Infasme Support

Incident Management Process

[Version 1.0]

Table of Contents

About this document

This document describes the Incident Process. The Process provides a consistent method for everyone to follow when Clients report issues regarding services from Infasme Support Center.

Who should use this document?

This document should be used by:

- Engineers responsible for the restoration of services
- Engineers involved in the operation and management of Incident Process

Summary of changes

This section records the history of significant changes to this document. Only the most significant changes are described here.

Version	Date	Author	Description of change
1.0		Khaled Moawad	Initial version

Where significant changes are made to this document, the version number will be incremented by 1.0.
Where changes are made for clarity and reading ease only and no change is made to the meaning or intention of this document, the version number will be increased by 0.1.

Chapter 1. Incident Process

1.1. Primary goal

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 here as service operation within SLA limits.

1.2. Process Definition:

Incident Management includes any event which disrupts, or which could disrupt, a service. This includes events which are communicated directly by users or Infasme staff through the Service Desk or through an interface from Event Management to Incident Management tools.

1.3. Objectives - Provide a consistent process to track incidents that ensures:

- Incidents are properly logged
- Incidents are properly routed
- Incident status is accurately reported
- Queue of unresolved incidents is visible and reported
- Incidents are properly prioritized and handled in the appropriate sequence
- Resolution provided meets the requirements of the SLA for the customer

1.4. Definitions

1.4.1. Customer

A customer is someone who buys goods or Services. The Customer of an IT Service Provider is the person utilizing the service purchased by the customer's organization. The term Customers is also sometimes informally used to mean Users.

1.4.2. Impact

Impact is determined by how many personnel or functions are affected. There are three grades of impact:

- 3 - Low – One or two personnel. Service is degraded but still operating within SLA specifications
- 2 - Medium – Multiple personnel in one physical location. Service is degraded and still functional but not operating within SLA specifications. It appears the cause of the incident falls across multiple service provider groups
- 1 - High – All users of a specific service. Personnel from multiple agencies are affected. Public facing service is unavailable

The impact of an incident will be used in determining the priority for resolution.

1.4.3. Incident

An incident is an unplanned interruption to an IT Service or reduction in the Quality of an IT Service. Failure of any Item, software or hardware, used in the support of a system that has not yet affected service is also an Incident. For example, the failure of one component of a redundant high availability configuration is an incident even though it does not interrupt service.

An incident occurs when the operational status of a production item changes from working to failing or about to fail, resulting in a condition in which the item is not functioning as it was designed or implemented. The resolution for an incident involves implementing a repair to restore the item to its original state.

A design flaw does not create an incident. If the product is working as designed, even though the design is not correct, the correction needs to take the form of a service request to modify the design. The service request may be expedited based upon the need, but it is still a modification, not a repair.

1.4.4. Incident Repository

The Incident Repository is a database containing relevant information about all Incidents whether they have been resolved or not. General status information along with notes related to activity should also be maintained in a format that supports standardized reporting. At Infasme Support Center, the incident repository is contained within SupportSystem.com and integrated with Microsoft CRM.

1.4.5. Priority

Priority is determined by utilizing a combination of the incident's impact and severity. For a full explanation of the determination of priority refer to the paragraph titled Priority Determination.

1.4.6. Response

Time elapsed between the time the incident is reported and the time it is assigned to an individual for resolution.

1.4.7. Resolution

Service is restored to a point where the customer can perform their job. In some cases, this may only be a work around solution until the root cause of the incident is identified and corrected.

1.4.8. Service Agreement

A Service Agreement is a general agreement outlining services to be provided, as well as costs of services and how they are to be billed. A service agreement may be initiated between OSF/ISD and another agency or a non-state government entity. A service agreement is distinguished from a Service Level Agreement in that there are no ongoing service level targets identified in a Service Agreement.

1.4.9. Service Level Agreement

Often referred to as the SLA, the Service Level Agreement is the agreement between Infasme Support Center and the customer outlining services to be provided, and operational support levels as well as costs of services and how they are to be billed.

