Yale University Incident Management Process Guide

Learn more:

(888) 440-2730 x702
info@FruitionPartners.com
www.FruitionPartners.com

RESEARCH
EDUCATE
IMPLEMENT
bring IT to fruition.™

Introduction

Purpose

This document will serve as the official process of Incident Management for Yale University. This document will introduce a Process Framework and will document the workflow, roles, procedures, and policies needed to implement a high quality process and ensure that the processes are effective in supporting the business. This document is a living document and should be analyzed and assessed on a regular basis.

Scope

The scope of this document is to define the Incident Management Process, and process inputs from, and outputs to, other process areas. Other service management areas are detailed in separate documentation. The following is a specific list of items that are in scope for this document. Other items not listed here are considered out of scope for this document.

In scope:

- Incident Management Overview
  - Incident Definition
  - Incident Management Objectives
  - Incident Management Policies
- Incident Management Process Flow
- Incident Management Roles
- Incident Management RACI
- Incident Management Procedure Flows and Descriptions
- Incident Management Prioritization scheme
- Incident Management Service Categorization Model
- Incident Management Process Metrics

Incident Management Overview

Incident Definition

An Incident is an unplanned interruption to a technology service or reduction in quality of a technology service. Failure of a Configuration Item or product that has not yet impacted service is also an incident (i.e. failure of one disk from a mirror set).

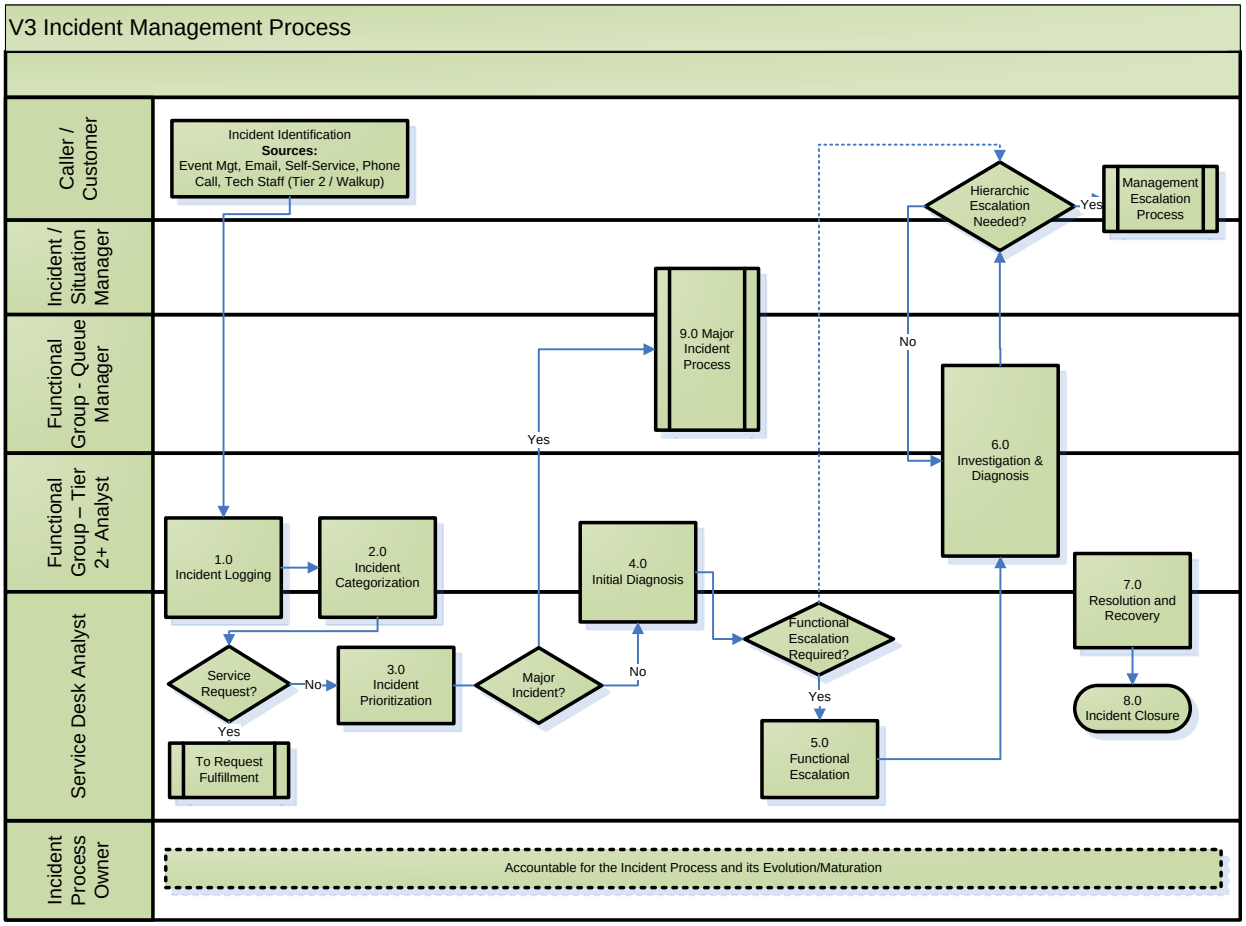
Incident Management Objectives

The goal of Incident Management is to restore service operations as quickly as possible. Timely and efficient resolution will minimize business impact and increase productivity.

