ITSM Process Description

Office of Information Technology

Incident Management

Table of Contents

1. Introduction

The purpose of this document is to provide a general overview of the Office of Information Technology (OIT) Incident Management Process. It includes Incident Management goals, objectives, scope, benefits, key terms, roles, responsibilities, authority, process diagrams and associated activity descriptions.

The content within this general overview is based on the best practices of the ITIL® framework[1].

2. Incident Management Goals, Objectives, CSFs and KPIs

Goals, objectives and critical success factors (CSFs) define why Incident Management is important to the Office of Information Technology's overall vision for delivering and supporting effective and efficient IT services. This section establishes the fundamental goals, objectives and CSFs that underpin the Incident Management process. The agreed and documented goals, objectives and CSFs provide a point of reference to check implementation and operational decisions and activities.

Incident Management is the process responsible for managing the lifecycle of all Incidents irrespective of their origination.

The goals for the Incident Management process are to:

- *Restore normal service operation as quickly as possible*
- *Minimize the adverse impact on business operations*
- *Ensure that agreed levels of service quality are maintained*

To achieve this, the objectives of OIT's Incident Management process are to:

- *Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of Incidents*
- *Increase visibility and communication of Incidents to business and IT support staff*
- *Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur*
- *Align Incident management activities and priorities with those of the business*
- *Maintain user satisfaction with the quality of IT services*

CSFs identified for the process of Incident Management and associated Key Performance Indicators (KPIs) are:

CSF #1 - OIT commitment to the Incident Management process; all departments using the same process.

KPI 1.1 - Number of self service tickets via a customer portal verses tickets created by the Service Desk.

1.1.1 - Review metrics via ITSM tool on all incident requests recorded and escalated within OIT.

KPI 1.2 - Management is known to review standardized reports produced by the Incident Management process.

1.2.1 - ITSM tool, standardized/customized reports made available.

KPI 1.3 - Number of incidents in ITSM tool per department.

1.3.1 - Review metrics via ITSM tool on all incident requests recorded and escalated within OIT.

KPI 1.4 - Management is known to be a user of the Incident Management process.

1.4.1 - Review metrics via ITSM tool on all incident requests recorded and escalated within OIT.

CSF #2 - Consistent, positive experience for all customers

KPI 2.1 - Improved assignment, response and closure time.

2.1.1 Review metrics via ITSM tool on all incident requests recorded and escalated within OIT specifically focusing on MTTR and customer satisfaction surveys.

KPI 2.2 - Customer use of self service portal increases.

2.2.1 Review metrics via ITSM tool on all incident requests recorded via self service portal.

KPI 2.3 - Amount of journal entries consistent with SLA.

2.3.1 Review metrics via ITSM tool for services with SLA specifically focusing on the quantity and quality of updates in incident requests.

KPI 2.4 - number of incidents reopened.

2.4.1 Review metrics via ITSM tool specifically looking at incidents that were reopened.

CSF #3 Ability to track internal process performance and identify trends.

KPI 3.1 - Process performance meets established standards in OIT Baseline SLA including: Assignment time, response time, resolution time, closure time.

3.1.1 Review metrics via ITSM tool on all incident requests recorded and escalated within OIT; measuring MTTR and SLA requirements.

KPI 3.2 - Number of re-assigned tickets between departments.

3.2.1 Review metrics via ITSM tool on all incident requests recorded specifically looking at incidents that were reassigned.

3. Incident Management Scope

Scope refers to the boundaries or extent of influence to which Incident Management applies to the Office of Information Technology. OIT's Incident Management process consists of three sub-processes titled Tier 1, Tier 2 and Verify Document and Close (VD&C). The Tier 1 sub-process is initiated by any department dealing directly with the user and able to resolve the incident without involving additional departments. The Tier 2 sub-process is initiated when an Incident requires multiple departments to resolve an Incident. The VD&C sub-process provides a consistent experience for the user ensuring high levels of customer service. Although it is an optional process, it is considered best practice for departments to adhere to. Boundaries for the extent of deployment within the Office of Information Technology are identified for users, service providers, geography, IT services and service components and environment.

3.1 General Process Scope

Any event which disrupts, or which could disrupt, a service, including those:

- Reported directly by users
- Reported and/or logged by technical staff
- Detected by Event Management
- Reported and/or logged by Suppliers

Incident Management encompasses all IT service providers, internal and third parties, reporting, recording or working on an Incident.

All Incident Management activities should be implemented in full, operated as implemented, measured and improved as necessary.

3.2 Deployment Scope

Incident Management will be deployed and applicable to:

- Users covered by Service Level Agreements (SLAs) specifying service targets for resolution of Incidents
- Service Providers adopting the Incident Management responsibilities outlined by Service Level Agreements, Operating Level Agreements (OLAs), and Underpinning Contracts (UCs)
- Services to which Incident Management Resolution Targets agreed in Service Level Agreements apply

4. Benefits

There are several qualitative and quantitative benefits that can be achieved, for both the IT service providers and users, by implementing an effective and efficient Incident Management process. The Incident Management project team has agreed that the following benefits are important to OIT and will be assessed for input to continuous process improvement throughout the Incident Management process lifecycle:

- Capturing accurate data across OIT to analyze the level of resources applied to the Incident Management process
- Informing business units of the services OIT provides and the level of support and maintenance required for ongoing service levels
- Minimize impacts to business functions by resolving incidents in a timely manner
- Providing the best quality service for all users

4.1 Benefits To The IT Service Providers

Incident Management is highly visible to the business and it is easier to demonstrate its value than most areas in Service Operation. A successful Incident Management process can be used to highlight other areas that need attention:

- Improved ability to identify potential improvements to IT services
- Better prioritization of efforts
- Better use of resources, reduction in unplanned labor and associated costs
- More control over IT services
- Better alignment between departments
- More empowered IT staff
- Better control over vendors through Incident Management metrics

4.2 Benefits To The Users

- Higher service availability due to reduced service downtime
- Reduction in unplanned labor and associated costs
- IT activity aligned to real-time business priorities
- Identification of potential improvements to services
- Identification of additional service or training requirements for the business or IT

5. Key Terms & Definitions

Common terms and vocabulary may have disparate meanings for different organizations, disciplines or individuals. It is essential early in a process implementation to agree on the common usage of terms. It is recommended, where possible, not to diverge from Best Practice unless necessary as many other users and suppliers may be also using the same terms if they are following best practice process frameworks. This brings unity in the areas of communication to help enhance not only internal dialog but also documentation, instructions, presentations, reports and interaction with other external bodies. The following key terms and definitions for the Incident Management process have been agreed by the Incident Management Project Team on behalf of the Office of Information Technology. These terms and definitions will be used throughout the process documentation, communications, training materials, tools and reports.