1.4.10. Service Level Objective

Service Level Objective is a commitment that is documented in a Service Level Agreement. Service Level Objectives are based on Service Level Requirements, and are needed to ensure that the IT Service continues to meet the original Service Level Requirements.

1.4.11. Severity

Severity is determined by how much the user is restricted from performing their work. There are three grades of severity:

- 3 - Low - Issue prevents the user from performing a portion of their duties.
- 2 - Medium - Issue prevents the user from performing critical time sensitive functions
- 1 - High - Service or major portion of a service is unavailable

The severity of an incident will be used in determining the priority for resolution.

1.5. Incident Scope

The Incident process applies to all specific incidents in support of larger services already provided by Infasme Support Center.

1.5.1. Exclusions

Request fulfilment, i.e., Service Requests and Service Catalog Requests are not handled by this process.

Root cause analysis of original cause of incident is not handled by this process. Refer to Problem Management. The need for restoration of normal service supersedes the need to find the root cause of the incident. The process is considered complete once normal service is restored.

1.6. Inputs and Outputs

Input	From
Incident (verbal or written)	Customer
Categorization Tables	Functional Groups
Assignment Rules	Functional Groups

Output	To
Standard notification to the customer when case is closed	Customer.

1.7. Metrics

Metric	Purpose
Process tracking metrics # of incidents by type, status, and customer – see detail under **Reports and Meetings**	To determine if incidents are being processed in reasonable time frame, frequency of specific types of incidents, and determine where bottlenecks exist.

Chapter 2. Roles and Responsibilities

Responsibilities may be delegated, but escalation does not remove responsibility from the individual accountable for a specific action.

2.1. Infasme Support Center Service Desk

- Owns all reported incidents
- Ensure that all incidents received by the Service Desk are recorded in CRM
- Identify nature of incidents based upon reported symptoms and categorization rules supplied by provider groups
- Prioritize incidents based upon impact to the users and SLA guidelines
- Responsible for incident closure
- Delegates responsibility by assigning incidents to the appropriate provider group for resolution based upon the categorization rules
- Performs post-resolution customer review to ensure that all work services are functioning properly and all incident documentation is complete
- Prepare reports showing statistics of Incidents resolved / unresolved.
- Gets complete details of customer environment and system logs.
- Tries to find a fast resolution and workaround if possible.

2.2. Service Provider Group

- Composed of technical and functional staff involved in supporting services
- Correct the issue or provide a work around to the customer that will provide functionality that approximates normal service as closely as possible.
- If an incident reoccurs or is likely to reoccur, notify problem management so that root cause analysis can be performed and a standard work around can be deployed

Chapter 3. Incident Categorization, Target Times, Prioritization, and Escalation

In order to adequately determine if SLA's are met, it will be necessary to correctly categorize and prioritize incidents quickly.

3.1. Categorization

The goals of proper categorization are:

- Identify Service impacted and appropriate SLA and escalation timelines
- Indicate what support groups need to be involved
- Provide meaningful metrics on system reliability

For each incident the specific service (as listed in the published Service Catalog) will be identified. It is critical to establish with the user the specific area of the service being provided. For example, if it's Documentum, is it Archive Department, Human Resources, or another area? If it's Documnetum for Archive, is it for Find Documents, Adding More Documents, etc.? Identifying the service properly establishes the appropriate Service Level Agreement and relevant Service Level Targets.

In addition, the severity and impact of the incident need to also be established. All incidents are important to the user, but incidents that affect large groups of personnel or mission critical functions need to be addressed before those affecting 1 or 2 people.

Does the incident cause a work stoppage for the user or do they have other means of performing their job? An example would be a broken link on a web page is an incident but if there is another navigation path to the desired page, the incident's severity would be low because the user can still perform the needed function.

The incident may create a work stoppage for only one person but the impact is far greater because it is a critical function. An example of this scenario would be the person processing payroll having an issue which prevents the payroll from processing. The impact affects many more personnel than just the user.

3.2. Priority Determination

The priority given to an incident that will determine how quickly it is scheduled for resolution will be set depending upon a combination of the incident severity and impact.

