Incident Management Procedures

November 22, 2013
Version 1.4

Table of Contents

Document Control

Summary of Changes

Version	Version Date	Nature of Change	Edited By
1.0	2009-October-15	Initial Document	
1.0.1	2009-October-20	Edited for Formatting	Matt Gruhn
1.0.2	2009-October-21	Edited ARCI Definitions	Aaron Mansfield
1.1			Don Strickland
1.1.1	2009-December-08		Michael Satut
1.2	2009-December-10	Edited Don's suggestions; edited for formatting	Lynne Jeffers
1.2.1	2009-December-17	Edited for formatting	Matt Gruhn
1.2.2	2009-December-17	Edited definitions	Aaron Mansfield
1.2.3	2009-December-22	Edited for formatting	Lynne Jeffers
1.3	2009-December-23	Updated process flows and work instructions	Matt Gruhn
1.3.1	2009-December-30	Updated and formatted communication timelines	Matt Gruhn
1.3.2	2010-November-09	Updated formatting	Aaron Mansfield
1.4	2011-March-28	Edited priority matrix	Aaron Mansfield
1.4.1	2011-May-06	Updated priority 1 and 2 resolution goals and associated content	Aaron Mansfield
1.4.2	2011-June-24	Updated timing related to Major Incident Management	Aaron Mansfield
1.4.3	2011-August-04	Updated P2 Communication Guidelines	Aaron Mansfield
1.4.4	2013-November-22	Updated priority 1 to include problem ticket information	Aaron Mansfield

Document Change-Approver

Title	Name	E-mail
TSS Associate Director (Document Owner)	Aaron Mansfield	aaron@northwestern.edu
Senior Technical Services Specialist	Michael Jones	michael@northwestern.edu

Document Approvals

The document owner is responsible for the accuracy and integrity of this document.

Document changes are made through the change management process. To initiate a change to this document, e-mail the document owner.

Proposed changes will be reviewed by the document change-approvers listed above.

After approval from those listed above, the updated document will be presented to the Change Advisory Board (CAB) for final approval.

Document Review Plans

This document is reviewed and updated as defined below:

- As required to correct or enhance information content
- Following an annual review

How to Find the Latest Version of this Document

The latest and official version of this document may be obtained on the process documentation page of the NUIT wiki at

http://wiki.it.northwestern.edu/wiki/index.php/Process_Documentation

Printed copies are for reference only and are not controlled. It is the responsibility of users of this document to ensure that they are using the most recent version.

Overview

The incident management process includes the coordination of service recovery, notification, escalation, and event review for all services as defined in the Northwestern University Information Technology (NUIT) Service Catalog. This document is intended to provide high-level overview of the incident management workflow.

This document is to be used as reference for all NUIT staff to clearly understand the standards and procedures put in place to manage an incident through service restoration and incident review.

Description and Scope

This document describes the process to be followed for assessing an incident and determining the level of priority based on definitions of impact and urgency. Once priority is determined, the appropriate route for managing the incident resolution process is followed.