The following are key terms and Best Practice definitions used in Incident Management. The Incident Management Project Team carefully read and agreed to each key term. Any changes and/or additional key terms should be listed, defined and agreed in this section.

Note: Key terms and definitions must be verified and documented consistently across all ITIL processes implemented in the organization.

Change Management: The process for managing the addition, modification or removal of anything that could have an effect on IT Services resulting in minimal disruption to services and reduced risk. The Scope should include all IT Services, Configuration Items, Processes and Documentation.

Escalation: An Activity that obtains additional resources when these are needed to meet service level targets or user expectations. Escalation may be needed within any IT service management process but is most commonly associated with Incident Management, Problem Management and the management of user complaints. There are two types of escalation: functional escalation and hierarchical escalation.

Event: Any change of state that has significance for the management of an IT service or other configuration item. The term can also be used to mean an alert or notification created by any IT service, Configuration Item or a Monitoring tool. Events typically require IT Operations personnel to take actions and often lead to Incidents being logged.

Failure: Loss of ability to operate to specification, or to deliver the required output. The term Failure may be used when referring to IT services, processes, activities and Configuration Items. A Failure often causes an Incident.

Function: A team or group of people and the tools they use to carry out one of more Processes or Activities; for example, the Service Desk.

Group: A number of people who are similar in some way. People who perform similar activities, even though they may work in different departments within OIT.

Hierarchic Escalation: Informing or involving more senior levels of management to assist in an escalation.

Impact: A measure of the effect of an Incident, Problem, or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and urgency are used to assign priority.

Incident: An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a Configuration Item that has not yet impacted service is also an Incident; for example, failure of one disk from a mirror set.

Incident Management: The process responsible for managing the lifecycle of all Incidents. The primary purpose of Incident Management is to restore normal IT service operation as quickly as possible.

Incident Record: A record containing the details of an Incident. Each Incident record documents the lifecycle of a single Incident.

Incident Workflow: A way of predefining the steps that should be taken to handle a process for dealing with a particular type of Incident in an agreed way.
Incident Status Tracking: Tracking Incidents throughout their lifecycle for proper handling and status reporting using indicators such as Open, In progress, Resolved and Closed.

Normal Service Operation: The Service Operation defined within the Service Level Agreement (SLA) limits.

Primary Technician: The technician who has responsibility for correcting the root cause issue and must keep users informed of progress. They are also responsible for coordinating child records.

Priority: A category used to identify the relative importance of an Incident, Problem or Change. Priority is based on impact and urgency and is used to identify required times for actions to be taken. For example, the SLA may state that Priority 2 Incidents must be resolved within 12 hours.

Priority 1 Incident: The highest category of impact for an Incident which causes significant disruption to the business. A separate procedure with shorter timescales and greater urgency should be used to handle Major Incidents.

Problem: The cause of one or more incidents.

Quality Assurance (QA): Optional departmental process for ensuring a desired level of customer service. This process is defined by the departments that choose to review tickets prior to closure.

RACI Matrix: A responsibility matrix showing who is Responsible, Accountable, Consulted and Informed for each activity that is part of the Incident Management process.

Role: A set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process. One person or team may have multiple roles; for example, the roles of Configuration Manager and Change Manager may be carried out by a single person.

Service Desk: The Single Point of Contact between the Service Provider and the users. A typical Service Desk manages Incidents and Service Requests and also handles communication with the users.

Severity: A measure of how long it will be until an Incident, Problem or Change has a significant impact on the business. For example, a high Impact Incident may have low urgency, if the impact will not affect the business until the end of the financial year. Impact and urgency are used to assign Priority.

Tier 1: Line staff who are the subject matter experts for assessing, planning and monitoring Incident Management for their functional organization and specific technology platform. They function as contact people between the different departments for a specific process and may be responsible for the design of processes within their own departments.

Tier 2: More in-depth technical support than tier 1. Tier 2 support personnel may be more experienced or knowledgeable on a particular product or service. Additionally, Tier 2 may be able to provide onsite troubleshooting and/or resolution. Specialized departments (i.e. Networks, Servers, Video) will provide Tier 2 Support in their respective areas of expertise.

User: Someone who uses the IT service on a day-to-day basis. Sometimes informally referred to as the customer.

6. Roles & Responsibilities

A role refers to a set of connected behaviors or actions that are performed by a person, team or group in a specific context. Process roles are defined by the set of responsibilities, activities and authorities granted to the designated person, team or group.

Some process roles may be full-time jobs while others are a portion of a job. One person or team may have multiple roles across multiple processes. Caution is given to combining roles for a person, team or group where separation of duties is required. For example, there is a conflict of interest when a software developer is also the independent tester for his or her own work.

Regardless of the scope, role responsibilities should be agreed by management and included in yearly objectives. Once roles are assigned, the assignees must be empowered to execute the role activities and given the appropriate authority for holding other people accountable.

All roles and designated person(s), team(s), or group(s) should be clearly communicated across the organization. This should encourage or improve collaboration and cooperation for cross-functional process activities.

6.1 Incident Management Process Owner

Profile	The person fulfilling this role is responsible for ensuring that the process is being performed according to the agreed and documented process and is meeting the aims of the process definition. There will be one, and only one, Incident Management Process Owner.

Responsibilities	• Assist with and ultimately be responsible for the process design • Define appropriate policies and standards to be employed throughout the process • Define Key Performance Indicators (KPIs) to evaluate the effectiveness and efficiency of the process and design reporting specifications • Ensure that quality reports are produced, distributed and utilized • Review KPIs and take action required following the analysis • Periodically audit the process to ensure compliance to policy and standards • Address any issues with the running of the process • Review opportunities for process enhancements and for improving the efficiency and effectiveness of the process • Ensure that all relevant staff have the required technical and business understanding, knowledge and training in the process and are aware of their role in the process • Ensure that the process, roles, responsibilities and documentation are regularly reviewed and audited • Interface with the line management, ensuring that the process receives the needed staff resources • Provide input to the on-going Service Improvement Program • Communicate process information or changes, as appropriate, to ensure awareness • Review integration issues between the various processes • Integrate the process into the line organization • Promote the Service Management vision to top-level/senior management • Function as a point of escalation when required • Ensure that there is optimal fit between people, process and technology/tool • Ensure that the Incident Management process is Fit for Purpose • Attend top-level management meetings to assess and represent the Incident Management Requirements and provide Management Information