Incident Priority			Severity		
			3 - Low Issue prevents the user from performing a portion of their duties.	2 - Medium Issue prevents the user from performing critical time sensitive functions	1 - High Service or major portion of a service is unavailable
Impact	3 - Low	One or two personnel Degraded Service Levels but still processing within SLA constraints	3 - Low	3 - Low	2 - Medium

	2 - Medium	Multiple personnel in one physical location Degraded Service Levels but not processing within SLA constraints or able to perform only minimum level of service It appears cause of incident falls across multiple functional areas	2 - Medium	2 - Medium	1 - High
	1 - High	All users of a specific service Personnel from multiple agencies are affected Public facing service is unavailable Any item listed in the Crisis Response tables	1 - High	1 - High	1 - High

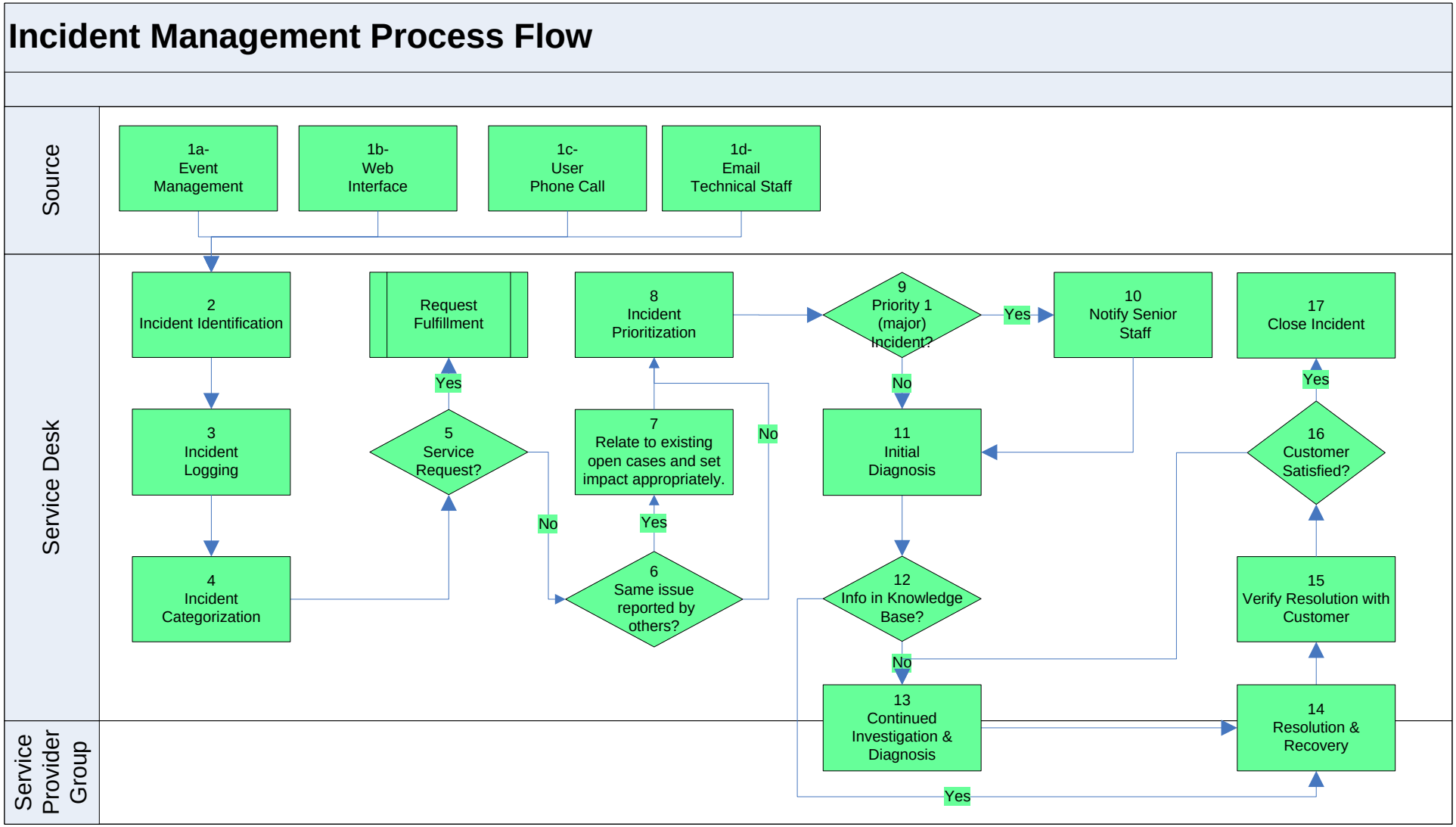
3.3. Target Times

Incident support for existing services is provided 24 hours per day, 7 days per week, and 365 days per year. Following are the current targets for response and resolution for incidents based upon priority.

Priority	Target Response
3 - Low	90% - 4 business hours
2 - Medium	90% - 3 hours
1 - High	95% - 1 Hour

Chapter 4 Process Flow

The following is the standard incident management process flow outlined in ITIL Service Operation but represented as a swim lane chart with associated roles within OSF ISD.



4.1. Incident Management Process Flow Steps

Role	Step	Description
Requesting Customer	➢ 1	Incidents can be reported by the customer or technical staff through various means, i.e., phone, email, or a self service web interface. Incidents may also be reported through the use of automated tools performing Event Management.
Infasme Support Center Service Desk	➢	Incident identification **Work cannot begin on dealing with an incident until it is known that an incident has occurred. As far as possible, all key components should be monitored so that failures or potential failures are detected early so that the incident management process can be started quickly.**
	➢	Incident logging All incidents must be fully logged and date/time stamped, regardless of whether they are raised through a Service Desk telephone call or whether automatically detected via an event alert. All relevant information relating to the nature of the incident must be logged so that a full historical record is maintained – and so that if the incident has to be referred to other support group(s), they will have all relevant information at hand to assist them.
