Incident Management Process and Procedures

Process and Procedure Information	
Document Name	Incident Management (IM) Process and Procedures
Description	This document describes the life cycle of a typical incident including the step-by-step procedures that facilitate it.
Applicable To	All personnel
Document Owner	Incident Manager

Revision Information			
Version	**Date**	**Author**	**Comment**
0.1	5/3/2017	Weisman	Initial draft

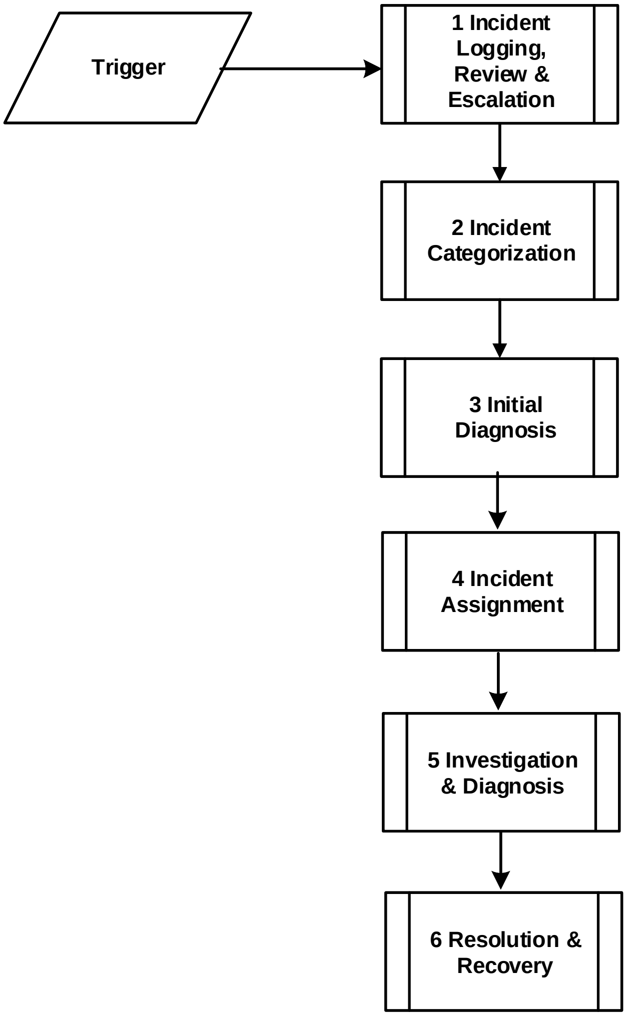
Table of Contents

INCIDENT MANAGEMENT PROCESS

INCIDENT MANAGEMENT PROCESS FLOW DIAGRAM

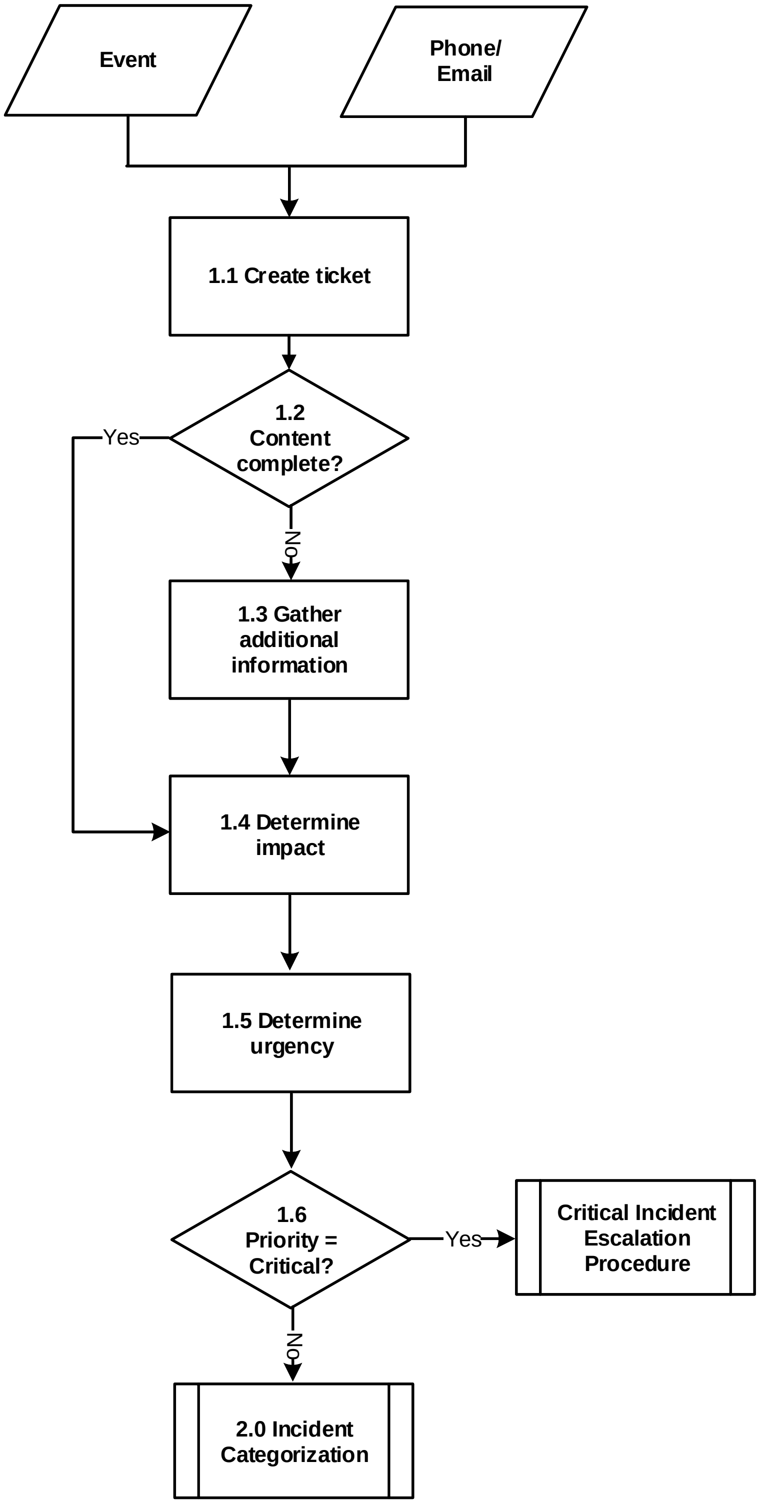
The IM process is comprised of six supporting procedures. These are identified as follows:

1. Incident Logging, Review & Escalation
2. Incident Categorization
3. Initial Diagnosis
4. Incident Assignment
5. Investigation & Diagnosis
6. Resolution & Recovery


Trigger
1 Incident Logging, Review & Escalation
2 Incident Categorization
3 Initial Diagnosis
4 Incident Assignment
5 Investigation & Diagnosis
6 Resolution & Recovery

INCIDENT MANAGEMENT PROCESS FLOW NARRATIVE	
Activity	**Description**
1	**Incident Logging, Review & Escalation** The procedure used to create the incident ticket, verify the necessary information and decide whether it is critical.
2	**Incident Categorization** The procedure used to determine product and operational categorizations.
3	**Initial Diagnosis** The procedure used to determine if this is a new incident or whether it's been encountered before.
4	**Incident Assignment** The procedure used to assign the incident to the appropriate resource.
5	**Investigation & Diagnosis** The procedure used, by the appropriate resource, to determine if the incident was categorized and assigned properly.
6	**Resolution & Recovery** The procedure used to test and verify the solution and close the incident.