6.2 Incident Management Process Manager

Profile	Tier 1 Technicians are the line staff who are the subject matter experts for assessing, planning and monitoring Incident Management for their functional organization and/or specific technology platform. They function as initial contact between those reporting incidents and the IT organization. Technicians residing in departments where Tier 2 support is commonly provided may function as Tier 1 support. In this case the Technician is the initial contact with those reporting incidents ands provides triage and resolution.
Responsibilities	• Promote the Incident Management process • Ensure the Incident Management process is used correctly • Provide management and other processes with strategic decision making information related to Incidents and potential Problems • Ensure Incident Management KPIs are met • Ensure that the Incident Management process operates effectively and efficiently through 1st, 2nd, and 3rd line support and Third Party organizations • Ensure Incident Management Staff are empowered in their jobs • Maximize the fit between people, process and technology • Provide the resolution of Incidents in a proper and timely manner as it is the end-responsibility of Incident Management. Ensure that Incidents are resolved in a proper and timely manner and the resolutions adhere to objectives set forth in Service Level Agreements • Participate with the Incident Management Process Owner in developing and maintaining the Incident Management Process, policies and procedures • Drive the efficiency and effectiveness of the Incident Management Process • Produce Management Information • Monitor the Incident Management process, using qualitative and quantitative Key Performance Indicators and make recommendations for improvement • Play a key role in developing and maintaining the Incident Management systems • Manage Major Incidents

	• Escalate to Line Management if Service Levels are threatened to be breached • Identify training requirements of support staff and ensure that proper training is provided to meet the requirements • Identify opportunities for improving the tools used • Audit the Incident Management process • Escalate to Management and the Incident Management Process Owner in the event of a conflict between process and Management • Promote the Service Desk with the end-user community, through the maintenance of a web-page, info mails, bulletins and training Service Desk staff in communication skills, where needed • Provide Service Desk staff with appropriate information to enable them to perform their function effectively. This includes process information, technical knowledge, record allocation information, and access to Known Error information

6.3 Tier 1 Technician

Profile	Tier 1 Technicians are the line staff who are the subject matter experts for assessing, planning and monitoring Incident Management for their functional organization and/or specific technology platform. They function as initial contact between those reporting incidents and the IT organization. Technicians residing in departments where Tier 2 support is commonly provided may function as Tier 1 support. In this case the Technician is the initial contact with those reporting incidents ands provides triage and resolution.
Responsibilities	• Log relevant Incidents • Categorize and prioritize incidents • Provide first-line investigation and diagnosis • Resolve those Incidents they are able to • Escalate incidents that cannot resolve within agreed timescales • Close all assigned and resolved Incidents • Communicate with users; keep them informed of incident progress, notifying them of impending changes or agreed outages, etc. • Take ownership of assigned Incidents

	• Understand and use the process, procedures, work instructions, policies, required documentation and tools

6.4 Tier 2 Incident Coordinator

Profile	Incident Coordinators are the line staff who are responsible for the planning and monitoring of the Incident Management process and associated records. They function as contact people between the different departments for a specific process and may be responsible for the design of processes within their own departments. In general the Tier 2 Incident Coordinator: • May be a department lead or a person identified as an Incident coordinator for a length of time. • Understands how the specific technology fits in with the overall IT service and Service Lifecycle • Must be an effective communicator • Is a member of a department who is able to combine daily departmental activities with the coordination role
Responsibilities	• Managing ownership of Incident records while providing monitoring and tracking of Incidents for their department • Validates, accepts and assigns Incident records to Tier 2 Incident Technicians • Closing all assigned and resolved Incidents • Determine whether an Incident record requires special reporting • Understand the process, procedures, work instructions, policies, required documentation and tools • Use the process, procedures, work instructions, policies, required documentation and tools as designed • Produce usage and performance data for his or her specific technology platform and report on performance against Incident Management process CSFs & KPIs • Initiate the Verify, Document and Close process

6.5 Tier 2 Incident Technician

Profile	Tier 2 Incident Technicians provide more in-depth technical support than Tier 1 Technicians. Tier 2 Technicians may be more experienced or knowledgeable on a particular product or service. Additionally, Tier 2 Technicians may be able to provide onsite troubleshooting and/or resolution. Tier 2 Technicians normally reside in specialized departments, such as Networks, Servers or Video, and will provide support in their respective areas of expertise.
Responsibilities	• If no Tier 2 Incident Coordinator role is identified, take ownership and provide monitoring and tracking of all Incidents • If no Tier 2 Incident Coordinator role is identified, validates, accepts and assigns Incident records • Communication with users – keeping them informed of incident progress, notifying them of impending changes, confirming Incident resolution or agreed outages, etc. • Closing all assigned and resolved Incidents • Initiate the Change Management process if an Incident requires a Change to resolve • Request interdepartmental work if required to resolve an Incident • Determine whether an Incident record requires special reporting • Understand the process, procedures, work instructions, policies, required documentation and tools • Use the process, procedures, work instructions, policies, required documentation and tools as designed • Initiate the Verify, Document and Close process

6.6 User

Profile	Any person who reports an incident or requests a change. This person may come from many of the ITSM roles to included, but not limited to: User, Service Owner, Service Provider, or Tier 1/Tier 2 Technician.
Responsibilities	• Provides the input into the Incident Management Process • Reports incidents when they occur • Uses the Service Desk, contacts a department directly, or opens a ticket directly in the ITSM Tool

	• Provides correct and complete information about the incident itself and the circumstances under which it occurred