	➢	Incident categorization All incidents will relate to one of the published services listed in the Service Catalog. If the customer is calling about an issue they have that is not related to one of the services in the catalog, then it is not an incident.
	➢	Is this actually a Service Request incorrectly categorized as an incident? If so, update the case to reflect that it is a Service Request and follow the appropriate Service Request process.
	➢	Has this issue already been reported by others?
	➢	If this is another person reporting the same issue, relate the issue to the cases already reported. More people reporting the same issue means the impact of the issue is broader than what might have been reported at first. The impact needs to be recorded base upon current knowledge of the impact.
	➢	Incident prioritization Before an incident priority can be set, the severity and impact need to be assessed. See paragraph 3.2 Incident Prioritization. Once the severity and impact are set, the priority can be derived using the prescriptive table.
	➢	Is this a priority 1 (major) incident?
	➢	If this is a priority 1 incident meaning that a service is unavailable in part or whole, all mid level and senior of Infasme Support Center management should be alerted to make certain any resources necessary to the resolution will be immediately made available.
	➢	Initial diagnosis If the incident has been routed via the Service Desk, the Service Desk analyst must carry out initial diagnosis, using diagnostic scripts and known error information to try to discover the full symptoms of the incident and to determine exactly what has gone wrong. The Service Desk representative will utilize the collected information on the symptoms and use that information to initiate a search of the Knowledge Base to find an appropriate solution. If possible, the Service Desk Analyst will resolve the incident and close the incident if the resolution is successful.
	➢	▪ Is the necessary information in the Knowledge Base to resolve the incident? If not, the case should then be assigned to the provider group that supports the service.