Incident Management Policies

Incident reporting must go through the Service Desk, providing Users with a single point of contact
All incidents must be logged, prioritized and solutions recorded in the Incident Management System
One standard Incident Management Process is defined and used to support all IT Service users
The Service Desk manages, tracks, escalates, closes and communicates status of all incident records and is responsible for all incident assignments
The Incident Management Process is the conduit of communication of any degradation of service, to the affected users and IT personnel
Closure of incidents is dependent on validating with the user that the incident has been resolved and service is restored
The Service Desk will own all incidents that they themselves log or that are assigned to them from a Tier 2 provider. Ownership will transfer to the Incident / Situation Manager for major incidents
Once a major incident has been validated by the Service Desk, escalation and communication protocols for high-priority incidents are initiated and managed by the Service Desk

Incident Management Process Flow



Roles

The following roles have been identified within the Incident Management Process.

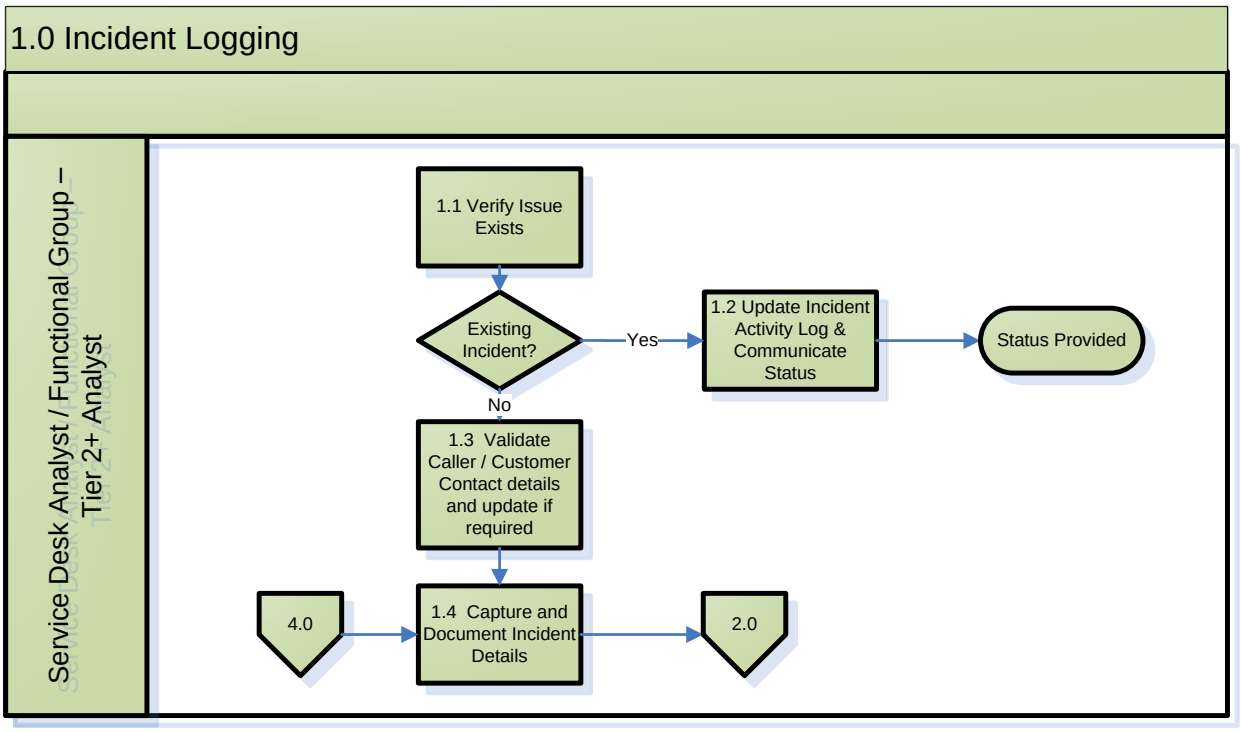
Role	Description
Incident Manager	• Oversee day to day process execution • Often the Service Desk Manager • Manages major incidents until the appropriate situation manager is identified
Situation Manager	• Manages and owns major incidents
Service Desk Manager	• Manages the service desk function, including staffing management activities • Provides guidance to Service Desk Analysts
Incident Process Owner	• Owns the process end-to-end, including the RACI, process & procedural steps, role & definitions • Accountable for maturing and evolving the process, based on monthly/quarterly/yearly review of process KPIs • Adjusts the process to address performance or changing business needs
Service Desk Site Lead	• Responsible for the operations of Service Desk Analysts that are geographically disperse, reporting to the Service Desk Manager
Service Desk Analyst	• Logs incidents • Provides initial diagnosis • Resolve incidents at first point of contact if possible • Escalates incidents

Role	Description
	• Owns non-major incidents
Caller / Customer	• The end user having or reporting the service interruption
Functional Group – Queue Manager	• Assigns incidents to individual Tier 2+ Analysts in the functional group • Monitors and manages support resolution performance • May directly manage (reporting manager) the day to day activities of Tier 2+ analysts outside of process activities
Functional Group – Tier 2+ Analyst	• Group of technical support experts that will handle issues escalated by the Service Desk • For example, a Network Engineer • Receive process direction for a functional group queue manager, staff management from a reporting manager

