University of California
San Francisco

Information Technology and Service

UCSF ENTERPRISE INCIDENT MANAGEMENT PROCESS

VERSION 1.3, REV. October 15, 2011

Document Version Control

Document Name		Enterprise Incident Management Process	
Process Owner		Darlena Torres	
Version Number	**Issue Date**	**Prepared By**	**Reason for Change**
1.0	6/15/11	Terrie Coleman	First draft
1.1	7/5/11	Terrie Coleman	Updated Process Owner. Aligned process and roles with ITIL V3. Updated procedures 27 & 33 with closure code direction. Updated RACI. Removed Impact, Urgency, Priority and Global Incident t Management Service Levels sections
1.2	9/27/11	Terrie Coleman	Merged Logging and Categorization and Incident Monitoring & Escalation Sub Process documents into Enterprise Incident Management Process document
1.3	10/15/12	Terrie Coleman	Corrected typo in Prioritization Matrix

Reviewers

Name	Role
Darlena Torres	Customer Service Manager, Medical Center
John Chin	Service Desk Supervisor, Medical Center
Quinn Hearne	Desktop Support Manager, School of Medicine
Tim Greer	IT Manager, SFGH
John Gingrich	IT Supervisor, SFGH
Dan Pucillo	Service Desk Supervisor, Campus
Peter Kearney	Project Manager, Operational Excellence
Peter Stampfer	Service Now Administrator, Medical Center

Approvers

Name	Role	Date
Joe Bengfort	CIO, Medical Center	7/15/11
Darlena Torres, on behalf of Julie Cox	Customer Service Director, Medical Center	7/15/11
Rebecca Nguyen	IT Service Management Product Manager	7/15/11
Jodi Muller	IT Service Management Project Manager	7/15/11

Table of Contents

1. INTRODUCTION ENTERPRISE INCIDENT MANAGEMENT

1.1. PURPOSE

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. Normal service operation is defined as service operation within service level agreement (SLA) limits.

1.2. SCOPE

The scope of the Incident Management process includes a standard set of processes, procedures, responsibilities and metrics that are utilized across the enterprise.

1.3. DEFINITIONS

An ***incident*** is any event which is not part of the standard operation of a service and which causes, or may cause an interruption to, or a reduction in the quality of that service.

The Incident Management process includes Incident Acceptance and Recording, Classification and Initial Support, Matching, Investigation and Diagnosis, Resolution and Recovery, Closure, and Progress Monitoring and Reporting

2. ROLES AND RESPONSIBILITIES

2.1. CUSTOMER

- Identifies incident
- Confirms incident has been resolved

2.2. SERVICE DESK – 1ST LEVEL SUPPORT

- First point of contact for customers reporting service disruption of service
- Responsible for recording and classifying incidents and undertaking an immediate effort in order to restore a failed IT service as quickly as possible
- Transfer incidents to expert technical support when no ad-hoc solution can be achieved
- Provide customer updates as required

2.3. 2ND LEVEL SUPPORT

- Takes over incident which cannot be solved immediately by Level 1 Support
- Responsible for incident investigation, diagnosis and recovery within defined priorities
- Request external support if necessary
- Aim to restore an IT service as quickly as possible
- Transfer incidents to Level 3 support when no solution can be found
- Provide customer updates as required

2.4. 3RD LEVEL SUPPORT

- Typically located at hardware or software manufacturers.
- Services are requested by 2nd Level Support if required for solving an Incident.Responsible for incident investigation, diagnosis and recovery within defined priorities
- Aim to restore an IT service as quickly as possible

2.5. MAJOR INCIDENT TEAM

- A dynamically established team formulated to concentrate on the resolution of a major incident

- Initiates the Event Communication Process
- Initiates the Problem Management Process
- Conducts SWAT session after event