Role	Step	Description
	➢	If the necessary information to resolve the incident is not in the Knowledge Base, the incident must be immediately assigned to an appropriate provider group for further support. The assignee will then research the issue to determine cause and remediation options.
	➢	After a possible resolution has been determined either from the Knowledge Base or through research, attempt the resolution.
	➢	Verify with the customer that the resolution was satisfactory and the customer is able to perform their work. An incident resolution does not require that the underling cause of the incident has been corrected. The resolution only needs to make it possible for the customer to be able to continue their work.
OSF ISD Service Desk	➢	If the customer is satisfied with the resolution, proceed to closure, otherwise continue investigation and diagnosis.
	➢	Incident Closure The Service Desk should check that the incident is fully resolved and that the users are satisfied and willing to agree the incident can be closed. The Service Desk should also check the following: **Closure categorization**. Check and confirm that the initial incident categorization was correct or, where the categorization subsequently turned out to be incorrect, update the record so that a correct closure categorization is recorded for the incident – seeking advice or guidance from the resolving group(s) as necessary. **User satisfaction survey**. Carry out a user satisfaction call-back or e-mail survey for the agreed percentage of incidents. **Incident documentation**. Chase any outstanding details and ensure that the Incident Record is fully documented so that a full historic record at a sufficient level of detail is complete. **Ongoing or recurring problem?** Determine (in conjunction with resolver groups) whether it is likely that the incident could recur and decide whether any preventive action is necessary to avoid this. In conjunction with Problem Management, raise a Problem Record in all such cases so that preventive action is initiated. **Formal closure**. Formally close the Incident Record. ▪

Chapter 5. Incident Escalation

According to ITIL standards, although assignment may change, ownership of incidents always resides with the Service Desk. As a result, the responsibility of ensuring that an incident is escalated when appropriate also resides with the Service Desk.

The Service Desk will monitor all incidents, and escalate them based on the following guidelines:

Priority	Time Limit before Escalation	
3 - Low	4 business hours	Manager
2 - Medium	3 hours	Manager
	If on-call contact cannot be reached during non-business hours	Manager
	If neither on-call contact or their manager cannot be reached during non-business hours	Senior Mgt
	24 hours	Senior Mgt
1 - High	Immediate	Manager
	Immediate	Senior Mgt