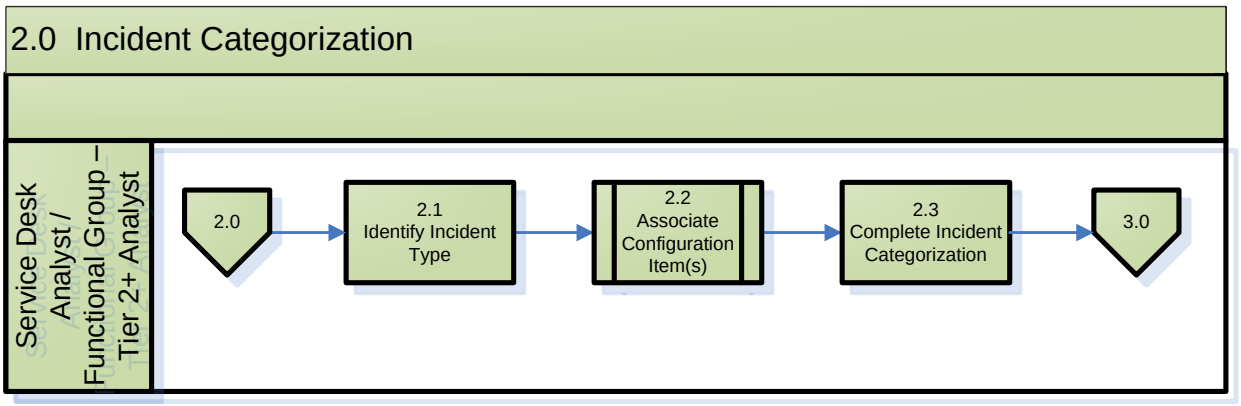
RACI

	Caller / Customer	Service Desk Analyst	Service Desk Site Lead	Incident Manager	Situation Manager	Functional Group – Queue Manager	Functional Group – Tier 2+ Analyst	Incident Process Owner
1.0 Incident Logging	C	R		A			R	
2.0 Incident Categorization	C	R		A			R	
3.0 Incident Prioritization	C	R		A, C, I				
4.0 Initial Diagnosis		R		A, C, I			R	
5.0 Functional Escalation		R		A, C				
6.0 Investigation & Diagnosis						A	R	
7.0 Resolution & Recovery	I	R		A			R	
8.0 Incident Closure	C	R	R	A			R	
9.0 Major Incident Process				A	R	R		
Process Maturity and Evolution	C, I	C	R	R	C	R	C	A