2.6. INCIDENT MANAGER – PROCESS OWNER

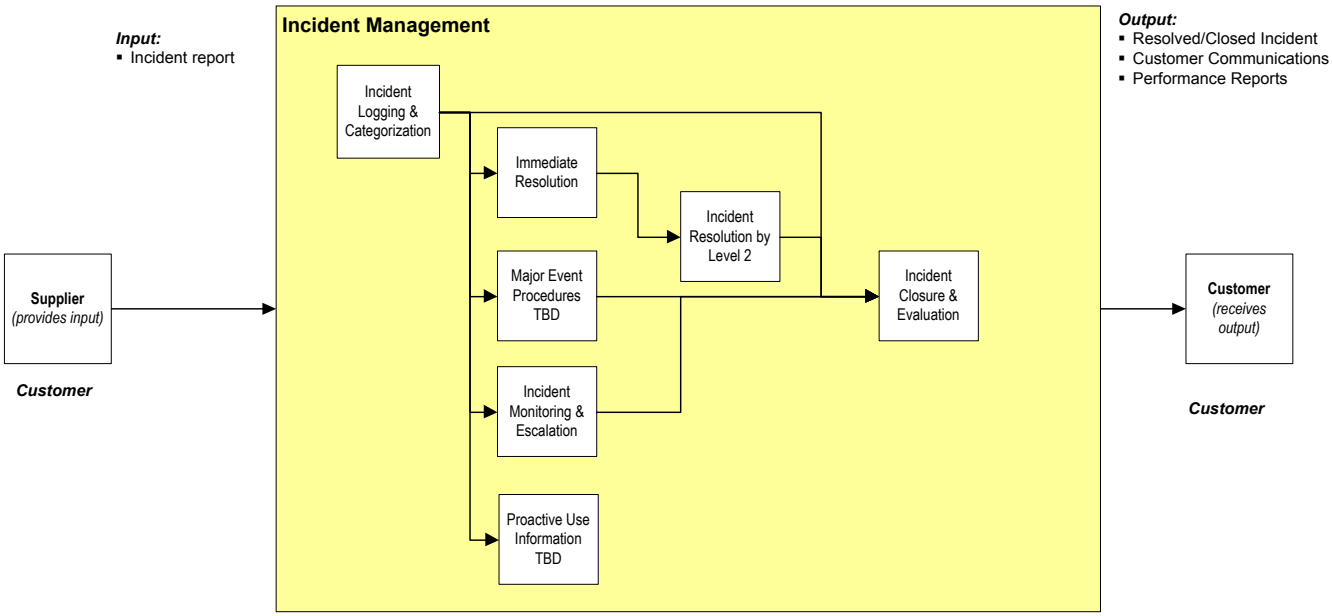
- Manages the effective implementation of the Incident Management Process
- Makes recommendations for process improvement
- Generates Incident Management performance reports
- Represents the first stage of escalation for incidents which are not resolved within the agreed Service Levels