5.1. Functional Escalation

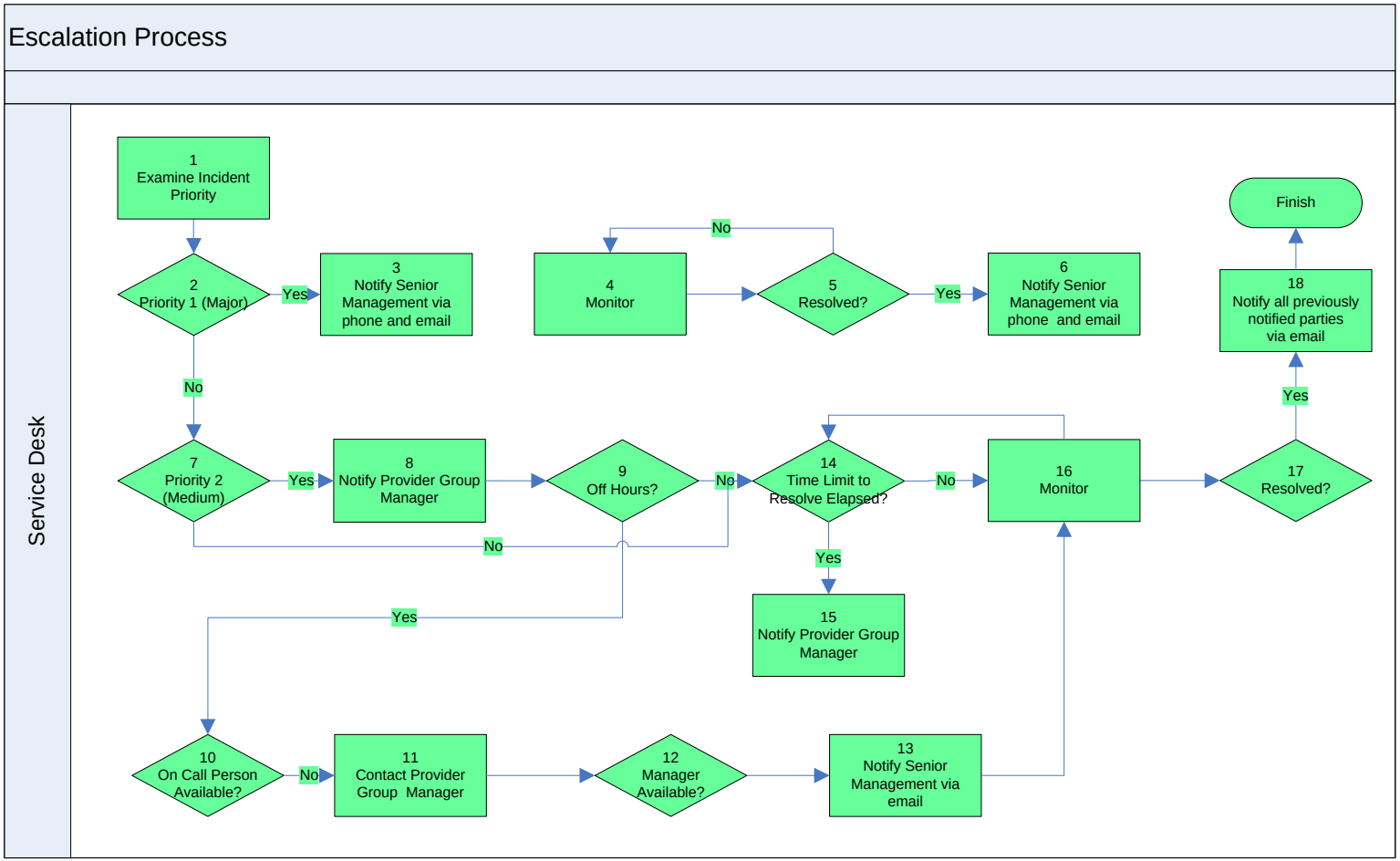
Infasme Support Center does not employ an official tiered support system that utilizes escalation from one provider group to another. When the Service Desk receives notification of an incident, they are to perform the initial identification and diagnosis to classify the incident according to service category and prioritization. If the incident is a known problem with a known solution, the Service Desk will attempt a resolution. If it is not a known problem or if the attempted solution fails, they will delegate responsibility for an incident to an appropriate provider group.

5.2. Escalation Notifications:

Any time a case is escalated, notification will occur to various individuals or groups depending upon the priority of the incident. Following are basic guidelines for notifications:

- The default mechanism for notification will be by email unless otherwise specifically stated.
- Whenever escalation or notification by phone is indicated, all known numbers for contact should be utilized, leaving voice mail on each until person is contacted. The master source for on call information will be the on-call files located in the Call Center System.
- Senior management notification will include CIO, CTO, and all functional managers. Escalation of a case does not remove the assignment from an individual. It is up to the manager of the provider group to make certain the right personnel are assigned. When additional personnel need to be involved, they may be added as interested parties.
- Any time a case is escalated, the case will be updated to reflect the escalation and the following notifications will be performed by the Service Desk:
- Customer will receive a standard escalation email informing them of the escalation.
- Person to whom case is currently assigned will be notified.
- Manager of functional group to whom case is currently assigned will be notified

5.3. Incident Escalation Process:



5.4. Incident Escalation Process Steps:

All escalation process steps are performed by the Service Desk. Some of the steps may be automated.

Step	Description
➢	Examine all open incidents and determine actions based upon incident priority.
➢	**Is this a priority 1 (high priority) incident?**
➢	If it is a high priority incident, immediately notify Infasme Support Center mid-level and senior management personnel. Senior management personnel should be contacted by phone.
➢	Monitor the status of the priority 1 incident providing informational updates to management at a minimum of every 4 hours.
➢	Has the incident been resolved? If not continue to monitor.
➢	If the incident has been resolved, notify Infasme Support Center mid-level and senior management of the resolution. Senior management should be notified by phone during business hours.
➢	Is this a priority 2 (medium priority) incident?
➢	If so, notify the manager of the provider group performing the resolution. Notification should be by email.
➢	Has the incident occurred during business hours or off hours? If during business hours, proceed to step 14.
➢	If the incident occurred during off hours, is the on call person available?
➢	If the on call person is not available, call the manager of the provider group assigned for resolution.
➢	▪ Is the manager of the provider group available?
➢	If neither the provider group on-call person or the manager of the provider group is available, notify senior management via email and phone.
➢	Has the time limit to resolve the incident elapsed?
➢	If the time limit to resolve has elapsed, notify the manager of the provider group via email.
➢	Continue to monitor the incident
➢	▪ Has the incident been resolved?
➢	▪ If the incident has been resolved notify the customer and all personnel previously contacted of the resolution.