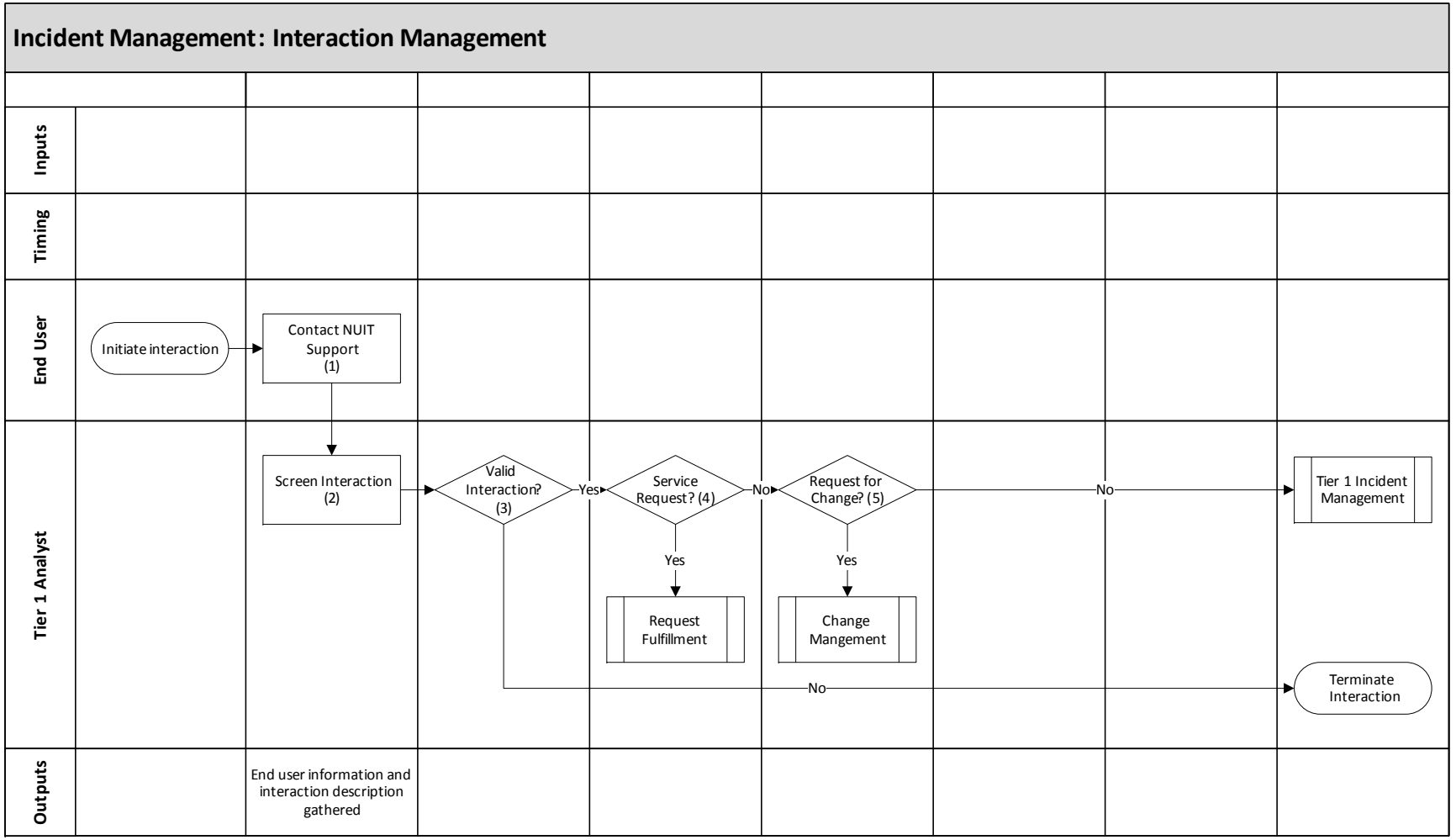
Objectives and Performance Metrics

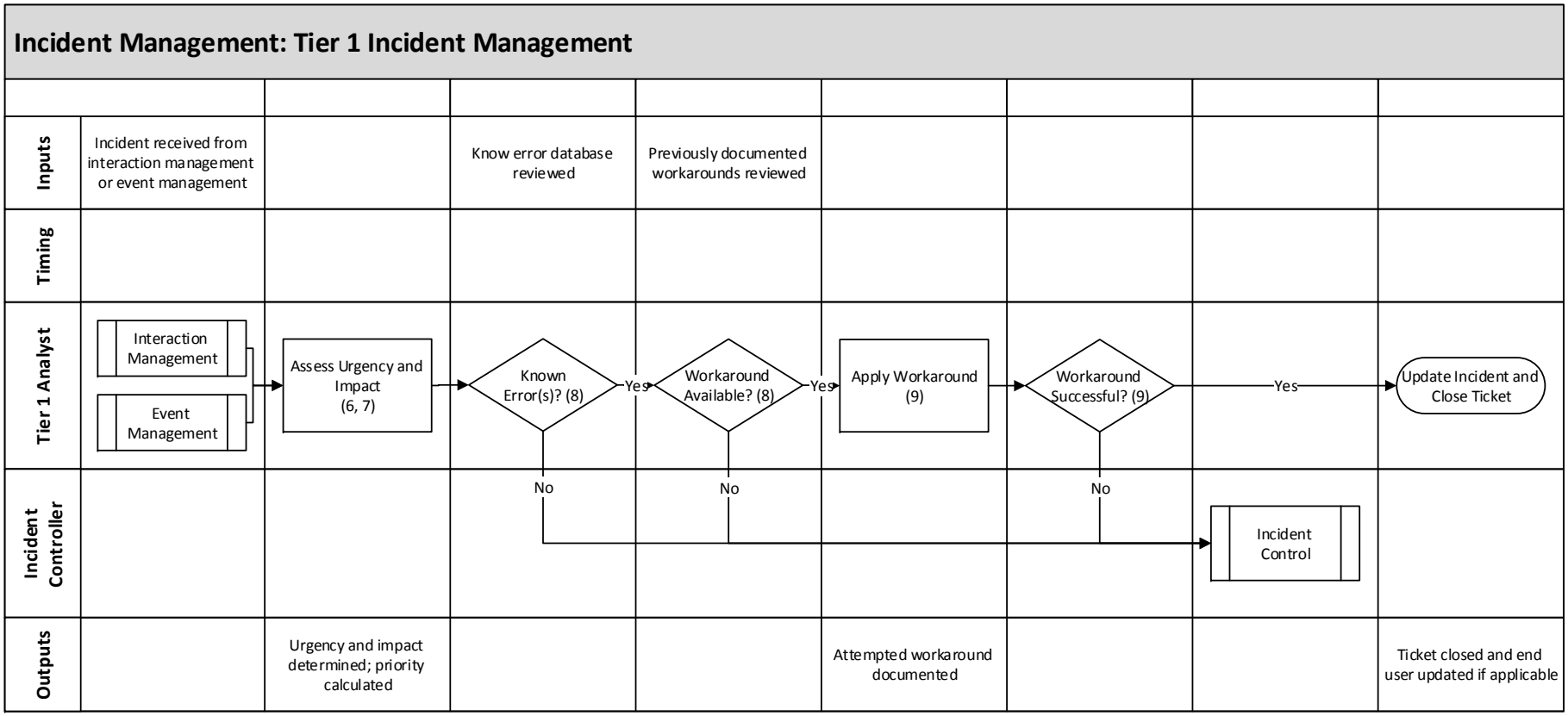
All processes must be measured to ensure compliance, effectiveness, and efficiency and to serve as a baseline for improvement.