7.0 Incident Management High Level Process Flow

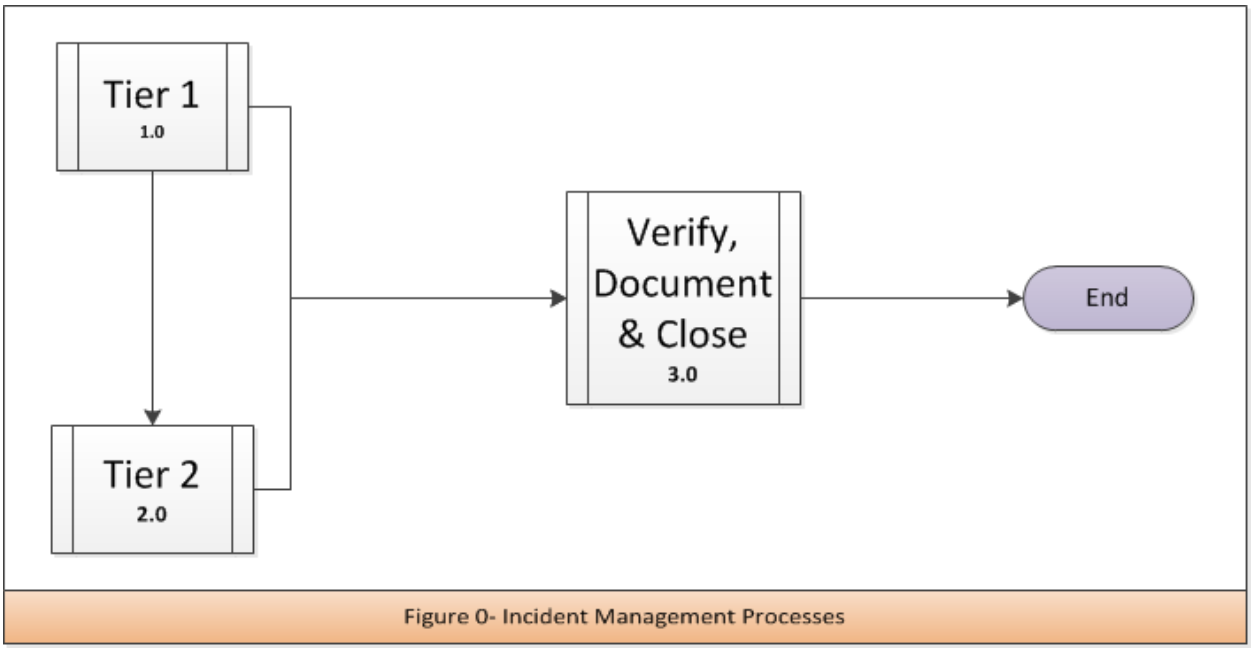

Figure 0- Incident Management Processes

7.1 Incident Management High Level Process Descriptions

Activity	Description
1.0 Incident Management Tier 1	This process describes the activities that take place to resolve incidents within Tier 1, which may be either the Support Center or a department that has been contacted directly. If Tier 2 is contacted directly, they will act on behalf of Tier 1, following the process through to Tier 2, if the record requires escalation. Interactions which are determined to be anything other than an incident are outside the scope of this process.
2.0 Incident Management Tier 2	Incidents that are unable to be resolved at Tier 1 are escalated to second level support (Tier 2).
3.0 Incident Management Verify, Document & Close (V,D & C)	This process is used by both Tier 1 and Tier 2 to ensure all incidents are verified, documented and closed consistently.

8.0 Incident Management Tier 1 Process Flow

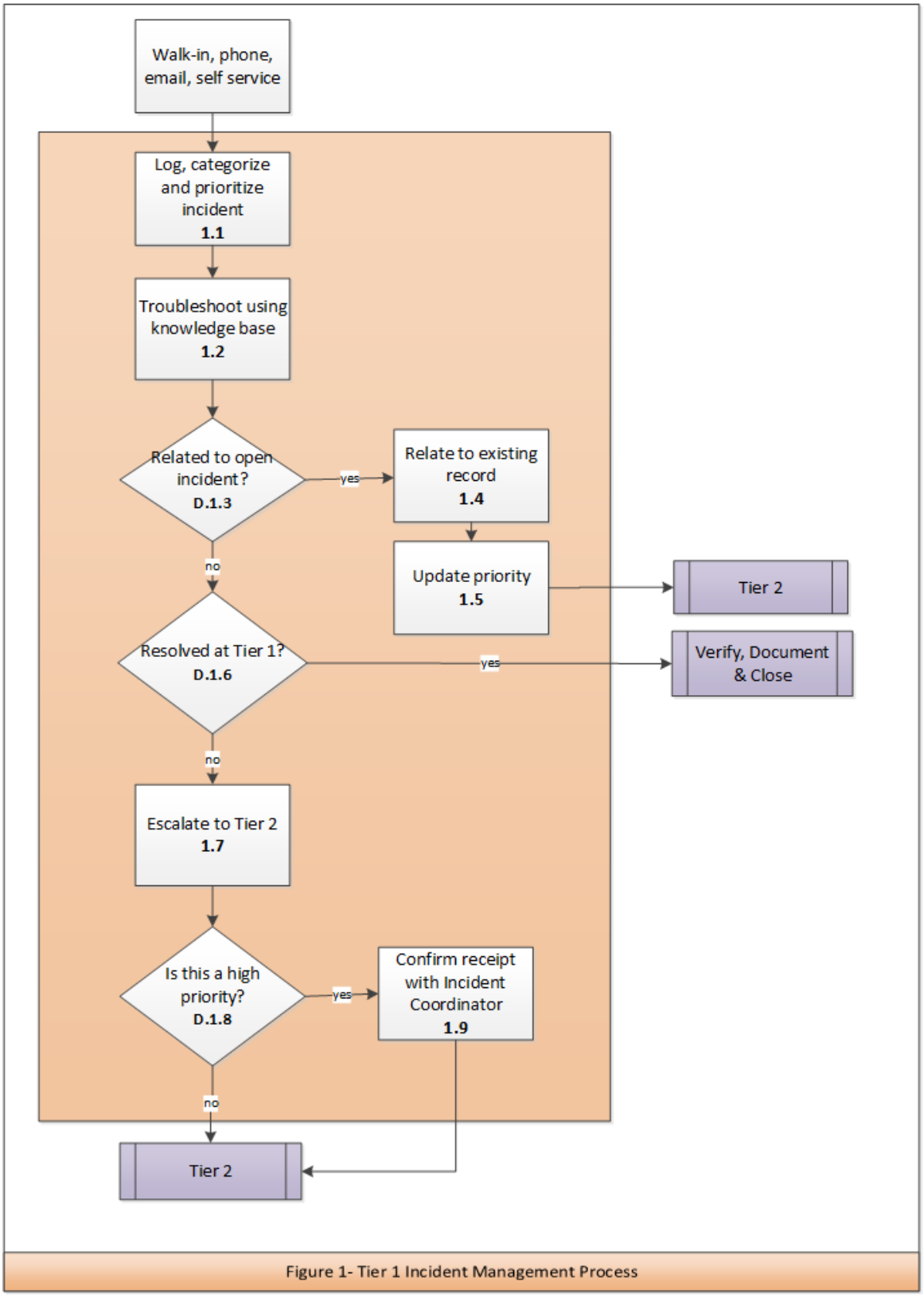

Figure 1- Tier 1 Incident Management Process

8.1 Incident Management Tier 1 Process Activity Descriptions

1.1	**Log, Categorize and Prioritize Incident**
Purpose	The incident is logged, prioritized, and categorized in the ITSM tool to enable tracking and monitoring through resolution of the incident
Requirement Statement	All incidents are tracked in the ITSM tool
Inputs	Phone, email, self service notification
Procedure or Work Instruction Steps	• Incident is logged in the ITSM tool • Include incident details • Incident is categorized based on internal agreement • Incident is prioritized based on impact and severity • Choose user notification method
Outputs	Incident record
Metric	• Total number of incidents reported • Number of incidents by category • Number of incidents by priority

