Incident Management Process, Use Case & Data

Table of Contents

Created by:	Business & Data Layer Tiger Teams
Version:	FINAL
Date completed:	December 4, 2017

Purpose

The purpose of this document is to communicate the findings of the Business & Data Layer Tiger Teams as it relates Package A to the GC ITSM WG.

The purpose of the Business and Data Layer Tiger teams is to provide specific deliverables related to interdepartmental business-level processes and data that is required to transit between departments to support those processes.

Terminology

Data Statements

Steps often require the transfer, recording, or modification of data, referred to here as the "Data Statement". Any step written in a fashion that would require multiple Data Statements depending upon some criteria, should be decomposed into sub-steps so that only one Data Statement per step is required.

Data Statement Syntax

Data Statements are in bullet form with formatting consistent with the following:

- Normal Text – Indicates that the data is not mandatory and is freeform with no expected convention
- Normal Text* – Indicates that the data is mandatory and must be provided to complete the current step or move to the next step
- *Italics* – Indicates that the data is very likely to be system-generated
- (Round Bracketed Text) – Indicates that the data is expected to conform to a known and documented convention, such as the naming of a server or a room or a person's name, such as "Last, First"
- [Square Bracketed Text] – Indicates that the data is expected to conform to a known list of values, such as a listed and ranked Priority

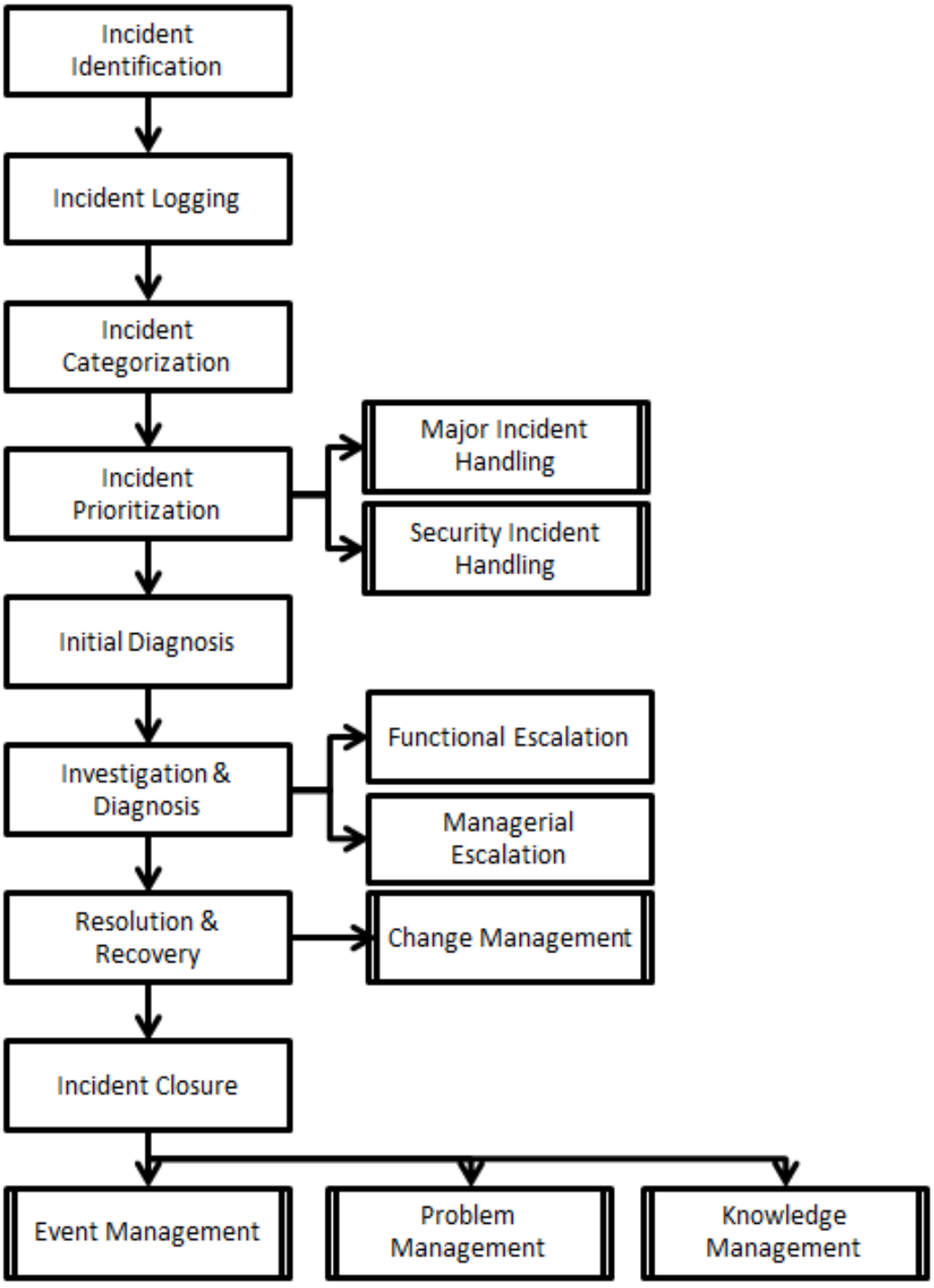
The syntax can be combined in any way, however, Normal* and Normal are considered mutually exclusive, as are Round and Square brackets. For example:

- [Urgency*] – Mandatory data that must also conform to a known list of values
- *Submission Date** – A mandatory value that is very likely automatically generated

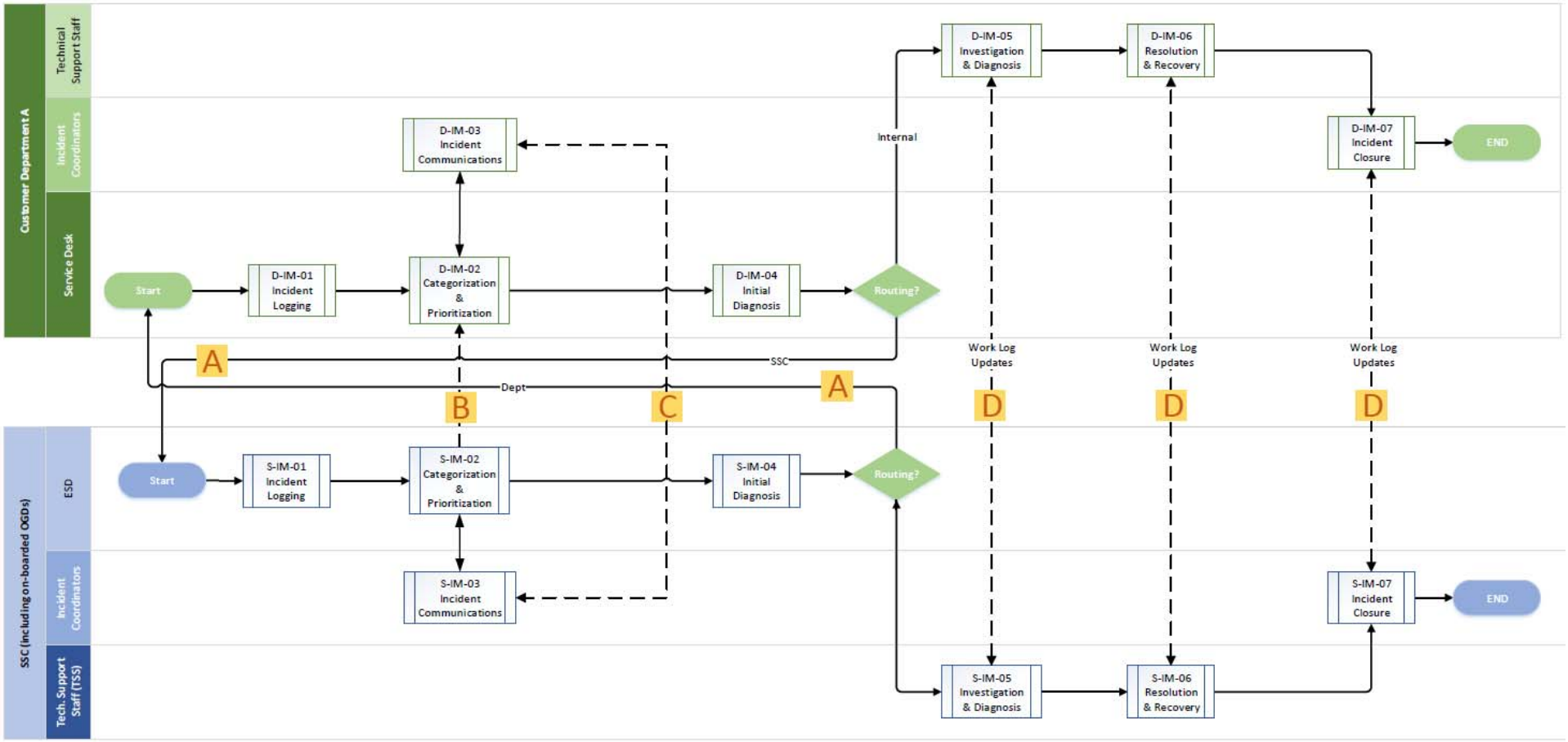
Incident Management Data Elements

A	B	C	D
· [End User Department]* · (End User) · [Affected CI] * · [Affected Technical Service]* · (End User Email) · (End User Phone) · [Category - Incident]* · Short Description* · Detailed Description · [Location]* · [Impact]* · [Urgency]* · [Priority]* · Work Log Entry* · [Contact Department]* · (Dept Technical Support Contact Name)* · (Dept Technical Support Contact Email)* · (Dept Technical Support Contact Phone)* · *Dept ITSM Incident ID**	· *SSC ITSM Incident ID** · *Dept ITSM Incident ID** · [Ticket Status]* · Work Log Entry* · (SSC Technical Support Contact Name)* · (SSC Technical Support Contact Email)* · (SSC Technical Support Contact Phone)*	· *SSC ITSM Incident ID** · *Dept ITSM Incident ID** · [Ticket Status]* · [Impact]* · [Urgency]* · [Priority]* · Short Description* · Detailed Description · Work Log Entry* · (Estimated TTR)*	· *Dept ITSM Incident ID** · [Ticket Status]* · Short Description* · Detailed Description · Work Log Entry* · [Resolution code]*