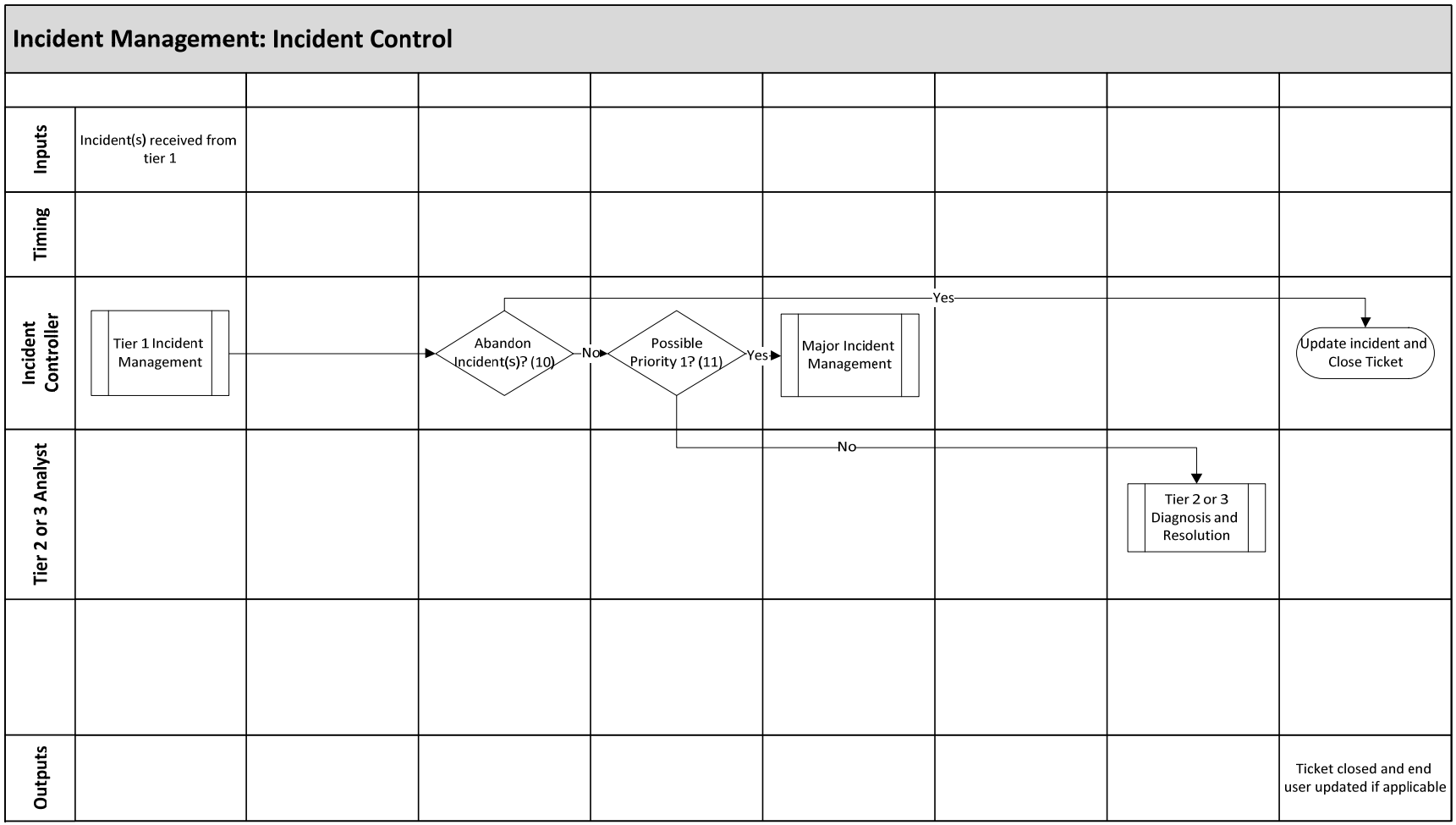
The objectives and associated metrics of the incident management process are as follows:

- Ensure timely incident resolution
    - Measured by mean time to repair (MTTR) statistics, including performance against associated targets
- Maximize service availability
    - Measured by incident handle time, broken down by support tier
    - Number of major incidents
- Effectively manage customer communications and notification
    - Measured by the number of updates and customer communications distributed via the following channels:
        - ACD emergency messages
        - Emergency bulk-mail messages
        - End user feedback
        - Service status web pages
- Improve communication between groups
    - Measured by status updates in the service manager tool, including performance against SLA or OLA requirements
- Accurately assign incidents
    - Measured by the percent of reassignments by the incident controller