3. PROCESS DEFINITION

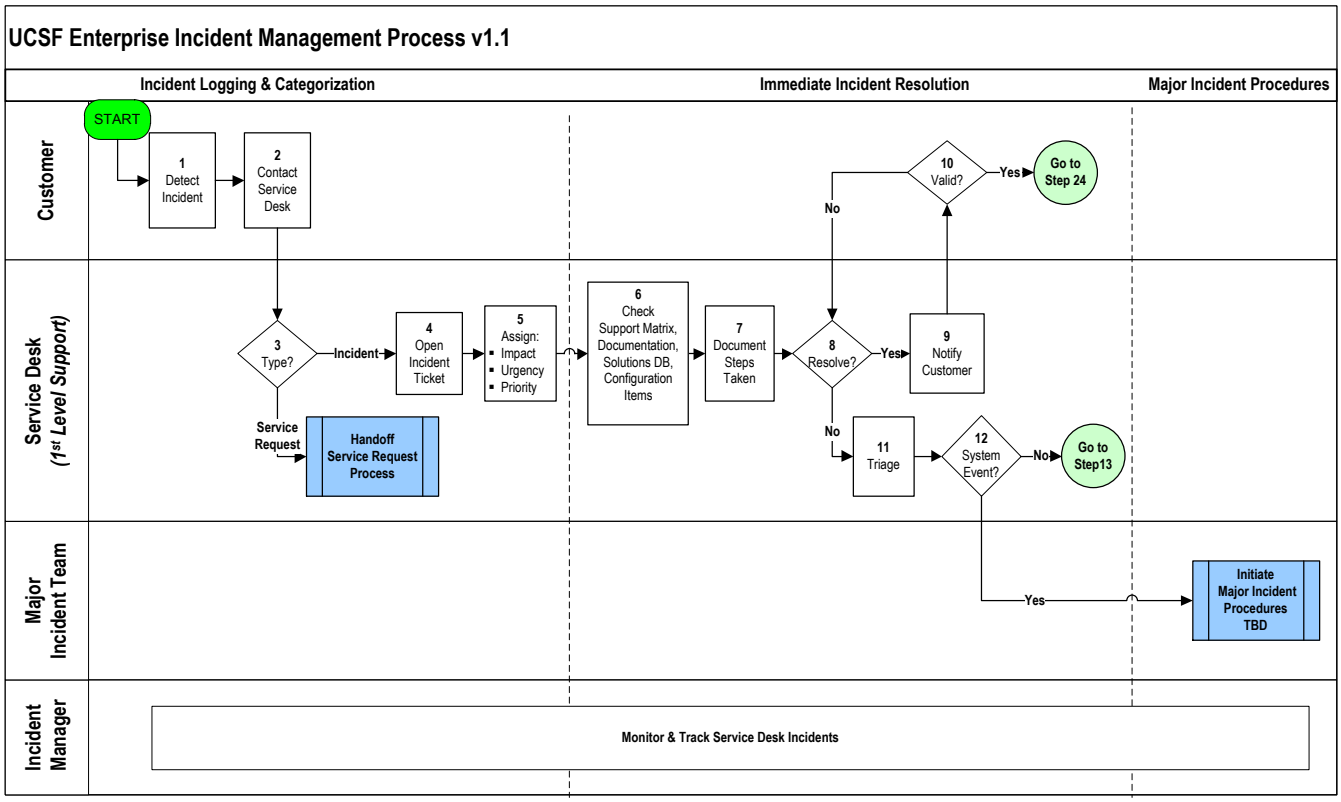
3.1. ENTERPRISE INCIDENT MANAGEMENT HIGH LEVEL PROCESS MAP

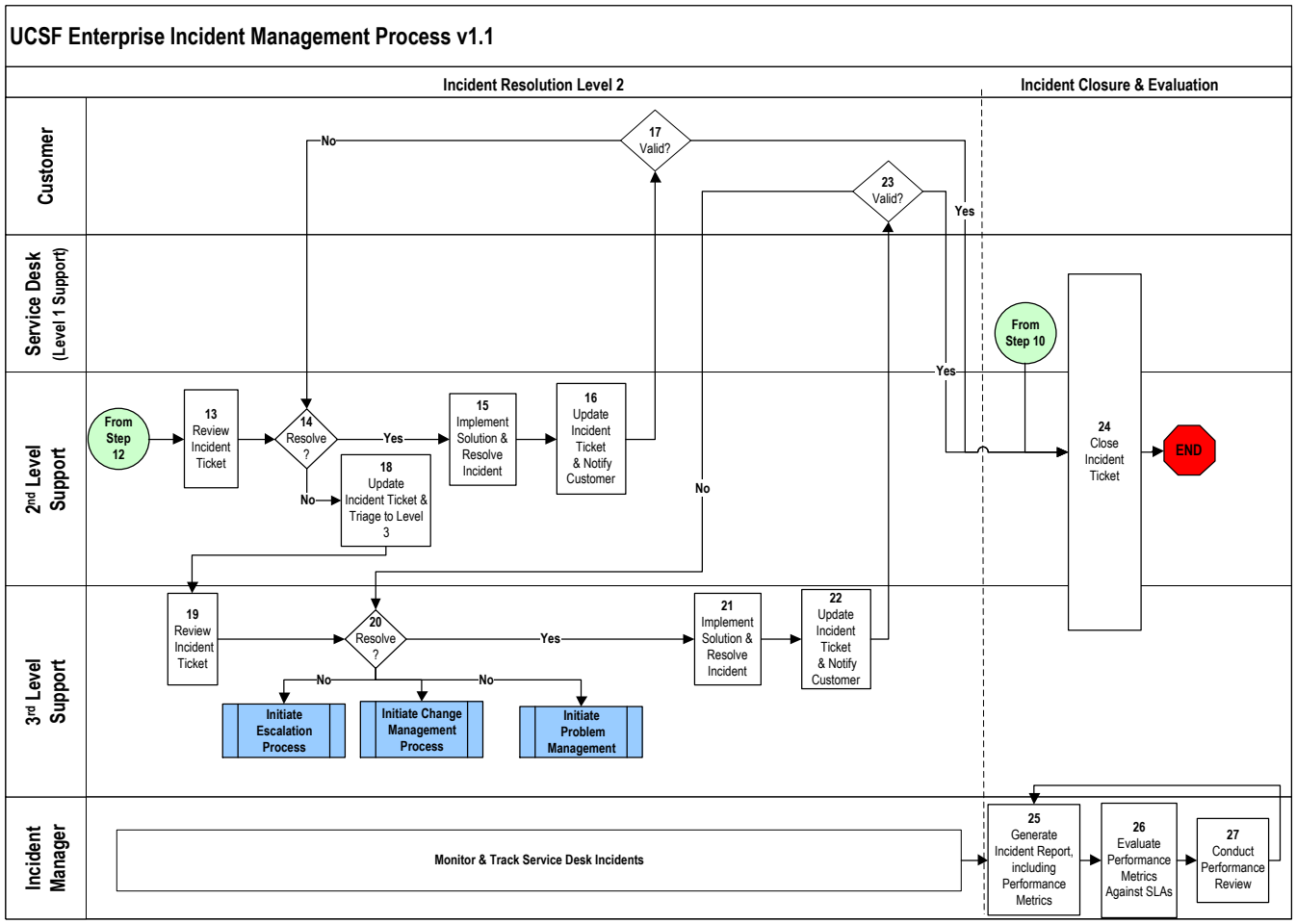
The Incident Management process is used to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, ensuring that the best possible levels of service quality and availability are maintained.