1.2	**Troubleshoot Using Knowledge Base**
Purpose	Resolve incident quickly, minimizing impact to the university
Requirement Statement	To resolve incident at initial point of contact
Inputs	Incident record and available knowledge base articles
Procedure or Work Instruction Steps	• Has another user called with a similar incident? • Use available knowledge to resolve the incident • Attempt to resolve the incident collaboratively with User • Attempt to resolve incident using remote assistance • Apply resolution if applicable
Outputs	• Updated Incident record • New or updated knowledge base record
Metric	• Time to resolve incident • Incidents resolved using remote assistance • Incidents resolved using knowledge base

D.1.3	**Related to Open Incident?**
Purpose	Tier 1 combines similar service requests into one incident. The purpose of relating records is to minimize the impact to Tier 2 resources.
Decision Logic	Yes – Go to 1.4 Relate to existing record No – Go to D.1.6 Resolved at Tier 1?

1.4	**Relate to Existing Record**
Purpose	To link similar incidents together under one parent incident record. When parent incident is closed, users are notified based on notification method in step 1.1
Requirement Statement	All duplicate incidents will be relate to a parent record. Related service requests should be combined together to minimize the number of incidents being worked on.
Inputs	Incident record
Procedure or Work Instruction Steps	• Relate new incident to open incident using ITSM tool referencing ERD managed by Incident Manager ○ If relationship error is made (not related appropriately or mis-assigned) first line support will break relation and modify parent/child relationships
Outputs	Updated Incident record
Metric	• Number of related requests to one incident • Number of incidents re-opened

1.5	**Update Priority**
Purpose	Multiple reports of a similar incident may reflect a larger scope of service degradation. Incident resolution may require additional resources.
Requirement Statement	Incidents will have an assigned priority allowing appropriate resources to be directed towards resolution.
Inputs	Multiple incident records, ERD
Procedure or Work Instruction	• Update priority of parent record

Steps	○ Priority based on impact and severity ○ Incident Manager communicates with the appropriate Incident Coordinator
Outputs	Updated incident record
Metric	• Number of high priority incidents

D.1.6	**Resolved at Tier 1?**
Purpose	Determine whether escalation is needed
Decision Logic	Yes – Go to VD&C process No – Go to 1.7 Escalate to Tier 2

1.7	**Escalate to Tier 2**
Purpose	To escalate incidents to the correct Tier 2 group based on established service agreements
Requirement Statement	Resolve all incidents at the lowest level possible
Inputs	Incident record
Procedure or Work Instruction Steps	• Validate completeness of incident record per established service agreements • Reference service agreements to determine Tier 2 assignment group ○ Support Center may act as Tier 2 in support of specific services • Escalate incident
Outputs	Updated incident record
Metric	• Number of incidents escalated • Number of incidents resolved at Tier 1

D.1.8	**Is This a High Priority?**
Purpose	High priority incidents require additional coordination with Tier 2 support
Decision Logic	Yes – Go to 1.9 Confirm receipt with Incident Coordinator No – Go to Tier 2 process

1.9	**Confirm Receipt with Incident Coordinator**
Purpose	Confirm Tier 2 is aware of a high priority incident ensuring resources are allocated to resolution in a timely manner
Requirement Statement	Incidents will have an assigned priority allowing appropriate resources to be directed towards resolution.
Inputs	Incident record
Procedure or Work Instruction Steps	• Tier 1 technician confirms the Tier 2 incident coordinator (or designee) received the incident record • Tier 1 technician makes Tier 2 incident coordinator (or designee) aware of the high priority incident • Tier 1 technician passes along incident details to the Tier 2 incident coordinator (or designee)
Outputs	Updated incident record
Metric	• Number of incidents by priority

8.2 Incident Management Tier 1 Process RACI Matrix

Activity	IM Process Owner/Manager	Tier 1 Technician	Tier 2 Incident Coordinator	Tier 2 Technician	User
1.1 Log, categorize and prioritize incident	**A**	**R**			**C**
1.2 Troubleshoot using knowledge base	**A**	**R**			
D.1.1 Related to open incident?	**A**	**R**			
1.3 Relate to existing record	**A**	**R**			
1.4 Update priority	**A**	**R**	**C**		**I**
D.1.2 Resolved at Tier 1?	**A**	**R**			
1.5 Escalate to Tier 2	**A**	**R**	**I**		
D.1.3 Is this a high priority?	**A**	**R**			
1.6 Confirm receipt with incident coordinator	**A**	**R**	**C**		