High-Level Incident Management Process Diagram



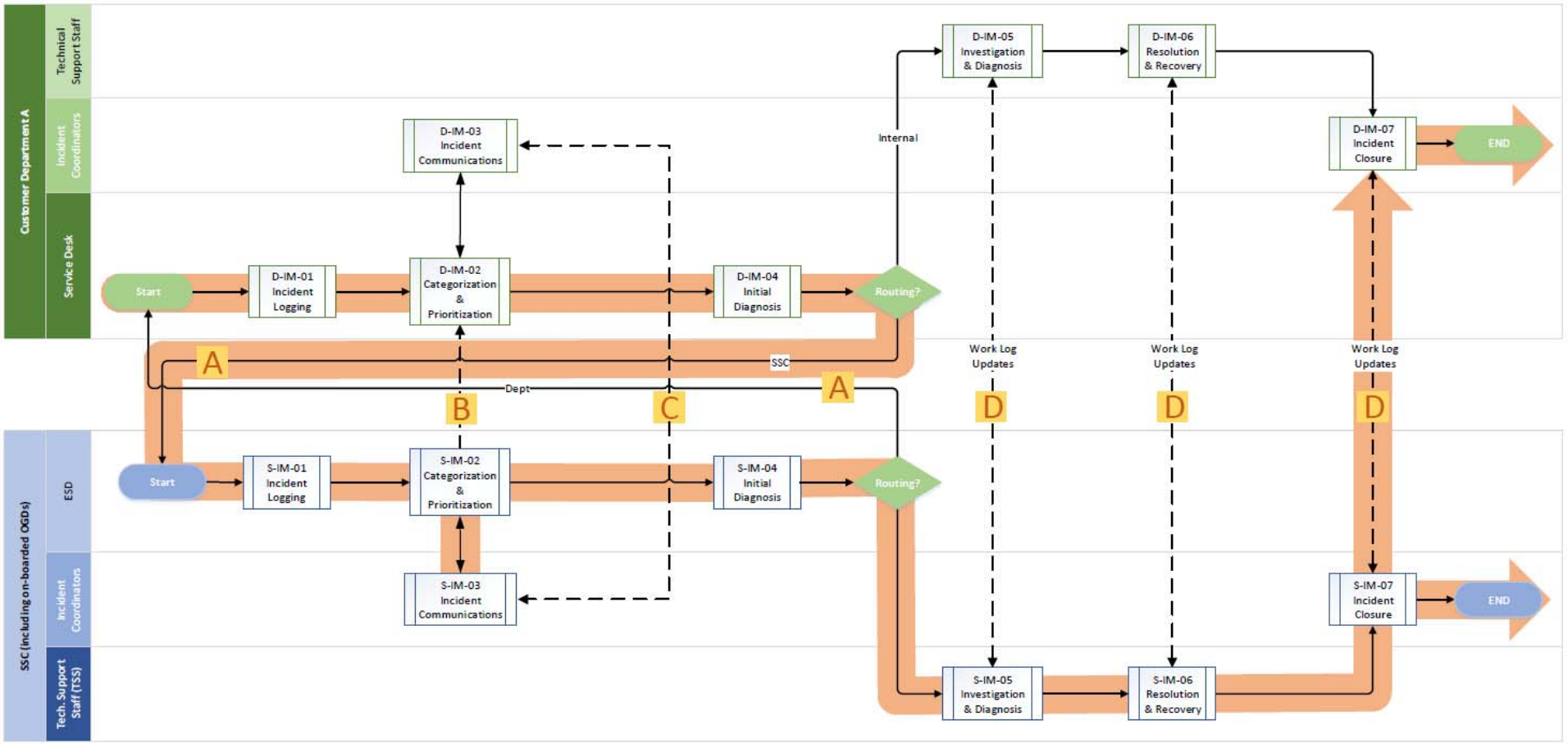
Incident Management Process Flow Diagram



