Tool
S8	Change Management Process	SI Change Management Lead	Service Knowledge Management System
S9	Request for Change	SI Change Management Lead	Service Management Tool
S10	Problem Management Process	SI Problem Management Lead	Service Knowledge Management System
S11	SLA / OLA	SI Service Level Management Lead	Service Knowledge Management System
S12	Service Integration Meeting Schedule and Agenda	SI Incident Management Lead	Service Knowledge Management System
S13	Service Integration Meeting Minutes	SI Incident Management Lead	Service Knowledge Management System
S14	Continual Service Improvement Process	SI Continual Service Improvement Lead	Service Knowledge Management System

6 GLOSSARY

Incident	“An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident - for example, failure of one disk from a mirror set.” *(ITIL definition)*
Incident Record	“A record containing the details of an incident. Each incident record documents the lifecycle of a single incident.” *(ITIL definition)*
ITIL	IT Infrastructure Library
KPI	Key Performance Indicator
OLA	Operational Level Agreement
RFC	Request for Change
SI	Service Integrator
SIAM	Service Integration and Management
SKMS	Service Knowledge Management System
SLA	Service Level Agreement