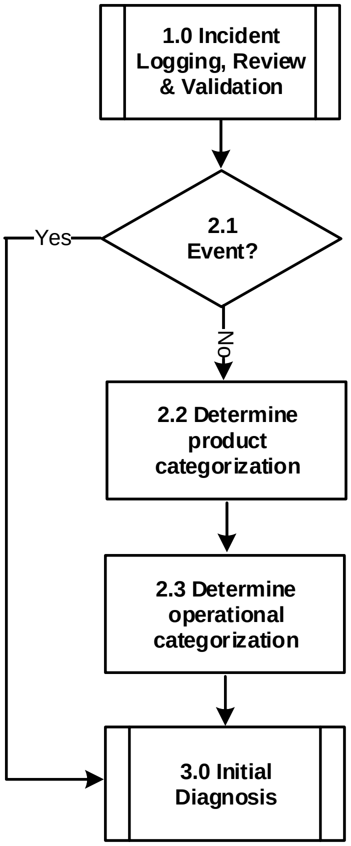
Incident Logging, Review & ESCALATION PROCEDURE Flow Diagram



INCIDENT LOGGING, REVIEW & ESCALATION PROCEDURE FLOW NARRATIVE		
Step	**Responsible Role**	**Procedure**
1.1	Customer Support Desk	All incidents are the result of a trigger from either a monitored event of a configuration item (CI) or someone calling or emailing it in. If the system does not automatically generate a ticket, then it must be created manually in the IT service management (ITSM) database.
1.2	Customer Support Desk	Is the content received from the trigger complete? • If yes, go to step 1.4. • If no, go to step 1.3.
1.3	Customer Support Desk	Gather the necessary information.
1.4	Customer Support Desk	Determine the impact of the incident using the criteria in Appendix 1.
1.5	Customer Support Desk	Determine the urgency of the incident using the criteria in Appendix 1.
1.6	Customer Support Desk	Use Table 1 in Appendix 1 to determine the priority of the incident. Is the priority critical? • If yes, invoke the Critical Incident Escalation Procedure. • If no, go to Procedure 2.0, Incident Categorization.