Trigger: Disruption of service



3.2. ENTERPRISE INCIDENT MANAGEMENT ACTIVITY DIAGRAM




UCSF Enterprise Incident Management Process v1.1
Incident Resolution Level 2
Incident Closure & Evaluation
Customer
Service Desk (Level 1 Support)
2nd Level Support
3rd Level Support
Incident Manager
17 Valid?
No
23 Valid?
Yes
Yes
From Step 10
From Step 12
13 Review Incident Ticket
14 Resolve ?
Yes
No
15 Implement Solution & Resolve Incident
16 Update Incident Ticket & Notify Customer
18 Update Incident Ticket & Triage to Level 3
No
24 Close Incident Ticket
END
19 Review Incident Ticket
20 Resolve ?
Yes
No
No
21 Implement Solution & Resolve Incident
22 Update Incident Ticket & Notify Customer
Initiate Escalation Process
Initiate Change Management Process
Initiate Problem Management
Monitor & Track Service Desk Incidents
25 Generate Incident Report, including Performance Metrics
26 Evaluate Performance Metrics Against SLAs
27 Conduct Performance Review

4. RACI CHART

Step #	Enterprise Incident Management Process	Customer	Service Desk	Incident Manager	Major Event Team	2nd Level Support	3rd Level Support	Output
Incident Logging and Categorization								
1	Detect Incident	R,A						
2	Contact Service Desk	R,A						
3	Type?		R,A					
4	Open Incident Ticket		R,A					
5	Assign: Impact, Urgency, Priority		R,A					
	Handoff to Service Rquest process		R,A					
Immediate Incident Resloultion by Level 1								
6	Check Support Matrix, Documentation,		R,A					
7	Document Steps Taken		R,A					
8	Resolve?		R,A					
9	Notify Customer	I	R,A					
10	Valid?	R,A	I					
11	Triage		R,A					
12	System Event?		R,A					
	Initiate Major Incident Procedures				R,A			
	Monitor & Track Incidents			RA				
Immediate Resolution by Level 2								
13	Review Incident Ticket					R,A		
14	Resolve?					R,A		
15	Implement Soluiton and Resolve Incident					R,A		
16	Update Incident Ticket & Notify Customer	I				R,A		
17	Valid?	R,A				I		
18	Update Incident Ticket & Triage to Level 3					R,A		
19	Review Incident Ticket						R,A	
20	Resolve?						R,A	
	Handoff to Change Management Process							
	Initiate Escalation Process							
	Initiate Problem Management Process							
21	Implement Soluiton and Resolve Incident						R,A	
22	Update Incident Ticket & Notify Customer	I					R,A	
23	Valid?	R,A						
Incident Closure and Evaluation								
24	Close Incident Ticket		R,A			R	R	
25	Generate Incident Report including			R,A				
26	Evaluate Performance Metrics Against SLAs			R,A				
27	Conduct Performance Review			R,A				

Responsible – People who do the work, facilitate it and/or organize it
Accountable – The one who insures that desired outcomes are reached and has yes/no decision making authority
Consulted – People who have critical expertise to contribute before a decision is made
Informed – People who are significantly affected by the activity/decision and must be informed to insure successful implementation