Responsible
Accountable
Consulted
Informed

9.0 Incident Management Tier 2 Process Flow

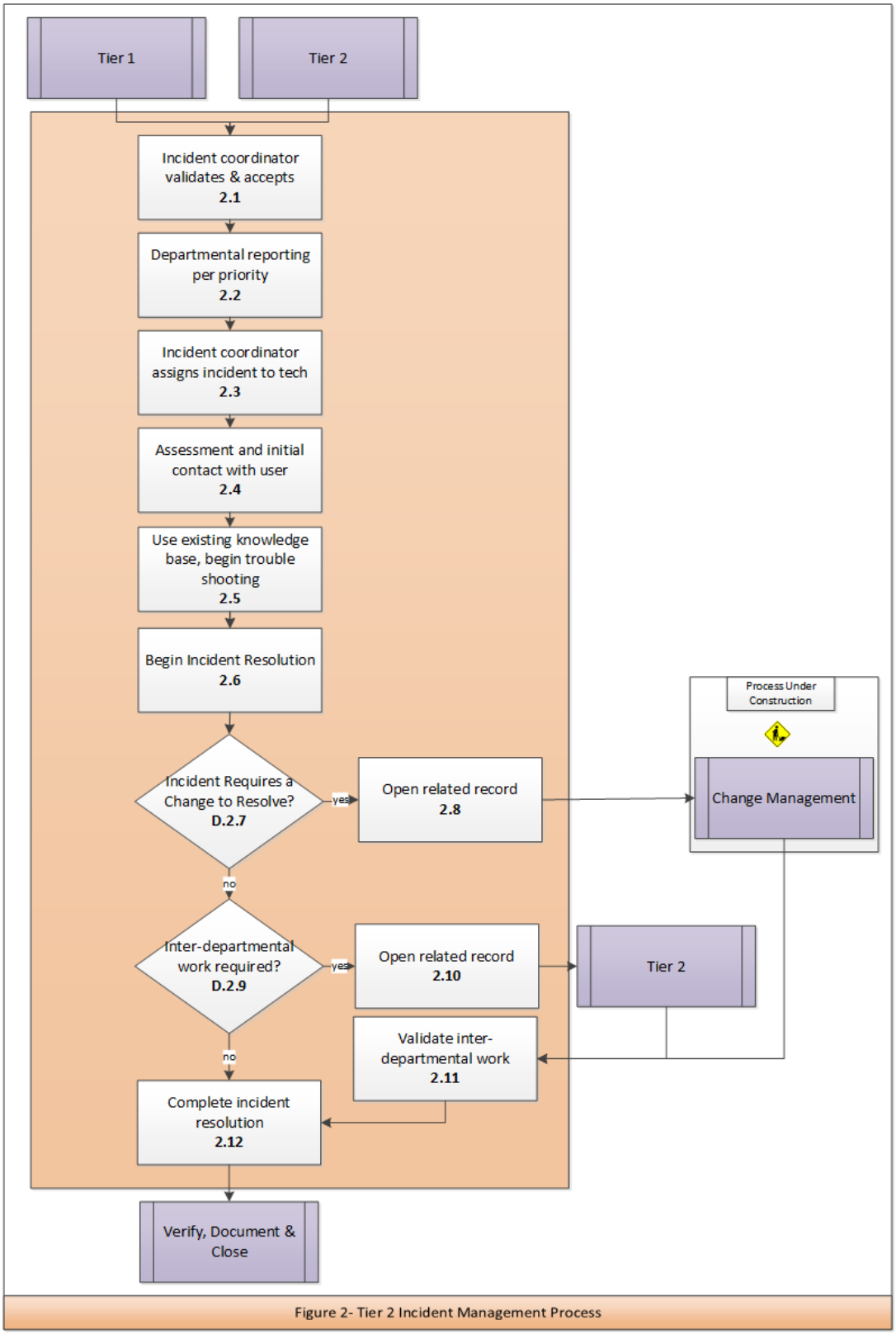

Figure 2- Tier 2 Incident Management Process

9.1 Incident Management Tier 2 Process Activity Descriptions

2.1	**Incident Coordinator Validates & Accepts**
Purpose	Verify that incident is assigned correctly, correct priority, valid incident and acknowledged by assignment team
Requirement Statement	When validating Incidents, it is the responsibility of the Incident Coordinator to determine if the ticket is assigned, prioritized and categorized correctly.
Inputs	Incident Record Related Record, Phone, Email, Alerts, Internal Service Request, Self Service
Procedure or Work Instruction Steps	• Incident Coordinator review Incident for accuracy ○ Incident Coordinator verifies assignment • Incident Coordinator acknowledges acceptance • Update Incident Record
Outputs	Updated Incident Record
Metric	• Number of records incorrectly assigned Incidents • Number of tickets by priority • Time to assignment

2.2	**Departmental Reporting Per Priority**
Purpose	Depending on Departmental requirements, reporting requirements might be different for various priorities.
Requirement Statement	If special reporting is required, it will be done according to Departmental requirement
Inputs	Incident Record
Procedure or Work Instruction Steps	• Determine whether the priority of this ticket requires special reporting • Follow procedures for special reporting
Outputs	Updated Incident Record
Metric	• Number of tickets requiring special handling

2.3	**Incident Coordinator Assigns Incident to Tech**
Purpose	The incident will be assigned to a technician to begin work
Requirement Statement	All incidents will be assigned to a technician to begin steps for resolution
Inputs	• Incident Record
Procedure or Work Instruction Steps	• Incident Coordinator assigns Incident to technician
Outputs	• Updated Incident Record

2.4	**Assessment and Initial Contact with User**
Purpose	To begin assessment of the Incident and contact the user, informing them that their request is being worked on
Requirement Statement	All incidents must be assessed to determine steps to resolution and the user of the related record will be contacted notifying them that work has begun
Inputs	Incident Record
Procedure or Work Instruction Steps	• Technician will make initial contact with the user to confirm that their Incident is being addressed and ask any preliminary questions that may be needed to troubleshoot • Technician will conduct an initial assessment of the incident
Outputs	• Updated Incident Record

2.5	**Use Existing Knowledge Base, Begin Troubleshooting**
Purpose	Use existing knowledge base, if applicable, to begin troubleshooting
Requirement Statement	OIT / Departmental knowledge bases assist technicians with troubleshooting
Inputs	Incident Record
Procedure or Work Instruction Steps	• Technician will check the knowledgebase to see if there is information available on the Incident • Technician will begin troubleshooting
Outputs	• Updated Incident Record

2.6	**Begin Incident Resolution**
Purpose	Incident Technician will take initial steps required to complete the Incident resolution
Requirement Statement	All Incidents must be resolved
Inputs	Incident Record
Procedure or Work Instruction Steps	• Incident Technician begins initial work required to resolve the incident • If resolution requires assistance from a vendor or the acquisition and/or replacement of hardware: o Set incident record status accordingly o Annotate record with case, ticket, order or RMA number o Notify user of possible delays
Outputs	• Updated Incident Record

D.2.7	**Incident Require a Change to resolve?**
Purpose	If a change is required to resolve the incident, a related Change record must be created. For additional information on OIT's Change Process, see Change Management Process Documentation.
Decision Logic	Yes – Go to 2.8 Open related record No – Go to D.2.10 Is interdepartmental work required?

2.8	Open Related Record
Purpose	To inform a department that a Change will be needed to resolve an Incident
Requirement Statement	If a Change is required to resolve an Incident, a related Change record is created to inform the department of the work they will need to complete
Inputs	Incident Record
Procedure or Work Instruction Steps	• Open a new/related Change record classified and prioritized appropriately ○ If the new/related Change record is a high priority, confirm that the necessary department received the new/related record.
Outputs	Updated Incident Record and Change Record
Metric	• Number of Incidents that require a Change to resolve

D.2.9	Is Inter-Departmental work required?
Purpose	If another department is needed to resolve an Incident, the technician must create a related record. If yes, go to 2.8. If no, go to D.2.11
Decision Logic	Yes – Go to 2.11 Open related record No – Go to 2.13 Complete Incident resolution

2.10	Open Related Record
Purpose	*Another internal OIT group is required to assist in the resolution of the parent incident. In most cases this relation will be in the form of an incident. Currently, some groups use this to escalate related (child) changes as well as related (child) incidents. As change management within OIT becomes more mature this will be used only for related incidents.* To inform another department that they will be involved in the resolution of an Incident.
Requirement Statement	If inter-departmental work is required, a related record is created to inform that department of the work they will need to complete