Incident Management Generic Use Case

Description	Supports the identification and recovery of service failures, supported by SSC.	
Primary Role	Department A - Service Desk	
Secondary Roles	Department A - Technical Support Staff - Incident Coordinator	SSC - Service Desk - Incident Coordinator - Technical Support Staff
Successful end condition	Service restored to user in time frame allowed by SLA	
Failure end condition	Service not restored to user in time frame allowed by SLA	
Trigger	Service Failure reported by user (employee of Department A)	
Successor	Problem Management Change Management Knowledge Management	Continual Service Improvement Service Asset and Configuration Management
Assumptions	• Users (non-IT staff) in Department A consume SSC services both directly (email and videoconferencing) and indirectly (infrastructure services supporting Department A solutions). This use case only applies to services provided by SSC and consumed by users of Department A. Therefore, certain situations are out of scope: (1) the provision of IT services by Department A to users from a third department and (2) the consumption of IT services supplied by a third department by SSC. • Department A and SSC each have their own ITSM Solutions (and there are some automated linkages possible between these tools) and their own Service Desks. • Only the Department A Service Desk will be able to report incidents to SSC. • This use case does not describe the interaction within Department A and the users of its IT services prior to the service failure being reported to SSC. • There is a standard method to calculate the priority of an incident which will be created based on its impact and urgency. • Category and priority on this activity will be aligned between the SSC and Department A to ensure there is no clashing priorities	

Process Flow Diagram



Activities

Task No.	Activity	Role	Task	Interaction	Data Statement
D-IM-01	Incident Logging	Department A Service Desk	User reports service failure.	Department A (D)	
D-IM-02	Categorization and Prioritization	Department A Service Desk	Categorize and prioritize incident.	D	
D-IM-04	Initial Diagnosis	Department A Service Desk	Perform initial diagnosis of the incident. Perform incident matching to existing records. Determine that the fault is with an SSC service.	D	
S-IM-01	Incident Logging	SSC Service Desk	Dept. A Service Desk reports service failure.	D >> SSC	A
S-IM-02	Categorization and Prioritization	SSC Service Desk	Categorize and prioritize incident. Notify Dept. A service desk that an SSC incident record has been created, providing the SSC identifier so Dept. A can update their record.	SSC >> D	B
S-IM-04	Initial Diagnosis	SSC Service Desk	Perform incident matching to existing records. Identify all stakeholders affected by the service failure. Assign to appropriate support resources.	SSC	
S-IM-03	Incident Communications - Notifications/Oversight and Escalation	SSC Incident Coordinator	Communicate current incident status to all stakeholders so that users can adjust to the interruption and to decrease user inquiries. [Additional notifications will be issued as required until	SSC >> D	C

Task No.	Activity	Role	Task	Interaction	Data Statement
			the incident is resolved.]		
S-IM-05	Investigation and Diagnosis	SSC Technical Support Staff	Document actions performed to diagnose the source of the service failure and identify remedial action required. Validate/update categorization and prioritization matrix. Where necessary, contact Dept. A technical resource to coordinate incident Investigation and diagnosis.	SSC >> D	D
D-IM-05	Investigation and Diagnosis	Dept. A Technical Support Staff	Document actions performed to diagnose the source of the service failure and identify remedial action required. Validate/update categorization and prioritization matrix. Where necessary, contact SSC technical resource to coordinate incident investigation and diagnosis.	D >> SSC	D
S-IM-06	Resolution and Recovery	SSC Technical Support Staff	Implement resolution. Where necessary, contact Dept. A technical resource to coordinate incident resolution and recovery. If RFC required, perform *Change Management*. **Note**: There may be interdepartmental interaction in this process to complete the change.	SSC >> D	D
D-IM-06	Resolution and Recovery	Dept. A Technical Support Staff	Implement resolution. Where necessary, contact SSC technical resource to coordinate incident resolution and recovery. If RFC required, perform *Change Management*. **Note**: There may be interdepartmental interaction in this process to complete the change.	D >> SSC	D

Task No.	Activity	Role	Task	Interaction	Data Statement
S-IM-07	Incident Closure	SSC Incident Coordinator	Provide final quality control to incident record before it is closed. Ensure any subsequent processes are supported. Validate information on incident record and generate post-incident report for high and critical incidents. Issue final Incident Notification to stakeholders. If a problem record must be created or updated, perform *Problem Management*. If a Knowledge Article/FAQ update is required, proceed to *Knowledge Management*. If the configuration information in the CMDB was incomplete or inaccurate, proceed to *Service Asset and Configuration Management.*	SSC >> D	D
D-IM-07	Incident Closure	Dept. A Incident Coordinator	Provide final quality control to incident record before it is closed. Ensure any subsequent processes are supported. Validate information on incident record and generate post-incident report for high and critical incidents. If problem record to be created / updated – *perform Problem Management*. If Knowledge Article/FAQ update required, *go to Knowledge Management.* If the configuration information in the CMDB was incomplete or inaccurate, go to *Service Asset and Configuration Management.*	D	

Incident Management Use Case Example: Web Application Not Working

Process Flow Diagram

Same path as Generic

Activities

Task No.	Activity	Role	Task	Interaction	Data Statement
START	Contacting the Service Desk	DND End User	Sally Sampson's Web application is not working and she calls the service desk to report an incident.	DND	
D-IM-01	Incident Logging	DND Service Desk	Frankie Foster (DND Service Desk) receives Sally's call and creates a new incident request record. Frankie gathers information from Sally about the incident	DND	
D-IM-02	Categorization and Prioritization	DND Service Desk	Frankie categorizes and prioritizes the incident.	DND	
D-IM-03	Initial Diagnosis	DND Service Desk	During the initial diagnosis, Frankie determines that there is a match to existing records. Frankie determines that the issue resides with the Server and not the application. Frankie determines that the issue is with an SSC service. Frankie sends the incident details to SSC for resolution, remembering to include the Technical Support contacts for the application – DND Application Gurus.	DND	
S-IM-01	Incident Logging	SSC Service Desk	Gerry Graham (SSC Service Desk) receives an incident request from Frankie (DND Service Desk). Gerry logs the Incident received from Frankie.	DND>>SSC	A