INCIDENT CATEGORIZATION PROCEDURE

INCIDENT CATEGORIZATION PROCEDURE FLOW DIAGRAM

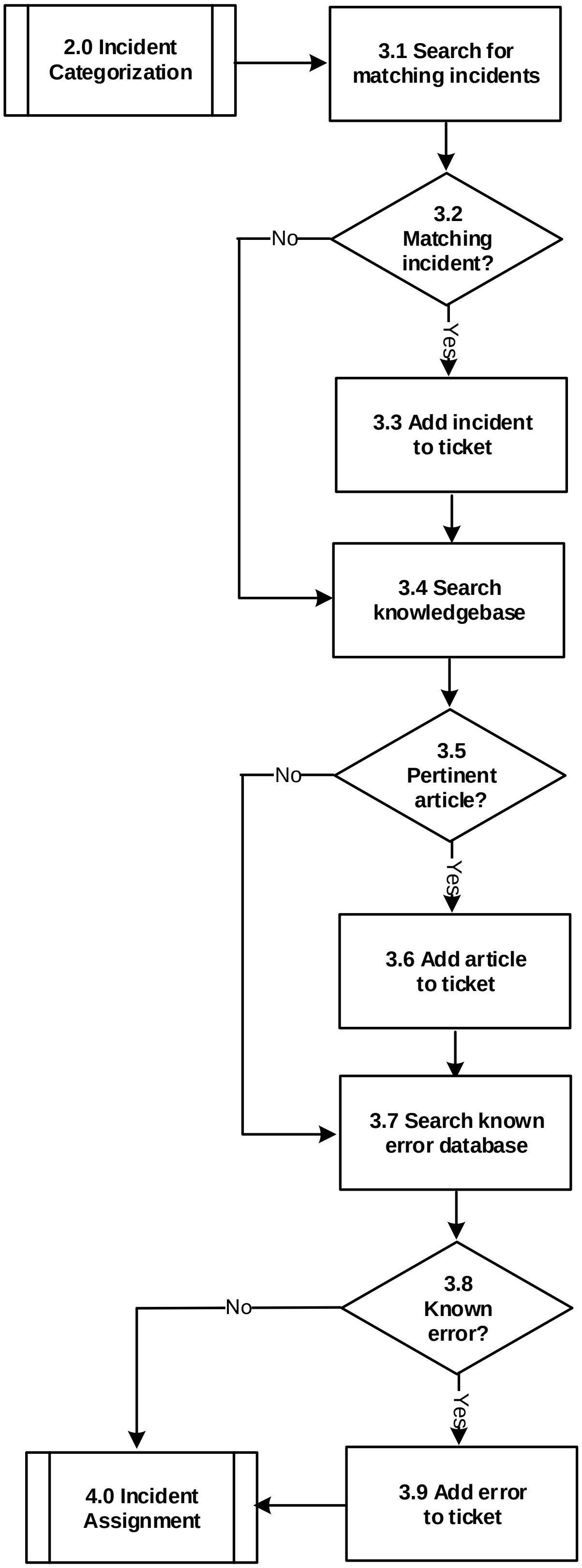

1.0 Incident Logging, Review & Validation
2.1 Event?
Yes
No
2.2 Determine product categorization
2.3 Determine operational categorization
3.0 Initial Diagnosis

INCIDENT CATEGORIZATION PROCEDURE FLOW NARRATIVE

Step	Responsible Role	Procedure
2.1	Customer Support Desk	Did the ticket come from a system-generated event? • If yes, go to Procedure 3.0, Initial Diagnosis. • If no, go to step 2.3.
2.2	Customer Support Desk	Determine product categorization for the ticket.
2.3	Customer Support Desk	Determine operational categorization for the ticket. For a complete list of operational categories, see Appendix 2. Go to Procedure 3.0, Initial Diagnosis.

INITIAL DIAGNOSIS PROCEDURE

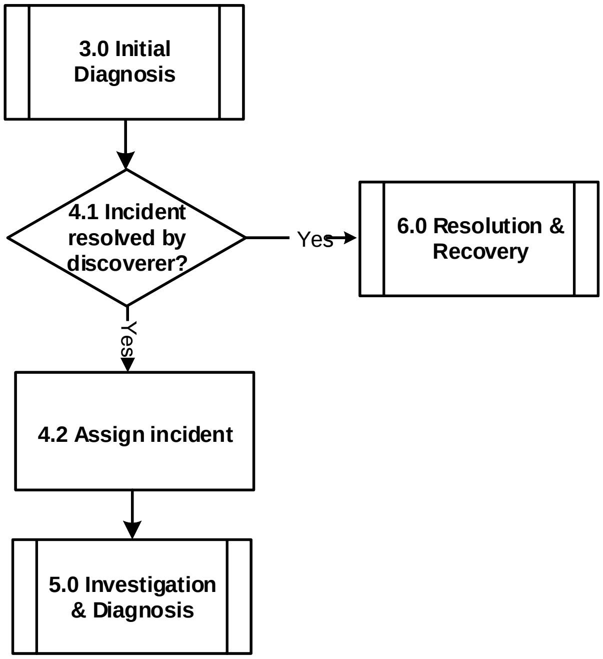
INITIAL DIAGNOSIS PROCEDURE FLOW DIAGRAM



INITIAL DIAGNOSIS PROCEDURE FLOW NARRATIVE		
Step	**Responsible Role**	**Procedure**
3.1	Customer Support Desk	Search for similar incidents in ITSM database using keywords.
3.2	Customer Support Desk	Any similar incidents? • If yes, go to step 3.3. • If no, go to step 3.4.
3.3	Customer Support Desk	Add incident information from that incident to the current incident.
3.4	Customer Support Desk	Search the ITSM knowledge base for articles related to this incident.
3.5	Customer Support Desk	Are there any pertinent articles? • If yes, go to step 3.6. • If no, go to step 3.7.
3.6	Customer Support Desk	Attach the article to the incident.
3.7	Customer Support Desk	Search the Known Error Database for errors related to this incident.
3.8	Customer Support Desk	Are there any related known errors? • If yes, go to step 3.9. • If no, go to Procedure 4.0, Incident Assignment.
3.9	Customer Support Desk	Add the known error information to the ticket and then go to Procedure 4.0, Incident Assignment.