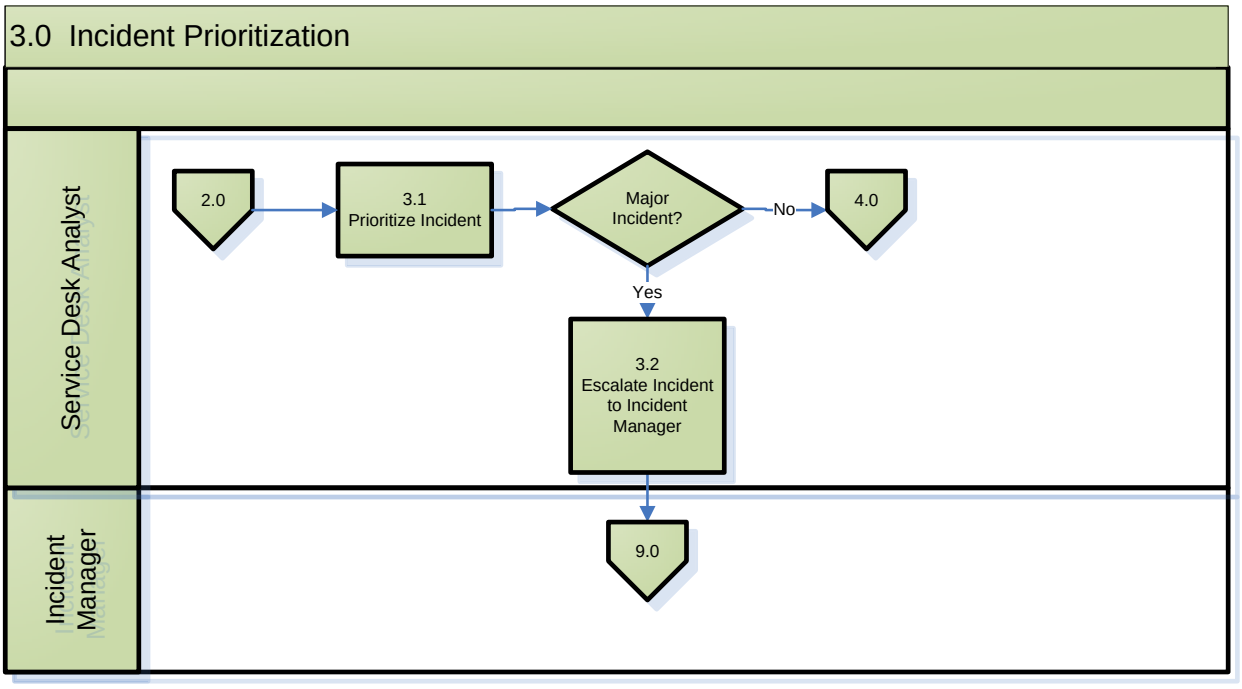
Process Procedures



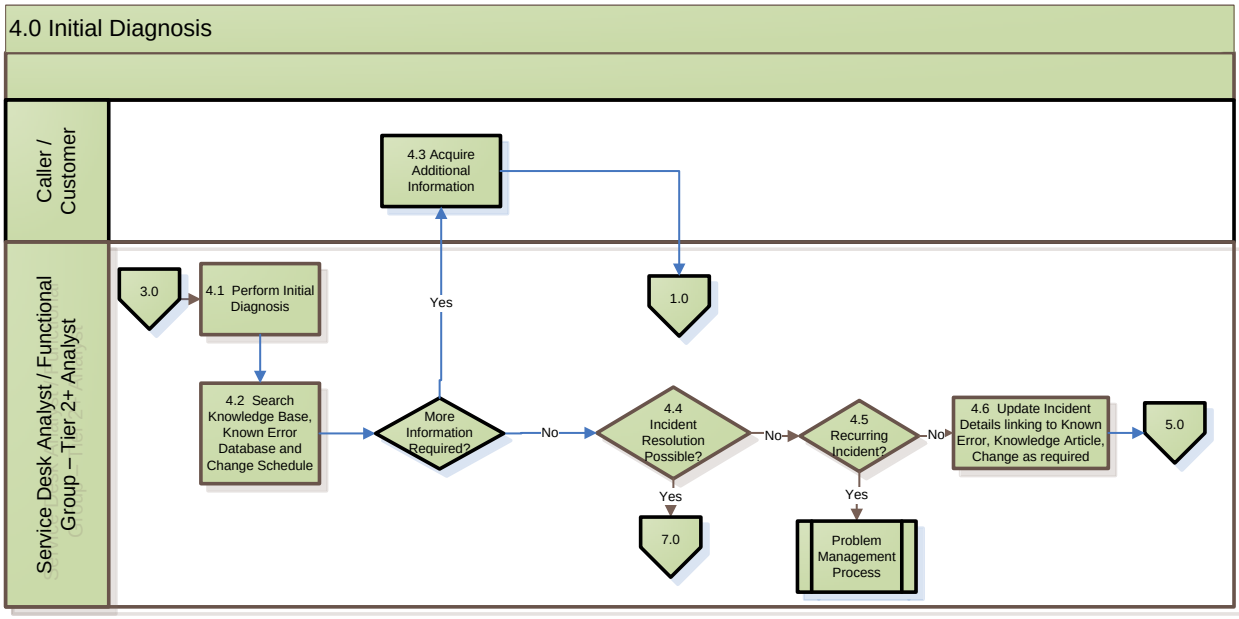
Step	Activities
1.1 Verify Issue Exists	Take steps to validate or replicate the interruption. Gather any data about the issue (screenshots, descriptions). Associate to any concurrent incident (e.g. major outage).
1.2 Update Incident Activity Log & Communicate Status	If the Caller is inquiring about status of an existing incident, provide the caller with status as available in the incident record and update the record indicating that the caller was inquiring and update with additional details if available.
1.3 Validate Caller / Customer Contact details and Update if Required	Complete caller data and ensure contact details are accurate and update if necessary.
1.4 Capture and Document Incident Details	Complete the short and long description, ensuring they are clear and can be understood by others. Collect incident symptoms.



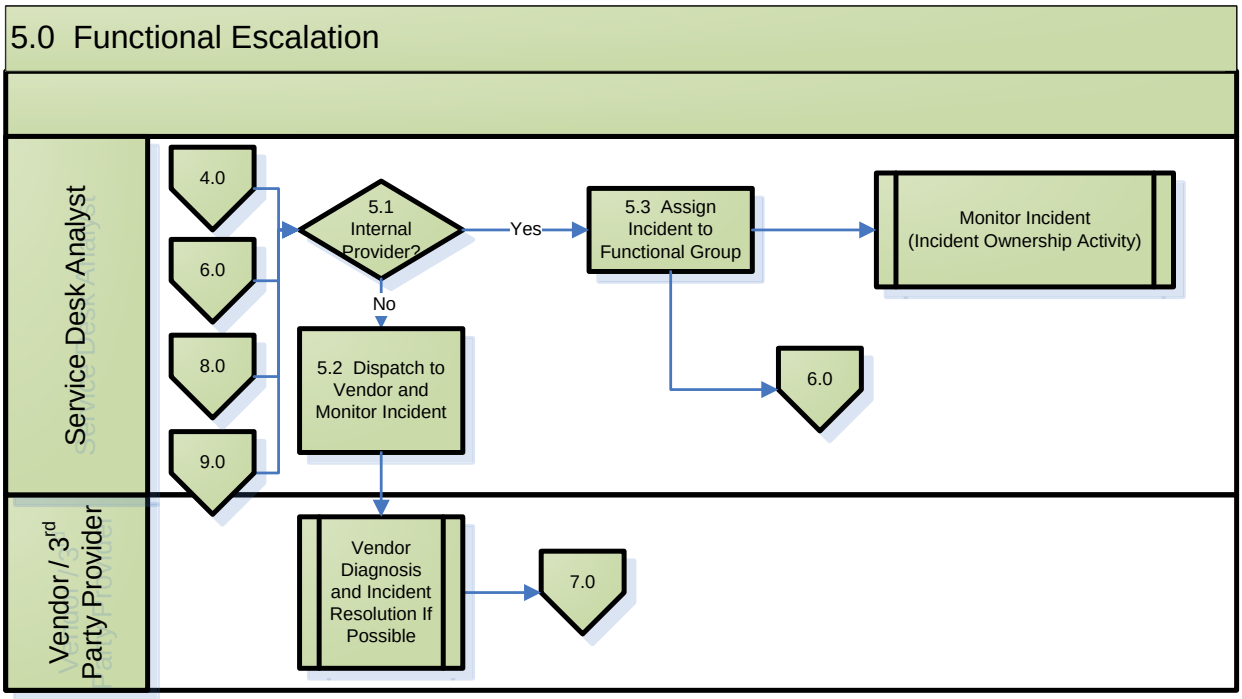
Step	Activities	
2.1 Identify Incident Type	Capture the incident type based on the customer-reported symptoms.	
2.2 Associate Configuration Items(s)	If a Configuration Management System (CMS) is present, associate the incident to the Configuration Item(s) (CI) diagnosed to have failed and are causing the incident. Note, IT Business and Provider Services may be captured as CI's, if implemented.	If there is no CMS present, capture the device name or ID, and based on the primary failed device, capture the component categorization.
2.3 Complete Incident Categorization	Capture IT Business Service categorization, as defined by the customer. Based on the symptoms and incident diagnosis, capture the IT Provider Service categorization.	