Chapter 6. RACI Chart

Obligation	Role Description
Responsible	Responsible to perform the assigned task
Accountable (only 1 person)	Accountable to make certain work is assigned and performed
Consulted	Consulted about how to perform the task appropriately
Informed	Informed about key events regarding the task

	Activity	SPG Mgr	SPG SME's	SPG Team	Service Desk	OSF Service Desk Mgr	
	Record Incident in CRM				R	A	
	Accept Information from Customer	R	R	R	R	A/R	

Chapter 7. Reports and Meetings

A critical component of success in meeting service level targets is for Infasme Support Center to hold itself accountable for deviations from acceptable performance. This will be accomplished by producing meaning reports that can be utilized to focus on areas that need improvement. The reports must then be used in coordinated activities aimed at improving the support.

7.1. Reports

7.1.1. Service Interruptions

A report showing all incidents related to service interruptions will be reviewed weekly during the operational meeting. The purpose is to discover how serious the incident was, what steps are being taken to prevent reoccurrence, and if root cause needs to be pursued.

7.1.2. Metrics

Metrics reports should generally be produced monthly with quarterly summaries. Metrics to be reported are:

- Total numbers of Incidents (as a control measure)
- Breakdown of incidents at each stage (e.g. logged, work in progress, closed etc)
- Size of current incident backlog
- Number and percentage of major incidents
- Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code
- Percentage of incidents handled within agreed response time as defined by SLA's standards
- Number of incidents reopened and as a percentage of the total
- Number and percentage of incidents incorrectly assigned
- Number and percentage of incidents incorrectly categorized
- Percentage of Incidents closed by the Service Desk without reference to other levels of support (often referred to as 'first point of contact')
- Number and percentage the of incidents processed per Service Desk agent
- Number and percentage of incidents resolved remotely, without the need for a visit
- Breakdown of incidents by time of day, to help pinpoint peaks and ensure matching of resources.

7.1.3. Meetings

The Quality Assurance Manager will conduct sessions with each service provider group to review performance reports. The goal of the sessions is to identify:

- Processes that are working well and need to be reinforced.
- Patterns related to incidents where support failed to meet targets
- Reoccurring incidents where the underlying problem needs to be identified and resolution activities are pursued
- Identification of work around solutions that need to be developed until root cause can be corrected

Chapter 8. Incident Policy

The Incident process should be followed for all incidents covered by an existing service agreement, regardless of whether the request is eventually managed as a project or through the Incident process.

Support for or enhancement of existing services identified in existing Service Agreements requires an Incident case to be opened.

If Infasme Support Center already provides a service to a customer, but that customer wants to significantly expand that service beyond the existing cost support model in place, the request should be treated as a Service Catalog Request and forwarded to the Infasme Support Center Service Desk.

Incidents should be prioritized based upon impact to the customer and the availability of a workaround.

"Incident Ownership remains with the Service Desk! Regardless of where an incident is referred to during its life, ownership of the incident remains with the Service Desk at all times. The Service Desk remains responsible for tracking progress, keeping users informed and ultimately for Incident Closure." – *ITIL Service Operation*

Rules for re-opening incidents - Despite all adequate care, there will be occasions when incidents recur even though they have been formally closed. If the incident recurs within one working day then it can be re-opened – but that beyond this point a new incident must be raised, but linked to the previous incident(s).

Workarounds should be in conformance with Infasme Support Center standards and policies.