Task No.	Activity	Role	Task	Interaction	Data Statement
S-IM-02	Categorization and Prioritization	SSC Service Desk	Gerry categorizes and prioritizes the incident. Gerry notifies DND that the service incident has been created, remembering to include the Technical Support contacts – SSC Server Gurus.	SSC >> DND	B
S-IM-04	Initial Diagnosis	SSC Service Desk	Gerry performs incident matching to existing records. Gerry identifies all stakeholders affected by the service failure. Garry assigns the incident to appropriate support resources – SSC Server Gurus.	SSC	
S-IM-03	Incident Communications - Notifications/Oversight and Escalation	SSC Incident Coordinator	Mary Master (SSC Incident Coordinator) communicates the incident status (Server is down) to all stakeholders so that users can adjust to the interruption and to decrease user inquiries. She includes the Estimated Time To Recover (TTR).	SSC >> DND	C
S-IM-05	Investigation and Diagnosis	SSC Technical Support Staff	The SSC Server Gurus document the actions performed to diagnose the source of the service failure and to identify the remedial action required. There is no need to validate or update the categorization and prioritization matrix. The SSC Server Gurus contact the DND Application Gurus to assist with the incident investigation and diagnosis. Work logs are updated with activities/decisions made.	SSC >> DND	D
D-IM-05	Investigation and Diagnosis	DND Technical Support Staff	The DND Application Gurus document the actions performed to diagnose the source of the service failure and to identify the remedial action required.	DND >> SSC	D

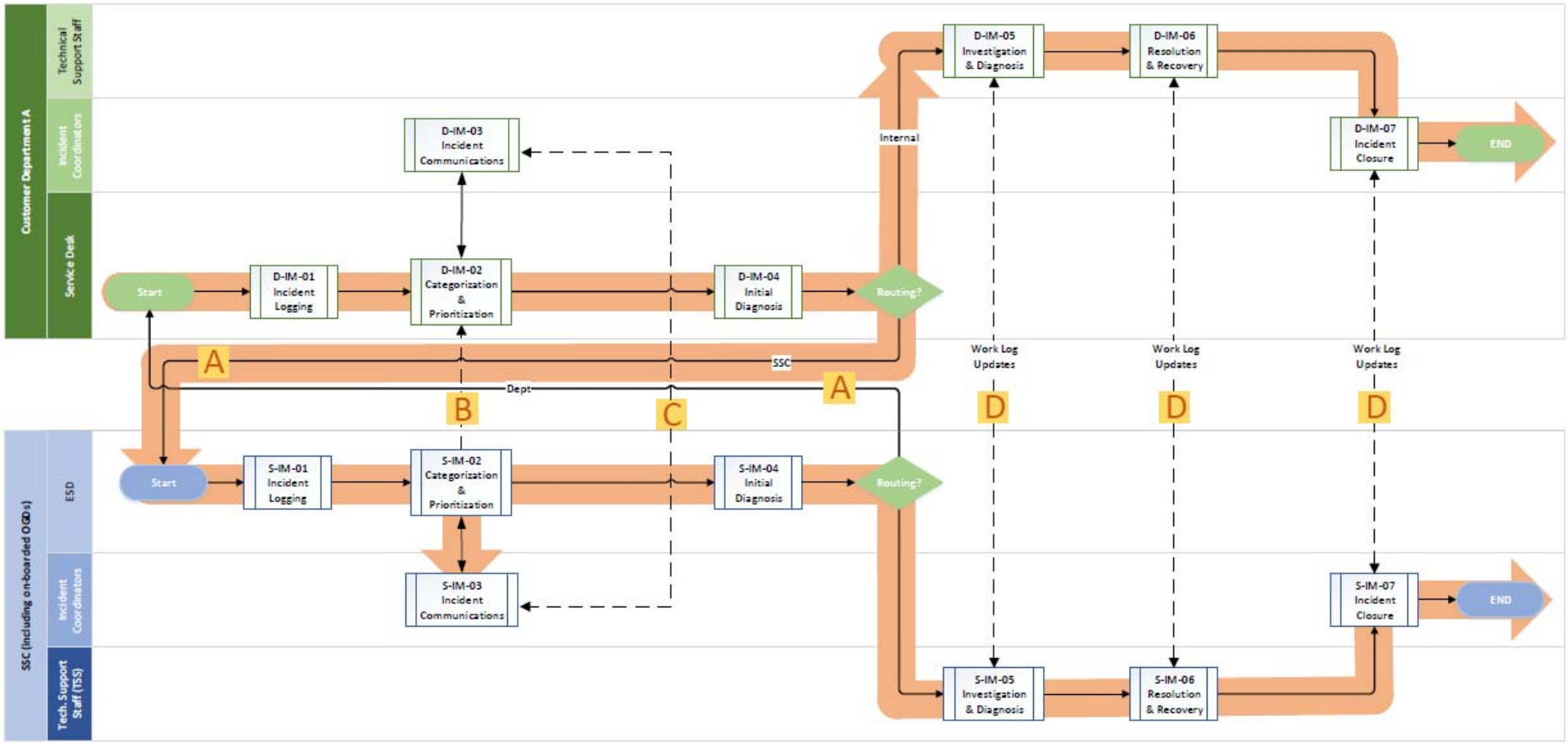
Task No.	Activity	Role	Task	Interaction	Data Statement
			There is no need to validate or update the categorization and prioritization matrix. The DND Application Gurus respond to the SSC Server Gurus' collaboration request. Work logs are updated with activities/decisions made		
S-IM-06	Resolution and Recovery	SSC Technical Support Staff	The SSC Server Gurus implement a resolution. The SSC Server Gurus work and communicate with the DND Application Gurus throughout the resolution and recovery process. Work logs are updated with activities/decisions made	SSC >> DND	D
D-IM-06	Resolution and Recovery	DND Technical Support Staff	The DND Application Gurus work and communicate with the SSC Server Gurus throughout the resolution and recovery process. Work logs are updated with activities/decisions made	DND >> SSC	D
S-IM-07	Incident Closure	SSC Incident Coordinator	Mary Master (SSC Incident Coordinator) conducts a final quality control to the incident record before it is closed and ensures that any subsequent processes (Event, Problem, Knowledge, Change Management or SACM) are supported. Mary validates information on the incident record and generates a post-incident report for high and critical incidents. Mary issues a final Incident Notification to stakeholders.	SSC >> DND	D
D-IM-07	Incident Closure	DND Incident Coordinator	Andrew Applewood (DND Incident Coordinator) conducts final quality control to the incident record before it is closed	DND	