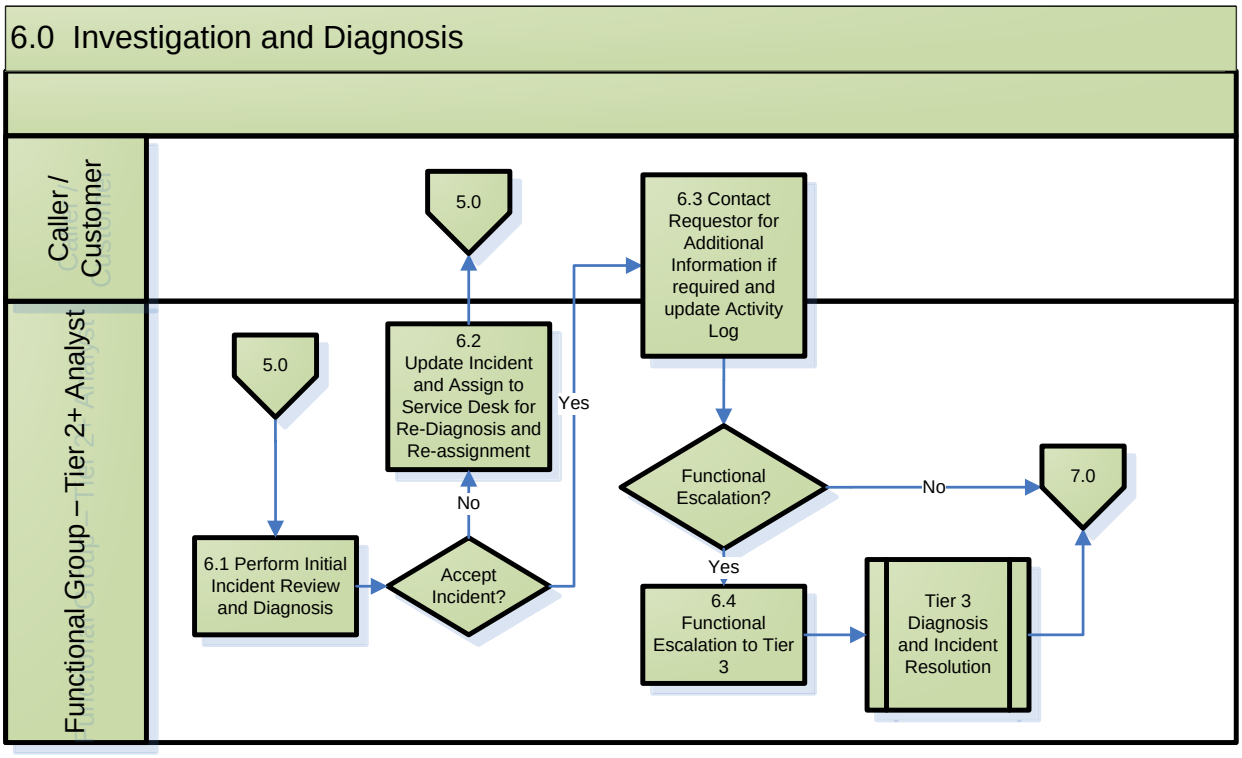
Step	Activities
3.1 Prioritize Incident	Select the impact and urgency of the Incident according to guidelines if it is not present. This will determine the priority. If priority-based service level monitoring is enabled, the selected priority to define the response and resolution time service level targets for the incident. If service-based monitoring is enabled, the selected priority will only define the response time service level targets for the incident. If the reported service does not have any restoration service level targets defined, a generic priority-based restoration service level target may be used.
3.2 Escalate Incident to Incident Manager / Situation Manager	Determine if this is a major incident. If so, the service desk agent will escalate to the incident manager accordingly.