Inputs	Incident Record
Procedure or Work Instruction Steps	• Open a new/related Incident record classified and prioritized appropriately ○ If the new/related Incident record is a high priority, confirm that the necessary department received the new/related Incident record.
Outputs	• Updated Incident Record

2.11	**Validate Inter-departmental Work**
Purpose	After related work is completed, either as a Change, another Incident or both, tasks will be confirmed by the department that created the related record
Requirement Statement	If a department creates a related record, all tasks completed by another department must be validated
Inputs	Incident Record
Procedure or Work Instruction Steps	● Ensure all related record have been closed and are validated
Outputs	● Updated Incident Record

2.12	**Complete Incident Resolution**
Purpose	Incident Technician will take final steps required to complete the Incident resolution
Requirement Statement	All Incidents must be resolved
Inputs	Incident Record
Procedure or Work Instruction Steps	● Incident Technician completes all work required to finalize resolution
Outputs	● Updated Incident Record

9.2 Incident Management Tier 2 Process RACI Matrix

Activity	IM Process Owner/Manager	Tier 1 Technician	Tier 2 Incident Coordinator	Tier 2 Technician	User
2.1 Incident Coordinator Validates & Accepts	A		R		
2.2 Departmental Reporting Per Priority	A		R	R	
2.3 Incident Coordinator Assigns Incident to Tech	A		R	C/I	
2.4 Assessment and Initial Contact with User	A			R	C
2.5 Use Existing Knowledge base, Begin Troubleshooting	A			R	
2.6 Begin Incident Resolution	A			R	C/I
D.2.7 Incident Require a Change to Resolve?	A		C/I	R	
2.8 Open Related Record	A			R	I
2.9 Assign Appropriate Priority to the Change	A			R	
D.2.10 Is inter-departmental work required?	A		C/I	R	
2.11 Open Related Record	A			R	I
2.12 Validate related work	A			R	
2.13 Complete Incident Resolution	A		I	R	C/I

10.0 Incident Management Verify Document & Close Process Flow

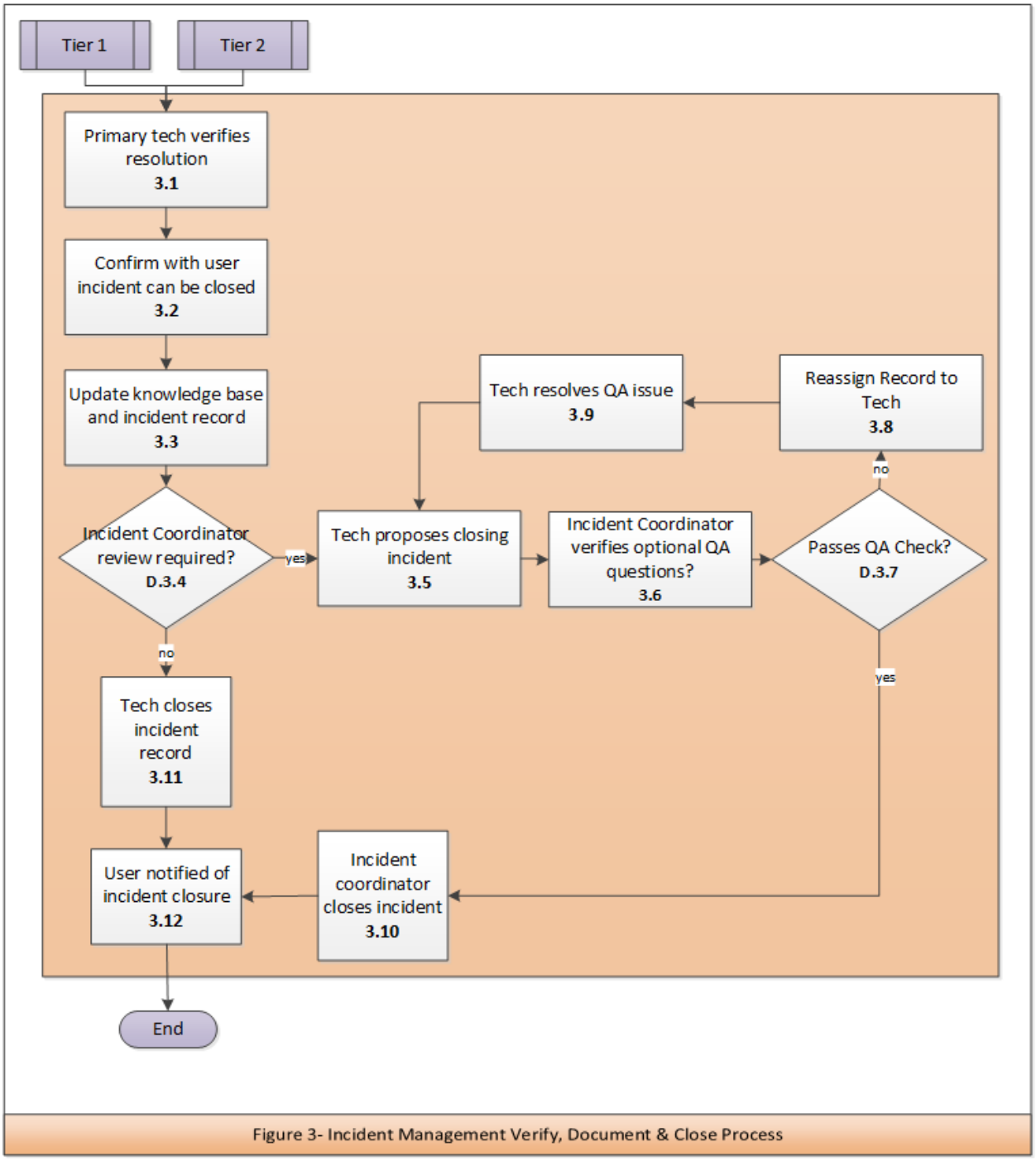

Figure 3- Incident Management Verify, Document & Close Process

10.1 Incident Management Verify, Document & Close (VD&C) Process Activity Descriptions

3.1	**Primary Tech Verifies Resolution**
Purpose	Verification of incident resolution with the user
Requirement Statement	Keeping with high standards of customer service, the tech must verify that the resolution applied fixed the issues the user was experiencing.
Inputs	Incident record (specifically the resolution)
Procedure or Work Instruction Steps	• Tech verifies fix applied resolves issue from tech's end; verification: did we apply the fix right? • Tech will contact the user • Tech confirms from user's perspective that the resolution applied fixed the issue that caused them to submit a ticket
Outputs	User verification that the resolution fixed their issue
Metric	• Length of time to resolution