Incident Assignment Procedure

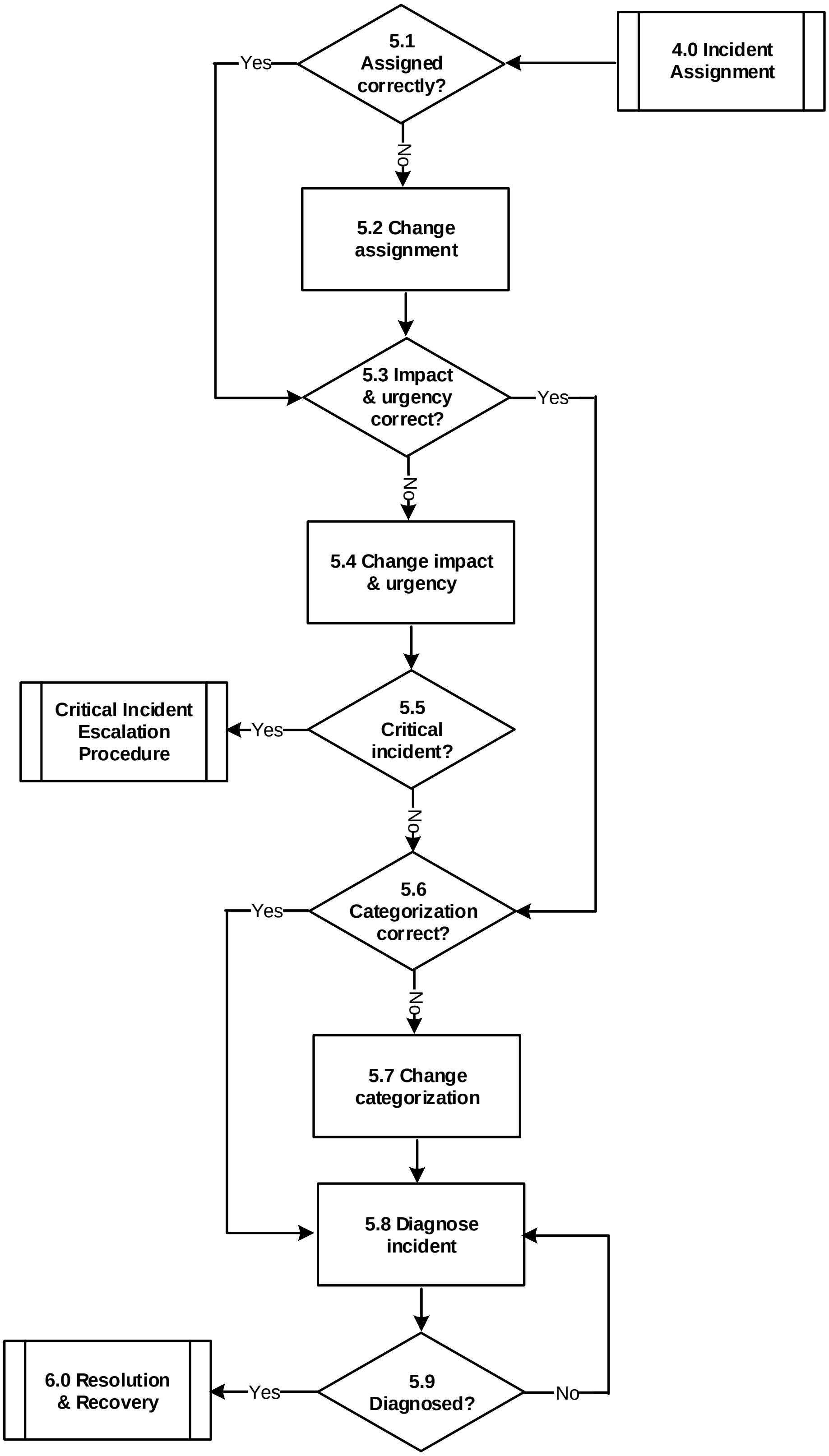
Incident Assignment Flow Diagram


3.0 Initial Diagnosis
4.1 Incident resolved by discoverer?
Yes
6.0 Resolution & Recovery
Yes
4.2 Assign incident
5.0 Investigation & Diagnosis

INCIDENT ASSIGNMENT PROCEDURE FLOW NARRATIVE		
Step	**Responsible Role**	**Procedure**
4.1	Customer Support Desk	Did the person who discovered the incident resolve it? • If yes, go to Procedure 5.0, Investigation & Diagnosis. • If no, go to step 4.2.