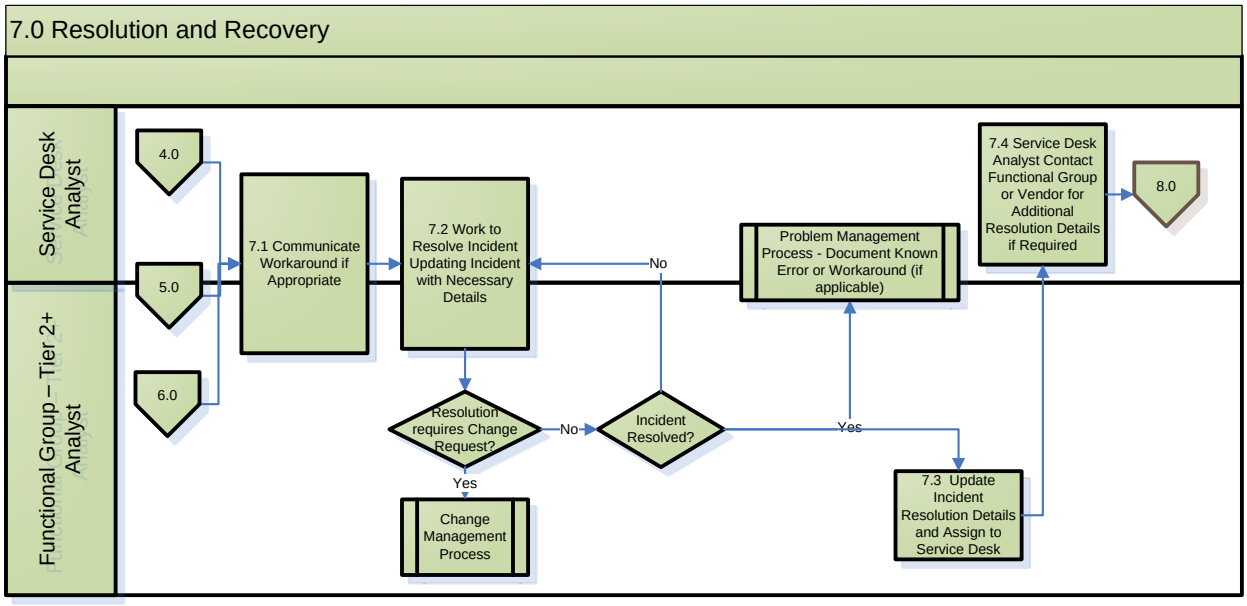
Step	Activities
4.1 Perform Initial Diagnosis	Document all trouble-shooting steps within the incident record.
4.2 Search Knowledge Base, Known Error, Database and Change Schedule	Use initial diagnosis details to search the knowledge base for relevant knowledge. Also check the known error database to see if a workaround exists and the change schedule to see if this is issue could be related to a recently implemented change. Ensure the incident record is coded appropriately.
4.3 Acquire Additional Information	If additional information is required, contact the customer. If the customer cannot be reached, place the incident on hold.
4.4 Incident Resolution Possible?	If a resolution is possible, proceed to step 7.0 Resolution and Recovery. If resolution is not possible, the incident may need to be assigned to a functional group for resolution.
4.5 Recurring Incident?	Determine if other incidents of the same nature have been experienced. If others exist and no root cause has been determined, this may be a good candidate for problem management.
4.6 Update Incident Details linking to Known Error, Knowledge Article, Change as required	Confirm that the incident record is updated and coded according to the diagnosis steps. Selection of a knowledge record may update (e.g. provider service, component category, urgency) incident categorization and details.



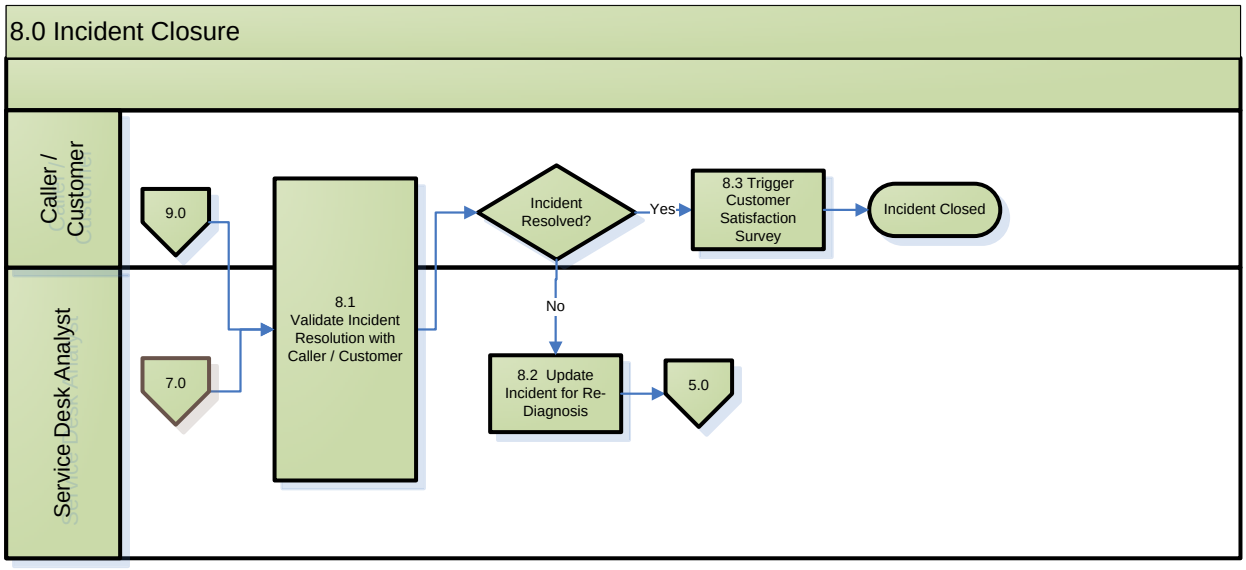
Step	Activities
5.1 Internal Provider?	If assignment is necessary, determine if the functional group that is equipped to resolve the incident is an internal support group or an established external partner that has a support agreement and process established for incident resolution.
5.2 Dispatch to Vendor and Monitor Incident	If the functional group is an external group, ensure that the established incident process is followed.
5.3 Assign Incident to Functional Group	If the functional group is an internal group, determine the proper group for assignment and assign it to the Group.
5.4 Monitor Incident	Optimally, the Service Desk owns the monitoring of incident to resolution and closure. Guidelines for ownership/monitoring include: - Providing customers with desk contact info for updates - Progress notifications originate from a desk monitored email account - Incidents that have not been accepted within response time targets should be initially escalated to the assignment group manager, and ultimately to the Incident Manager if required - Ownership of major incidents should be transferred to the incident manager/ situation manager