Task No.	Activity	Role	Task	Interaction	Data Statement
			and ensures that any subsequent processes (Event, Problem, Knowledge, Change Management or SACM) are supported. Andrew validates information on the incident record. As it was not a high and critical incident, no report is generated. Andrew sends a notification to all Stakeholders.		
END	Notification Received	DND End User	Sally is notified that her incident has been resolved.	DND	

Incident Management Use Case – Critical

Description	Ensure rapid identification of critical incidents and facilitate the assignment of all resources necessary to secure service restoration.	
Primary Role	SSC - Incident Coordinator	
Secondary Roles	Department A - Service Desk - Technical Support Staff - Incident Coordinator	SSC - Service Desk - Incident Manager - Technical Support Staff
Successful end condition	Service restored to user in time frame allowed by SLA	
Failure end condition	Service not restored to user in time frame allowed by SLA	
Trigger	Service Failure reported by user (employee of Department A)	
Successor	Change Management Problem Management Knowledge Management Continual Service Improvement Service Asset and Configuration Management	
Assumptions	Clear and approved criteria for declaring a Critical Incident.	

Process Flow Diagram



Activities

Task No.	Activity	Role	Task	Interaction	Data Statement
START D-IM-01 D-IM-02 D-IM-04 S-IM-01	As per Generic IM Use Case activities - *Incident Logging* - *Categorization and Prioritization* - *Initial Diagnosis* - *Incident Logging*				A
S-IM-02	Categorization and Prioritization	SSC Service Desk	Categorize and prioritize incident. Determine that this is a critical priority incident. Notify Dept. A Service Desk that incident has been created.	SSC >> D	B
S-IM-04 S-IM-03	As per Generic IM Use Case activities - *Initial Diagnosis* - *Incident Communications - Notifications Oversight and Escalation*				
S-IM-03	Incident Communications - Initiate Critical Incident Management	SSC Incident Coordinator	Obtain background information about the incident including affected services and customers. Send initial critical incident notification to all customers. [Additional notifications will be issued to stakeholders in affected departments ONLY, as required, until the incident is resolved.]	SSC >> D	C
S-IM-03	Incident Communications - Initiate Critical Incident Management	SSC Incident Coordinator	Contact Dept. An Incident Coordinator to secure additional resources, if required.	SSC >> D	C