4.2	Customer Support Desk	Assign the incident to the appropriate Support Engineer and then go to Procedure 5.0, Investigation & Diagnosis.

INVESTIGATION & DIAGNOSIS PROCEDURE

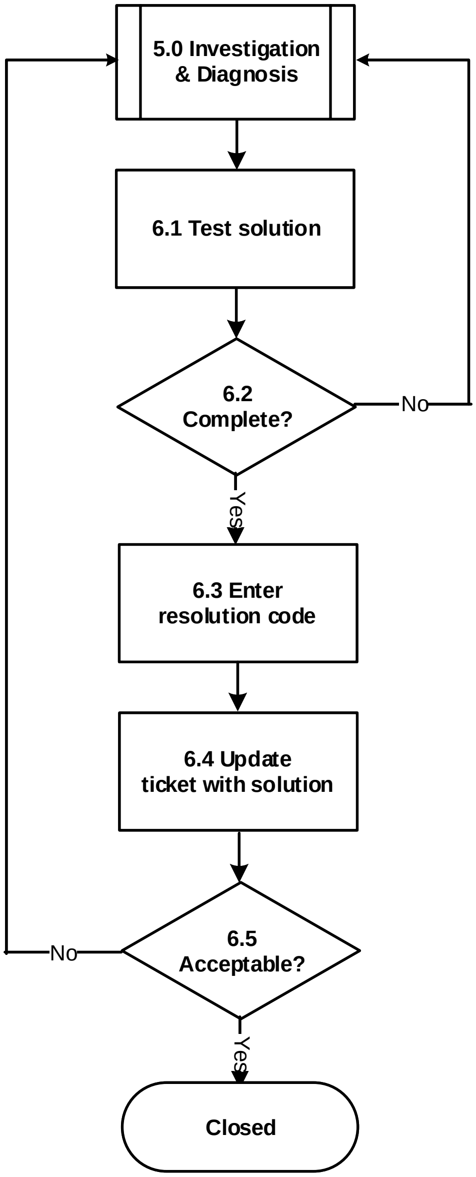
INVESTIGATION & DIAGNOSIS FLOW DIAGRAM



4.0 Incident Assignment
5.1 Assigned correctly?
Yes
No
5.2 Change assignment
5.3 Impact & urgency correct?
Yes
No
5.4 Change impact & urgency
5.5 Critical incident?
Yes
Critical Incident Escalation Procedure
No
5.6 Categorization correct?
Yes
No
5.7 Change categorization
5.8 Diagnose incident
5.9 Diagnosed?
Yes
6.0 Resolution & Recovery
No