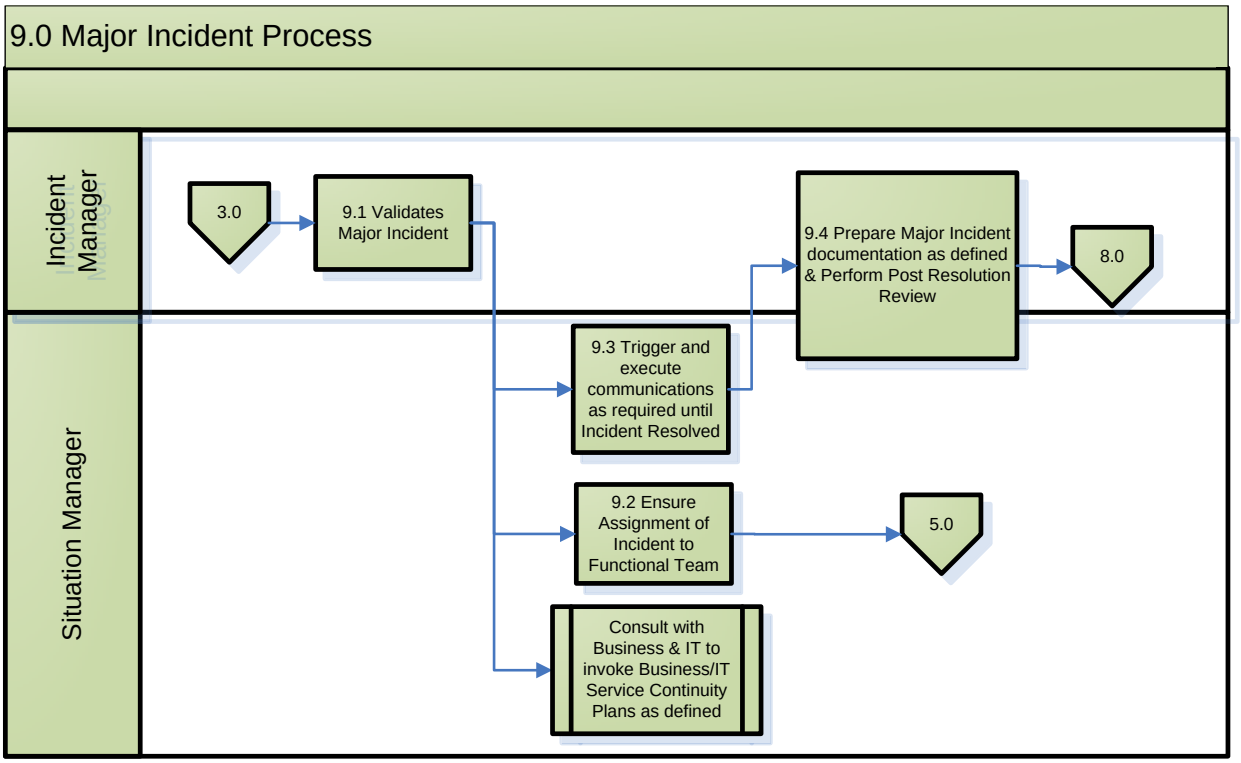
Step	Activities
6.1 Perform Initial Review & Diagnosis	Perform initial review to determine if the incident has been properly assigned.
6.2 Update Incident and Assign to Service Desk for Re-diagnosis and Re-assignment	If the incident was improperly assigned, the Functional Group assigns it back to the Service Desk for further diagnosis and assignment.
6.3 Contact Requestor for Additional Information if Required	If assignment is proper, accept the incident (work in progress) and determine if further information is required contact the customer to obtain then proceed to step 7.0 Resolution and Recovery.
6.4 Functional Escalation to Tier 3 if required	If the incident requires further assignment to Tier 3 or an external Vendor, the Functional Group is responsible to work with the external partners and maintain oversight of the incident record.



Step	Activities
7.1 Communicate Workaround if Appropriate	Investigate sources of information to see if a workaround exists. Check relevant knowledge, known error database, problem records, etc. and provide the work around to the customer.
7.2 Work to Resolve Incident Updating Incident with Necessary Details	If no workaround exists, begin resolution activities making sure to update the incident record with all details related to resolution activities. If resolution requires that a change be introduced, a Request for Change must be submitted and flow through the Change Management Process.
7.3 Update Incident Resolution Details and Assign to Service Desk	Once the incident has been resolved it is good practice to review the solution and determine if knowledge could be authored for future occurrences, or if there is a systemic issue that needs to be addressed through the Problem Management Process. Upon resolution, the incident is updated with the proper resolution information and coding, and is assigned to the Service Desk for final closure activities.
7.4 Service Desk Analyst Contact Functional Group or Vendor for Additional Resolution Details if Required	In preparation for closure activities, review the incident details to ensure it is completed properly and has the appropriate resolution details.



Step	Activities
8.1 Validate Resolution with Caller / Customer	Follow proper procedures to validate with the Customer that the incident has in fact been resolved. If it has been resolved, the incident will be closed according to procedures.
8.2 Update Incident for Re-Diagnosis	If the Customer indicates that the incident has not yet been resolved, it must be sent back for further diagnosis before the incident is closed. NOTE: If the incident is in a closed state when the customer indicates it was not resolved, a new incident should be opened and associated to the original incident.
8.3 Trigger Customer Satisfaction Survey	Once the customer has confirmed resolution and the incident is in process of being officially closed, a customer satisfaction survey is to be provided to inform future improvement opportunities.



Step	Activities
9.1 Validate Major Incident	If an incident is escalated to a "Major Incident" status, the Incident Manager must first ensure that it should be treated as a Major Incident and be given the enhanced communication and management attention that a Major Incident requires.
9.2 Ensure Assignment of Incident to Functional Team	Ensure that the incident has been assigned to the appropriate team for resolution and works with the management structure to coordinate a cross-functional team to address the situation if needed and where the underlying issue is unclear.
9.3 Trigger and execute communications as required until Incident Resolved	Ensure that the communication is planned and executed according to internal procedures and triggers. At a minimum communication is to be shared at the beginning and end of a Major Incident and perhaps at specific intervals throughout the resolution process. This communication can be to either internal IT stakeholders or Customers or a combination of both.
9.4 Prepare Major Incident documentation as defined & Perform Post Resolution Review	Upon resolution of a Major Incident, documentation must be prepared that summarizes the issue, actions taken and resolution details. It should also trigger root case analysis if required and allow for improvements that can be made to avoid the situation in the future.