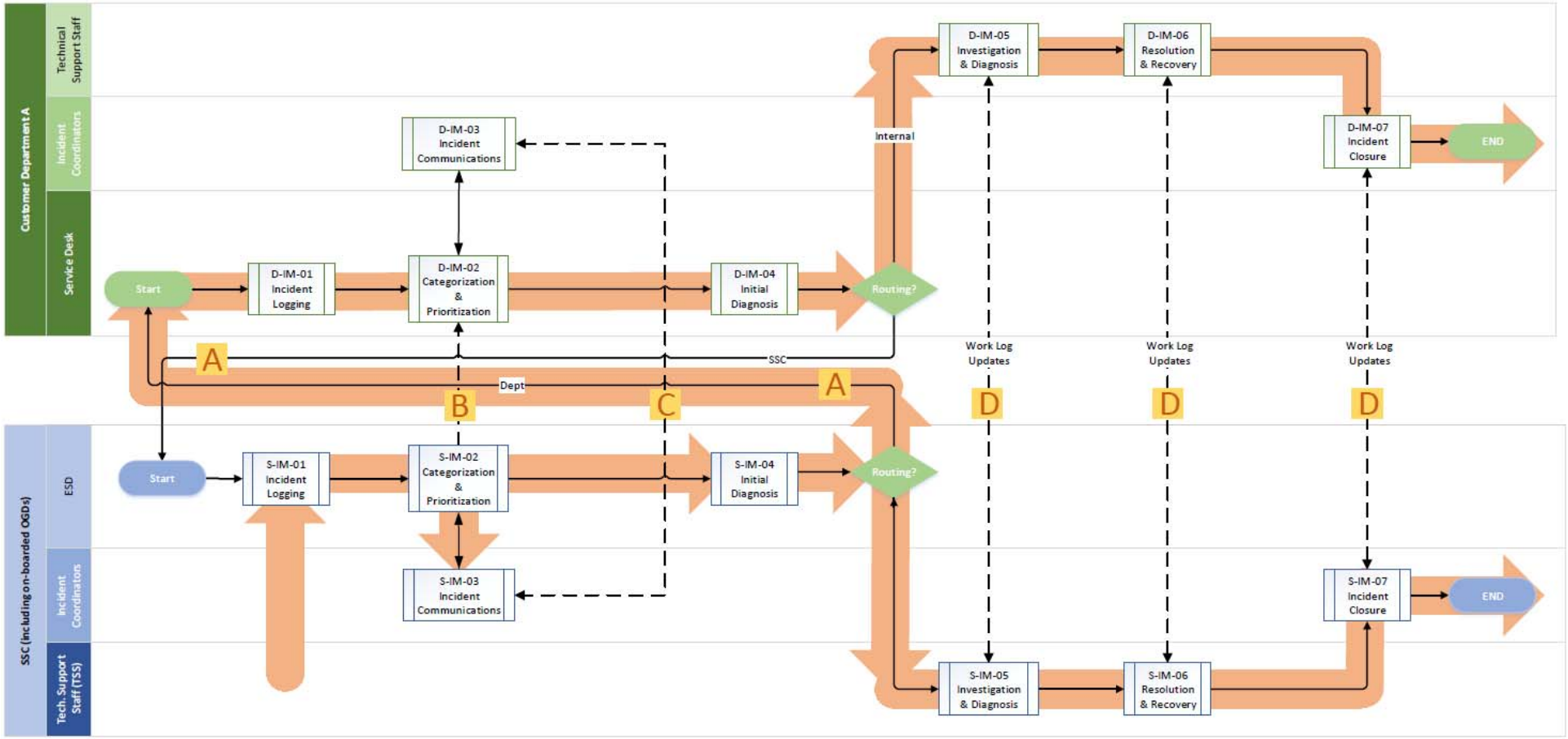
Task No.	Activity	Role	Task	Interaction	Data Statement
S-IM-05 D-IM-05 S-IM-06 D-IM-06	As per Generic IM Use Case activities - *Investigation and Diagnosis* - *Investigation and Diagnosis* - *Resolution and Recovery* - *Resolution and Recovery*				D
S-IM-07	Incident Closure	SSC Incident Coordinator	Provide final quality control to incident record before it is closed. Ensure any subsequent processes are supported. Validate information on incident record and generate post-incident report because this is a critical incident. Issue final Incident Notification to stakeholders across all partners. If problem record must be created or updated, perform *Problem Management*. If a Knowledge Article/FAQ update is required, proceed to *Knowledge Management*. If the configuration information in the CMDB was incomplete or inaccurate, proceed to *Service Asset and Configuration Management.*	SSC >> D	D
D-IM-07	Incident Closure	Dept. A Incident Coordinator	Provide final quality control to incident record before it is closed. Ensure any subsequent processes are supported. Validate information on incident record and generate post-incident report for high and critical incidents. If a problem record must be created or updated, perform *Problem Management*. If a Knowledge Article/FAQ update is required, proceed to *Knowledge Management*.	D	

Task No.	Activity	Role	Task	Interaction	Data Statement
			If the configuration information in the CMDB was incomplete or inaccurate, proceed to *Service Asset and Configuration Management.*		