5. ENTRY CRITERIA

- Incident report

6. PROCEDURE

ID	Step	Responsibility
Incident Logging and Categorization Sub-Process		

ID	Step	Responsibility
1	**Detect Incident** Identify a disruption of service.	▪ Customer
2	**Contact Service Desk** Customer contacts the Service Desk to report a disruption in service or request service.	▪ Customer
3	**Type?** Incident – go to step 4 / Service Request – Hand off to Service Request Process	▪ Service Desk
4	**Open Incident Ticket (classified at User Service Request)** Upon receiving a call (or request) from a Customer, the Service Desk Analyst enters the Customer and incident information into the ticket.	▪ Service Desk
	Hand-off to Service Request Process	
	Monitor and Track Incidents The Incident Manager is responsible for monitoring and tracking incident throughout the process.	▪ Incident Manager
5	**Assign: Impact, Urgency, Priority** Using the impact, urgency, priority matrix, determine and set the priority for the incident. Setting the priority begins the "clock" for the Service Level Agreement (SLA) associated with that priority. At this point, Service Desk Analyst becomes the Ticket Owner.	▪ Service Desk
Immediate Incident Resolution by Level 1 Sub-Process		
6	**Check Support Matrix, Documentation, Solutions Database and Configuration items** Review all available information for known errors and solutions to similar incidents.	▪ Service Desk
7	**Document Steps Taken** Update the worklog in the Incident Ticket with all of the troubleshooting steps taken to resolve the incident so far.	▪ Service Desk
8	**Resolve?** Yes – go to step9 / No – go to step 11	▪ Service Desk
9	**Notify Customer**	▪ Service Desk
10	**Valid?** Yes – go to step 24 / No – go to step 8	▪ Customer
11	**Triage** The Service Desk Analyst assigns the Incident ticket to Level 2 Support. At this stage the responsibility for resolving the incident and communicating with the Customer passes to the assigned Support Analyst however, the responsibility for final customer contact and closure of the incident remains with the Service Desk Analyst.	▪ Service Desk
12	**System Event?** Yes – go to step Initiate Major Incident Management Procedures / No – go to step 13	▪ Service Desk
	Initiate Major Incident Management Sub-Process	
	Monitor and Track Event The Event Manger is responsible for initiating the Communication Management Process and the Problem Management process as need. They are also responsible for tracking the event to resolution.	▪ Incident Manager
Immediate Resolution by Level 2 Sub-Process		

ID	Step	Responsibility
13	**Review Incident Ticket** Review the incident in order to understand the issue. Consult the Problem Management Database for known errors. If necessary, contact the Customer, IT Support Unit or the Service Desk to gain further clarity of the incident. Begin diagnosis of the incident.	▪ Level 2 Support
14	**Resolve?** Yes – go to step 15/ No – go to step 18 Determine if the incident can be resolved without making any system update and inform the customer of the solution. When the Level 2 Support Analysis is unable to resolve the incident it is escalated to Level 3 Support.	▪ Level 2 Support
15	**Implement Solution and Resolve Incident** Resolve the incident by implementing the necessary solution.	▪ Level 2 Support
16	**Update Incident Ticket and Notify Customer** Document the resolution in the Incident Ticket and enter the closure code. Contact the Customer with the solution to the incident	▪ Level 2 Support
17	**Valid?** Yes – go to step 24 / No - go to step 14	▪ Customer ▪ IT Support Group
18	**Update Incident Ticket and Triage to Level 3** Document the steps taken to diagnose/resolve the incident in the worklog of the Incident Ticket. When the Level 2 Support Analyst is unable to resolve the incident it is triaged to Level 3 Support. At this stage the responsibility for resolving the incident and communicating with the Customer passes to the assigned Support Analyst.	▪ Level 2 Support
19	**Review Incident Ticket** Review the incident in order to understand the issue. Consult the Problem Management Database for known errors. If necessary, contact the Customer, IT Support Unit or the Service Desk to gain further clarity of the incident. Begin diagnosis of the incident.	▪ Level 3 Support
20	**Resolve?** Yes – go to step 32 / No – hand-off to Escalation Process and/or Change Management Process and/or Problem Management The Level 3 Support Analyst determines if the incident can be resolved without making any system updates and informs the customer of the solution. If system updates are required the Level 3 Support Analyst will initiate the Change Management process	▪ Level 3 Support
	Initiate Monitoring and Escalation Sub-Process	
	Initiate Change Management Process	
	Initiate Problem Management Process	
21	**Implement Solution and Resolve Incident** The Level 3 Support Analyst resolves the incident by implementing the necessary solution.	▪ Level 3 Support
22	**Update Incident Ticket and Notify Customer** Document the resolution in the Incident Ticket and enter the closure code. Contact the Customer with the solution to the incident.	▪ Level 3 Support
23	**Valid?** Yes – go to step 24 / No go to step 20	▪ Customer ▪ IT Support Group
Incident Closure & Evaluation Sub-Process		