Prioritization scheme

The prioritization scheme is based on a combination of Impact and Urgency and used to:

- Generate a simplified value in order to drive escalation and notification
- Establish appropriate 'order and extent of work effort to achieve resolution

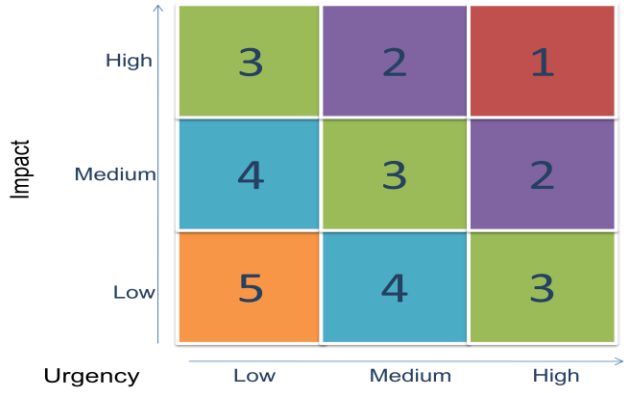
Impact:

- Measure of scope and criticality to business
- Often equal to the extent to which an incident leads to distortion of agreed or expected service levels
- Impact is often measured by the number of people affected, critical systems, or financial loss as a result of the service interruption

Urgency:

- Measure of how quickly an incident needs to be responded to based on the business needs of the customer
- Prioritizes workload; incidents with higher urgency will be addressed before others, unless SLA breaches are imminent

The follow table shows the resulting priority based on impact and urgency.

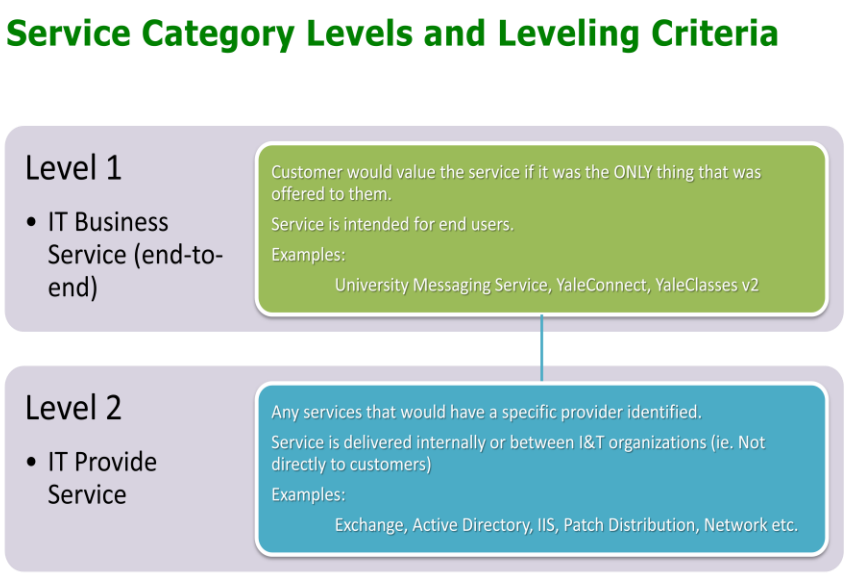


Service Categorization Model

A Service Categorization model is an important aspect that:

- Recognizes need to capture service vs. technology details
- Future-proofed for introduction of Service Asset and Configuration Management
- Enhances value of reporting by defining IT service view in terms the business should understand

The following shows the 2 Service Categorization levels that enable views from both Customer/Business and Provider perspectives:



Process Metrics

The following table describes the Incident Management KPIs identified.

Yale **KPI #**	**KPI Name**	**OM DESCRIPTION**
2.1	% Incidents logged	How many tickets are incidents? Incidents are tickets excluding service requests and complaints
DERIVED	Incidents by Source (e.g. Call, Email etc.)	How many incidents are logged via calls
11	First incident resolution	How many incidents were resolved correctly in first attempt?
12	Incidents resolved at Help Desk	How many incidents were resolved at the help desk?
13	Incidents that bypassed help desk support	How many incidents were not reported to help desk
17	Reassignment Count	How many incidents are reassigned to another work-group?
14	% Incidents assigned incorrectly	How many incidents are assigned to the wrong work-group?
	% Incidents escalated Inaccurately	How many incidents are assigned from Tier 2 to Tier 2, vs. being reassigned to Tier 1
15	% Incidents escalated	Incidents that are escalated to another group
17	Average time for second level support to respond	Time elapsed between a call being assigned to second level support and the call being accepted

Yale **KPI #**	**KPI Name**	**OM DESCRIPTION**
18	Incidents reopened	How many incidents were reopened?
19	Ageing incidents	How many incidents are unresolved past threshold
20	Incidents responded on time (Tier 2)	How many incidents were responded on time by Tier 2
NEW	Incidents responded on time (customer-perspective)	How many incidents were responded to on time from logging to last in-progress
21	Incidents resolved on time	How many incidents were resolved on time
DERIVED	Incidents by Priority	
24.1	Cost per Incident	Ratio of operational budget to users of IT services

Document History

Version	Date	Changes	Author
01	12/31/2011	Initial Document	Angie Massicotte / Michael Oas
02	01/02/2012	Minor Updates	Michael Oas