INVESTIGATION & DIAGNOSIS PROCEDURE FLOW NARRATIVE		
Step	**Responsible Role**	**Procedure**
5.1	Tier 2/Tier 3 Support	Was the ticket assigned to the correctly? • If yes, go to step 5.3. • If no, go to step 5.2.
5.2	Tier 2/Tier 3 Support	Change the assignment in the ITSM database to the correct one.
5.3	Tier 2/Tier 3 Support	Were the impact and urgency set correctly? • If yes, go to step 5.6. • If no, go to step 5.4.
5.4	Tier 2/Tier 3 Support	Correct the impact and/or urgency in the ITSM database.
5.5	Tier 2/Tier 3 Support	Is the incident a critical incident? • If yes, invoke the Critical Incident Escalation Procedure. • If no, go to step 5.6.
5.6	Tier 2/Tier 3 Support	Were the categorizations set correctly? • If yes, go to step 5.9. • If no, go to step 5.7.
5.7	Tier 2/Tier 3 Support	Correct the categorization in the ITSM database.
5.8	Tier 2/Tier 3 Support	Diagnose the incident.
5.9	Tier 2/Tier 3 Support	Has the incident been diagnosed? • If yes, go to Procedure 6.0, Resolution & Recovery. • If no, go to step 5.8.

RESOLUTION & RECOVERY FLOW DIAGRAM


5.0 Investigation & Diagnosis
6.1 Test solution
6.2 Complete?
No
Yes
6.3 Enter resolution code
6.4 Update ticket with solution
6.5 Acceptable?
No
Yes
Closed

RESOLUTION & RECOVERY PROCEDURE FLOW NARRATIVE		
Step	**Responsible Role**	**Procedure**
6.1	Tier 2/Tier 3 Support	Test the solution.
6.2	Tier 2/Tier 3 Support	Is the solution complete? • If yes, go to step 6.3. • If no, go to Procedure 5.0, Investigation & Diagnosis.
6.3	Tier 2/Tier 3 Support	Enter the resolution code into the ITSM database. See Appendix 3 for more information about resolution codes.
6.4	Tier 2/Tier 3 Support	Update the ticket with the details of the solution.
6.5	Tier 2/Tier 3 Support	Is the solution acceptable? • If yes, mark the ticked Resolved. • If no, go to Procedure 5.0, Investigation and Diagnosis.

DEFINITIONS	
CI	Configuration Item
IM	Incident Management
ITSM	IT Service Management

ROLES AND RESPONSIBILITIES	
Role	**Responsibility**
Customer Support Desk	• Records the incident. • Investigates and diagnoses incidents. Includes resolution when possible. • Provides initial support and assigns classifications. • Determines incident ownership. • Provides monitoring, tracking and communication. • Monitor incident details.
Tier 2/Tier 3 Support	• Provides initial support and validates classification and prioritization. • Verifies assignment. • Provide monitoring, tracking, and communication. • Detects possible problems and assigns them to the Problem Management. • Resolve assigned incidents.
Discoverer	• Discovers incidents. • Contacts Helpdesk Analyst and requests help with submitting a ticket.

KEY PERFORMANCE INDICATORS
The percentage of times an incident is resolved in a given timeframe.
The average time it takes to resolve an incident.

REPORTS			
Name	**Description**	**Distribution**	**Schedule**

OWNER APPROVAL			
Date:		**Last Review:**	
Document Owner	Incident Manager		

APPENDIX 1 – TICKET PRIORITIZATION

Incidents are prioritized based on their impact on the system users and the urgency of effecting a repair. The priority is calculated based on the assigned impact and urgency values (see Table 1).

Impact

1. **Extensive/Widespread**

   Affects an entire site or a large number of users and no alternate procedure is known.

2. **Significant/Large**

   Affects only part of the users at a site or a limited number of users or a critical feature/function and no alternate procedure is known.

3. **Moderate/Limited**

   Affects an entire site or a large number of users and an alternate procedure is documented.

4. **Minor/Localized**

   Affects only part of the users at a site or a limited number of users and an alternate procedure is documented.

Urgency

1. **Critical**

   Prevents the accomplishment of an operational or mission-essential capability.

2. **High**

   Adversely affects the accomplishment of an operational or mission-essential capability.