ID	Step	Responsibility
24	**Close Incident Ticket** The Ticket Assignee is responsible for closure of the Incident Ticket.	▪ Service Desk ▪ Level 2 Support ▪ Level 3 Support
25	**Generate Incident Report, including Performance Metrics**	▪ Incident Manager
26	**Evaluate Performance Metrics Against SLA**	▪ Incident Manager
27	**Conduct Performance Review**	▪ Incident Manager

7. EXIT CRITERIA

- Incident has been resolved to customer's satisfaction or has been handed off to another process.

8. INCIDENT LOGGING AND CATEGORIZATION SUB-PROCESS

8.1. SUB-PROCESS OBJECTIVE

Incident Logging and Categorization is a sub-process of the Incident Management Process. Its objective is to record and prioritize the Incident with appropriate diligence, in order to facilitate a swift and effective resolution.

8.2. LOGGING INCIDENTS

Incident Logging and Categorization is a sub-process of the Incident Management Process. Its objective is to record and prioritize the Incident with appropriate diligence, in order to facilitate a swift and effective resolution.

An Incident Record must contain the following information:

1. Unique ID of the Incident (usually allocated automatically by the system)
2. Date and time of recording
3. Service Desk agent responsible for the registration
4. Caller / user data
5. Description of symptom

8.3. CATEGORIZING INCIDENTS

The primary goal of Incident categorization is to provide a method for quickly routing and resolving an incident. The secondary goal is to provide trending reports.

The following fields are used to categorize an Incident:

1. Configuration Item (CI)

The Configuration Items (CI) field records what Service or Product is affected. The CI forms the basis of all categorization. A CI can be a physical CI (e.g., Workstation,

Software application, etc.) or an IT Service CI (e.g., Telecom Service, Email Service, Internet, etc.)

2. Short Description

The Short Description field records a brief summary of the symptom or request specific to the CI selected for the Incident. The Short Description field is populated by selecting a description from the drop down menu. Selections in the drop down menu are unique to the selected CI.

3. Type

The Type field records the kind of Incident that is being logged. There are two types of Service Desk interactions: Service Interruption and Service Request. The Type field is auto-populated based on the Short Description that was selected.

4. Category and Sub-category

The Category and Sub-category fields record what is being reported or requested by the end user (e.g., Troubleshoot / Error Message; Troubleshoot / Connectivity; Request / Password Reset; Investigate / Security Incident; Inquire/Request / How-to, etc.) The Category and Sub-category fields are auto-populated based on the selected Short Description. Since Short Descriptions are specific to the CI, Category and Sub-category provide a mechanism for grouping like symptoms across the CIs, enabling trend reporting.

8.4. **PRIOITIZATION OF INCIDENTS**

Three metrics are used for determining the order in which incidents are processed. Incident priority is assigned when the Ticket is opened and is determined primarily on the basis of urgency and impact.

- Impact - The effect on business that an incident has.
- Urgency - The extent to which the incident's resolution can bear delay.
- Priority – How quickly the service desk should address the incident

Prioritization Model					
		IMPACT			
		1 Extensive /Widespread	2 Significant/Large	3 Moderate/Limited	4 Minor/Localized
		Multiple Patients *(10)*	One Patient *(5)*	No Patients *(3)*	No Patients *(0)*
URGENCY	1 CRITICAL *(20)*	**1** *(30)*	**1** *(25)*	**2** *(23)*	**2** *(20)*
	2 HIGH *(15)*	**1** *(25)*	**2** *(20)*	**2** *(18)*	**3** *(15)*
	3 MEDIUM *(10)*	**2** *(20)*	**3** *(15)*	**3** *(13)*	**3** *(10)*
	4 NORMAL *(0)*	**3** *(10)*	**4** *(5)*	**4** *(3)*	**4** *(0)*

The value in parenthesis is used to determine the weight of the priority.
Priority 1 – weight of 24-30
Priority 2 – weight of 16-23
Priority 3 – weight of 6-15
Priority 4 – weight of 0-5

IMPACT TABLE

RANK	DESCRIPTION
1. Extensive/ Widespread:	Entire department, floor, branch, line of business, external customer or multiple patients affected.
2. Significant/ Large:	Greater than 5 business people or 1 patient affected.
3. Moderate/ Limited:	Less than 5 business people affected. No patients involved.
4. Minor/ Localized:	1 business person affected. No patients involved.