3.2	**Confirm with User Incident can be Closed**
Purpose	Validation and Confirmation of incident closure with the user
Requirement Statement	Keeping with high standards of customer service, the tech must confirm that the user is comfortable with closing their ticket because their issue has been resolved.
Inputs	Conversation with the user
Procedure or Work Instruction Steps	• After contacting the user via prefered method to validate that the applied resolution worked; validation: did we apply the right fix for the user? • Confirm with the user that the incident record is able to be closed.
Outputs	User validates that it is alright to close their record. If not, the record must be routed through the Tier2 process again.
Metric	• Length of time to closure

3.3	Update Knowledge Base and Incident Record
Purpose	Update the knowledge base accessed by your department or by OIT, whichever applies.
Requirement Statement	Sharing knowledge of incidents occurring throughout campus is a helpful tool when detecting root causes. Whether a departmental knowledge base or one knowledge base for all of OIT, the knowledge base must be updated to assist others using the ITSM tool.
Inputs	Steps to resolution
Procedure or Work Instruction Steps	• Update Incident Record with actions taken for 3.1 and user responses in 3.2 as well as any other responses that apply to the resolution of the incident • Update relevant Knowledge Base
Outputs	• Updated Incident Record and Knowledge Base

D.3.4	Is Review Required by the Incident Coordinator?
Purpose	To provide a "second pair of eyes," for additional Quality Assurance at the departmental level.
Decision Logic	Yes – Go to 3.5 Tech proposes closing Incident No – Go to 3.11 Tech closes Incident record

3.5	Tech Proposes Closing Incident
Purpose	If additional Quality Assurance check is required, another technician will verify the work that was completed
Requirement Statement	The technician believes that the incident was resolved and submits the incident record to management or the Incident Coordinator for review that it meets departmental standards and adheres to procedures.
Inputs	The Incident Record
Procedure or Work Instruction Steps	• Tech changes status to "Pending Closed" ○ Answer Optional QA Questions as appropriate • Submits the incident record for review to management or Incident Coordinator

Outputs	Updated Incident Record
Metric	• Number of additional Quality Assurance reviews by department.

3.6	**Incident Coordinator Verifies Optional QA Questions**
Purpose	Provides a second opportunity to ensure that the technician completed the required steps
Requirement Statement	Some departments may deem it necessary to use additional Quality Assurance steps. If so, ensure affirmative or appropriate context is provided in the incident record.
Inputs	Incident Record
Procedure or Work Instruction Steps	• Verify the record contains acceptable outputs for activity 3.5. • Here are some examples of Quality Assurance questions: • What were the steps completed to resolve the Incident? • Did the technician test the resolution? • Did the user test the resolution? • Did the user verify that the Incident Record can be closed? • What Knowledge Base article was used?
Outputs	Updated Incident Record
Metric	• Number of Incidents that fail Quality Assurance Check

D.3.7	**Passes Quality Assurance Check?**
Purpose	It is the responsibility of the Incident Coordinator to determine whether the incident passes the Quality Assurance Check.
Decision Logic	Yes – Go to 3.10 Incident Coordinator closes Incident No – Go to 3.8 Reassign record to tech

3.8	**Reassign Record to Tech**
Purpose	Assign to Technician to resolve outstanding QA Issues
Requirement Statement	It is the responsibility of the Incident Coordinator to assign the incident to a technician to resolve all outstanding issues
Inputs	Incident Record
Procedure or Work Instruction Steps	• Incident Coordinator assigns Incident Record to technician • Incident coordinator communicates needed information to be included in the incident records or appropriate changes to bring resolution into compliance with QA
Outputs	Updated Incident Record
Metric	• Number of Incidents Failing Quality Assurance Check

3.9	**Tech Resolves Quality Assurance Issue**
Purpose	Technician to resolve outstanding Quality Assurance Issues
Requirement Statement	In order to pass a Quality Assurance check, the technician ensures that all standard operating procedures have been met
Inputs	Incident Record
Procedure or Work Instruction Steps	• Technician resolves all outstanding QA issues • Resubmit record to Incident Coordinator, step 3.5
Outputs	• Updated Incident Record

3.10	**Incident Coordinator Closes Incident**
Purpose	Incident passed the Quality Assurance check enabling the Incident Coordinator to close the record
Requirement Statement	All Incident Records will be closed upon completion
Inputs	Incident Record
Procedure or Work Instruction Steps	• Incident Coordinator changes the status of the record to closed • Include Quality Assurance questions and answers in resolution
Outputs	• Closed Incident Record

3.11	Tech Closes Incident Record
Purpose	If no Quality Assurance check was needed, the technician closes the incident record
Requirement Statement	All Incident Records will be closed upon completion
Inputs	Incident Record
Procedure or Work Instruction Steps	• Technician changes the status of the record to closed
Outputs	• Closed Incident Record

3.12	User Notified of Incident Closure
Purpose	The user must be notified that their Incident has been closed in the ITSM tool
Requirement Statement	All users must be notified when their Incident Record has been closed in the ITSM tool
Inputs	Closed Incident Record
Procedure or Work Instruction Steps	• User is notified based upon their notification preference o If preference is email then automated email generated from the ITSM tool is sufficient o If preference is telephone, the Support Center is notified and will follow up with the User via telephone
Outputs	• User Notification of closure

10.2 Incident Management VD&C Process RACI Matrix

Activity	IM Process Owner/Manager	Tier 1 Technician	Tier 2 Incident Coordinator	Tier 2 Technician	User
3.1 Primary Tech Verifies Resolution	**A**	**R**		**R**	**C**
3.2 Confirm with User Incident can be Closed	**A**	**R**		**R**	**C**
3.3 Update Knowledge base and Incident Record	**A**	**R**	**C**	**R**	
D.3.4 Is Additional Incident Coordinator Review Required?	**A**	**R**	**R**	**R**	
3.5 Technician Proposes Closing Incident	**A**	**R**		**R**	
3.6 Incident Coordinator Verifies Optional QA Questions	**A**	**C**	**R**	**C**	
D.3.7 Passes QA Check?	**A**		**R**		
3.8 Reassign Record to Technician	**A**	**I**	**R**	**I**	
3.9 Tech Resolves QA Issue	**A**	**R**	**C**	**R**	**C**
3.10 Incident Coordinator Closes Incident	**A**		**R**		
3.11 Technician Closes Incident Record	**A**	**R**		**R**	