3. **Medium**

   Delays the accomplishment of an operational or mission-essential capability.

4. **Low**

   Results in user/operator inconvenience or annoyance, but does not prevent a required operational or mission-essential capability.

As shown in Table 1, priority is calculated based on the values entered for impact and urgency.

Note: Mission-essential infrastructure and applications are those that have a current or imminent impact on production. Training environments are not considered mission-essential and should be classified with a criticality of 4-Low. Development systems and environments may be considered mission-essential in certain situations.

Table 1 – Determination of Priority Based on Impact and Urgency

Impact	Urgency	Priority
1	1	Critical
1	2	Critical
1	3	High
1	4	Low
2	1	Critical
2	2	High
2	3	Medium
2	4	Low
3	1	High
3	2	High
3	3	Medium
3	4	Low
4	1	High
4	2	Medium
4	3	Medium
4	4	Low

APPENDIX 2 – OPERATIONAL CATEGORIZATION

Operational categories provide an additional level of detail for incidents and changes created in the ITSM database. Operational Category Tier 1 is required for all incidents. The table below list all of the operation categorization combinations.

Operational Category Tier 1	Operational Category Tier 2
Backup	Configuration
Backup	Database
Backup	File System
Backup	Virtual Machine
Change	Access
Change	Configuration
Change	Location
Change	Media
Change	Password
Copy/Duplicate	Account
Copy/Duplicate	Account Setup
Copy/Duplicate	Configuration
Copy/Duplicate	Database
Copy/Duplicate	Media
Copy/Duplicate	Virtual Machine
Non-Fatal Error	Screen display error
Notify/Alert	Capacity
Notify/Alert	Degradation
Notify/Alert	Failure
Notify/Alert	Outage
Notify/Alert	Physical Security Breach
Notify/Alert	Threshold Exceeded
Notify/Alert	Unauthorized System Access
Notify/Alert	Virus/Worm
Power Outage	Power Outage
Provision/Install	Equipment
Provision/Install	Hardware
Provision/Install	Service
Provision/Install	Software
Provision/Install	Storage
Provision/Install	Virtual System
Reinstall	Software
Remove	Access
Remove	Account
Remove	Account Admin
Remove	Bandwidth
Remove	Component

Operational Category Tier 1	Operational Category Tier 2
Remove	Connectivity
Remove	Database
Remove	Equipment
Remove	Inappropriate Material
Remove	Report
Remove	Server
Remove	Service
Remove	Software
Remove	Storage/Capacity
Remove	Virtual System
Remove	Virus/Worm
Repair/Failure	Connectivity
Repair/Failure	Equipment
Repair/Failure	Software
Replace	Component
Replace	Equipment
Replace	Hardware
Request	Access
Request	Account
Request	Account Admin
Request	Advice/How To
Request	Bandwidth
Request	Baseline
Request	Component
Request	Connectivity
Request	Consumables
Request	Database
Request	Documentation
Request	Enhancement
Request	Equipment
Request	Network
Request	Professional Services
Request	Project
Request	Report
Request	Security
Request	Service
Request	Software
Request	Storage/Capacity
Request	Training
Request	Virtual System
Reset	Password
Restart	Hardware
Restart	Host
Restart	Software

Operational Category Tier 1	Operational Category Tier 2
Restore	Access
Restore	Baseline
Restore	Configuration
Restore	Connectivity
Restore	Database
Restore	File System
Restore	Service
Restore	Storage/File System
Restore	Storage/File System
Restore	VM Snapshot
Server	Other
Terminate/Recover	Account
Terminate/Recover	Hardware
Unlock	Account
Windows OS	Browser Incompatibility
Workstation	Browser
Workstation	Other
Workstation	Software Distribution

APPENDIX 3 – RESOLUTION CODES
Cancelled
Database repaired
Hardware repaired/replaced/installed
Software repaired/replaced/installed
Network connection issue
No problem found
Other
Restart/reboot
Works as designed
Duplicate incident