URGENCY TABLE

RANK	DESCRIPTION
1. Critical:	Process stopped; customer cannot work. System and/or service is unavailable. Generally customers are unable to work and no workaround is available
2. High:	Process stopped, customer cannot work and require expedited restoration of service, but can bear minimal delays. System and/or service partially unavailable. Customers may or may not have a workaround, or workaround may only provide partial relief.
3. Medium:	Process affected; certain functions are unavailable to customers. System and/or service are degraded. May or may not have workaround available.
4. Normal	Process affected; certain functions are unavailable to customers. The work can be scheduled. System and/or service. Inconvenienced but still available (Work, Excel, etc). Workaround available.

9. INCIDENT MONITORING AND ESCALATION SUB-PROCESS

9.1. SUB-PROCESS OBJECTIVE

Incident Monitoring and Escalation is a sub-process of the Incident Management Process. The objective of this process is the continuous monitoring of outstanding incidents so that counter-measures may be introduced as soon as possible if service levels are likely to be breached.

9.2. GLOBAL INCIDENT MANAGEMENT SERVICE LEVELS

Priority	Definition	Incident Management Service Level	
		Response Time	Target Resolution
Critical	Major incident that is affecting a large group of users or critical business processes.	• Notice of the issue to relevant users and communication of the expected downtime must take place within 15 minutes	• < 1 hours
High	Significant incident that is causing work to slow or stop.	• Response to the customer must take place within 1 hours	• < 2 hours
Medium	Incidents that may be impacting work but for which there is a work-around.	• Response to the customer must take place within 2 hours	• < 3 business days
Normal	Incidents with low impact or where a work-around is easily followed.	• Response to the customer must take place within 24 business hours	• < 5 business days

9.3. ESCALATION

Escalation of an incident can take place at any time and at any support level in the resolution process, as defined in the Service Level Agreement.

- Functional escalation – involving personnel with more specialist skills, time or access privileges to solve the incident.
- Hierarchical escalation – involving a higher level of organization authority, when it appears that the current level of authority is insufficient to ensure that the incident will be resolved in time and/or satisfactorily.

9.4. SERVICE DESK RESPONSE TIMES

The following Priority Chart shows response time after initial Assessment/Assignment and creation of a ticket by the Service Desk (10 to 30 minutes.) Times are measured in clock hours and/or minutes unless otherwise specified. If a ticket is initiated by a telephone call, it will be created within 10 minutes; if initiated by eMail, the ticket will be created within 48 hours.

- The **Target Incident Response Acknowledgement Time** is the time the Service Desk has to respond to the customer to acknowledge receipt of the ticket and that it is being actively worked.
- The **Target Status Update Time** is the time interval the assigned group/individual has to update the Service Desk on ticket status.
- The **Customer Status Update Time** is the interval that the Service Desk has to update the customer on ticket status.
- The **Target Resolution Time** is the total time from ticket creation to resolve the incident and restore service to the user.
- The **Target Percentage of Calls Resolved on Time** is the percentage of calls that meet the priority time frame criteria.

Incident Priority Chart

Priority	Target Incident Response Acknowledgement Time (*to Customer from the Service Desk*)	Target Status Update Time (*to Service Desk from assigned group/person*)	Customer Status Update Time Goal	Target Resolution Time	Target % of Calls Resolved on Time
Critical	15 minutes	Within 15 minutes, then every hour by the assigned working team until resolution has been achieved or identified	Service Desk will: • Provide initial communication within 60min • Update Service Alert Page every 60 min • Send resolution notice	1 hour	90%
High	1 hour	Within 1 hour, then every 2 hours thereafter by the assigned working team until resolution has been achieved or identified	Service Desk will: • Provide initial communication within 60min • Update Service Alert Page every 60 min • Send resolution notice	2 hours	90%
Medium	24 hours	Within 3 hours	Service Desk will provide status upon request	3 business days	80%
Normal	24 hours	Within 1 business day	Service Desk will provide status upon request	5 business days	80%