Incident Management Use Case – Security

Description	To ensure the appropriate and rapid response to security incidents.	
Primary Role	SSC - Security Operations Centre [as Technical Support Staff]	
Secondary Roles	Department A - Service Desk - Incident Coordinator - Technical Support Staff	SSC - Service Desk - Incident Coordinator - Technical Support Staff
Successful end condition	Implement actions to contain or resolve security incident.	
Failure end condition	Delays in implementing actions to contain or resolve security incident.	
Trigger	Security incident identified by SSC Security Operations Centre that requires immediate action by SSC to contain or resolve.	
Successor	Problem Management Change Management Knowledge Management Continual Service Improvement	
Assumptions	More detail on the Security Incident Management process is provided in the GC Cyber Security Event Management Plan. Security incidents are tracked and managed by the SSC's Security Operations Centre outside of the ITSM solution. The Security Operations Centre will report an incident to SSC's Service Desk in order to secure the immediate action of other Technical Support Resources to contain or resolve the security incident. Impact-Urgency-Priority (IUP) categorization will allow a higher prioritization for incidents reported by Security Operations Centre in order to ensure immediate response.	

Process Flow Diagram



Activities

Task No.	Activity	Role	Task	Interaction	Data Statement
START	Incident Identification	SSC Technical Support Resource	Security Operations Centre immediately identifies actions required to contain or resolve a security incident.	SSC	
S-IM-01	Incident Logging	SSC Service Desk	Security Operations Centre reports service failure.	SSC	
S-IM-02	Categorization and Prioritization	SSC Service Desk	Categorize and prioritize incident.	SSC	
S-IM-04	As per generic IM use case S-IM-04 - *Initial Diagnosis*				A
S-IM-03	Incident Communications – Notifications/Oversight and Escalation	SSC Incident Coordinator	If it is determined that the action to contain or resolve the security will cause a service failure, communicate incident status to all stakeholders so that users can adjust to the interruption and to decrease user inquiries. [Additional notifications will be issued as required until the incident is resolved.]	SSC >> D	C
D-IM-01 D-IM-02 D-IM-04	*As per generic IM use case* - *Incident Logging* - *Categorization and Prioritization* - *Initial Diagnosis*				
S-IM-05 D-IM-05 S-IM-06 D-IM-06 S-IM-07 D-IM-07	As per Generic IM Use Case activities - *Dept - Investigation and Diagnosis* - *SSC - Investigation and Diagnosis* - *Dept - Resolution and Recovery* - *SSC - Resolution and Recovery* - *Dept - Incident Closure* - *SSC - Incident Closure*				D

Incident Management Data Definitions

Data set	GC Label	GC Description	Mandatory	Keyed Text	Drop-Down	System-Gen	Convention
A	Affected CI	Component impacting or related to the service.	X		X		
A	Affected Technical Service	List of SSC technical service(s) that have been affected by the Incident.	X		X		
A	Category - Incident	A category is the symptom of the incident, to know to whom to assign it. It is one of the following values: **Business** **Technical**	X		X		
A	Contact Department	Department name of the party who initiated the incident – on behalf of the end user.	X		X		
A,B,C,D	Department ITSM Incident ID	Unique identifier for a Department ITSM Incident.	X			X	
A	Dept Technical Support Contact Email	Technical Support contact's email address of originating department.	X	X			X
A	Dept Technical Support Contact Name	Technical Support contact's first and last name of originating department.	X	X			X
A	Dept Technical Support Contact	Technical Support contact's phone number of originating department. (country code, area code, local code, 4	X	X			X

Data set	GC Label	GC Description	Mandatory	Keyed Text	Drop-Down	System-Gen	Convention
	Phone	digits + extension).					
A,C,D	Detailed Description	Long description of the Incident.		X			
A	End User	The first and last name of the individual who has reported the incident.		X			X
A	End User Department	Department or Agency that reported the Incident.	X		X		
A	End User Email	The End User's Email address.		X			X
A	End User Phone	The End User's Phone number.		X			X
C	Estimated TTR	Estimated time to restore the service.	X	X			X
A,C	Impact	Describes the business impact resulting from the incident.	X		X		
A	Location	Physical location affected by the incident, typically the location of the user experiencing and reporting the incident - may change throughout the process.	X		X		
A,C	Priority	Each priority has a calculated numeric value (impact and urgency) associated (1 to 4) in the database.	X		X		
B,C,D	Ticket Status	Identifies the stage of the incident lifecycle.	X		X		

Data set	GC Label	GC Description	Mandatory	Keyed Text	Drop-Down	System-Gen	Convention
D	Resolution Code	A code assigned to the incident when it is resolved.	X		X		
A,C,D	Short Description	Brief description of the Incident.	X	X			
B,C	SSC ITSM Incident ID	Unique identifier for an SSC ITSM Incident.	X			X	
B	SSC Technical Support Contact Email	SSC Technical Support contact's email address.	X	X			X
B	SSC Technical Support Contact Name	SSC Technical Support contact's first and last name.	X	X			X
B	SSC Technical Support Contact Phone	SSC Technical Support contact's phone number (country code, area code, local code, 4 digits + extension).	X	X			X
A,C	Urgency	An indication of the time before the business is severely impacted.	X		X		
A,B,C,D	Work Log Entry	Running log of actions taken to remedy the situation.	X	X			