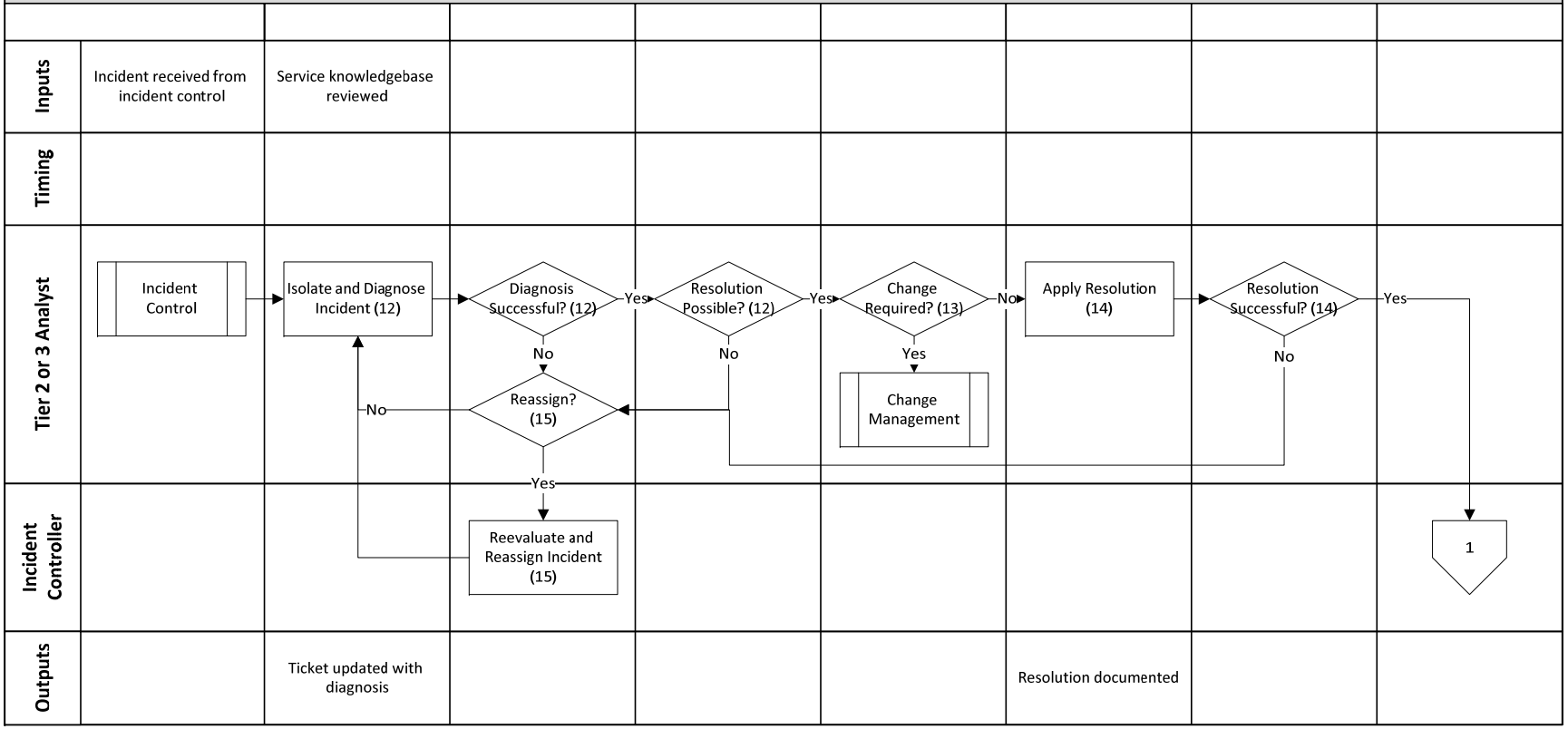
Incident Management Process Flows



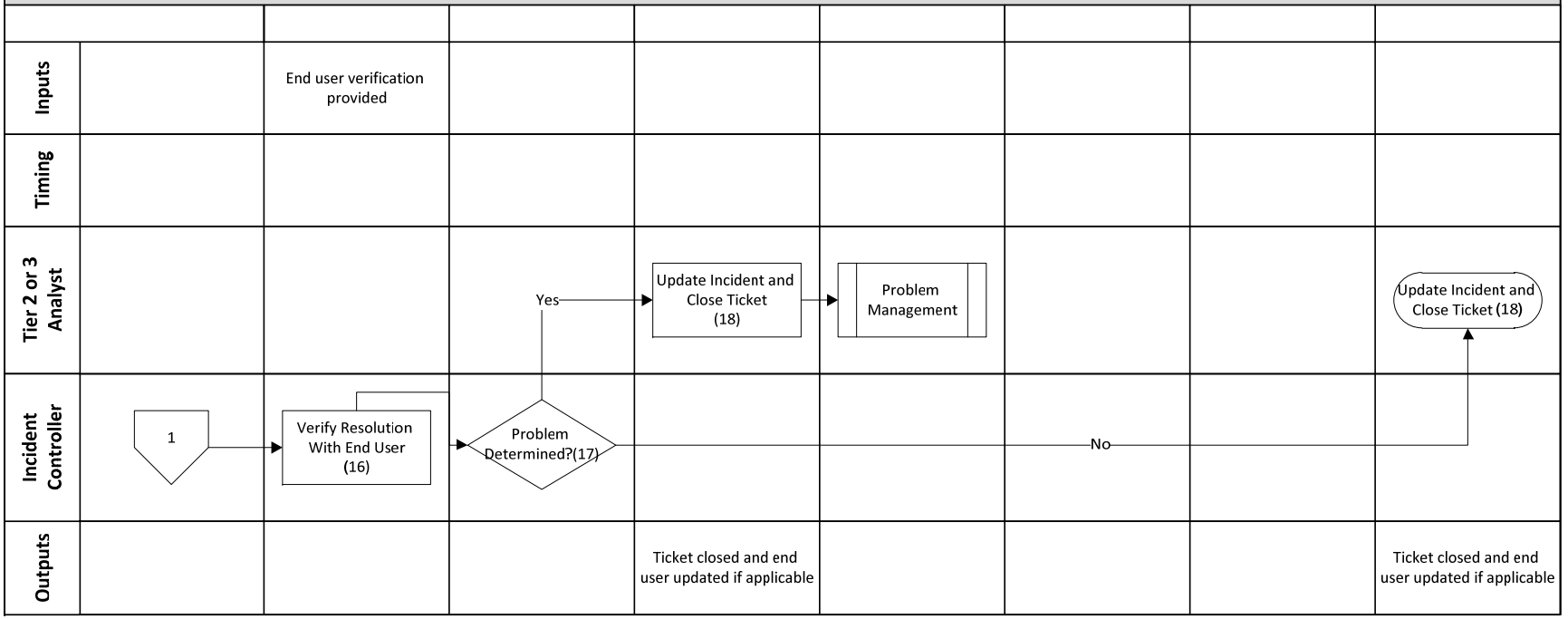

Incident Management: Tier 1 Incident Management
Inputs
Timing
Tier 1 Analyst
Incident Controller
Outputs
Incident received from interaction management or event management
Know error database reviewed
Previously documented workarounds reviewed
Interaction Management
Event Management
Assess Urgency and Impact (6, 7)
Known Error(s)? (8)
Yes
Workaround Available? (8)
Yes
Apply Workaround (9)
Workaround Successful? (9)
Yes
Update Incident and Close Ticket
No
No
No
Incident Control
Urgency and impact determined; priority calculated
Attempted workaround documented
Ticket closed and end user updated if applicable


Incident Management: Incident Control
Inputs
Incident(s) received from tier 1
Timing
Incident Controller
Tier 1 Incident Management
Abandon Incident(s)? (10)
No
Possible Priority 1? (11)
Yes
Major Incident Management
Yes
Update incident and Close Ticket
Tier 2 or 3 Analyst
No
Tier 2 or 3 Diagnosis and Resolution
Outputs
Ticket closed and end user updated if applicable

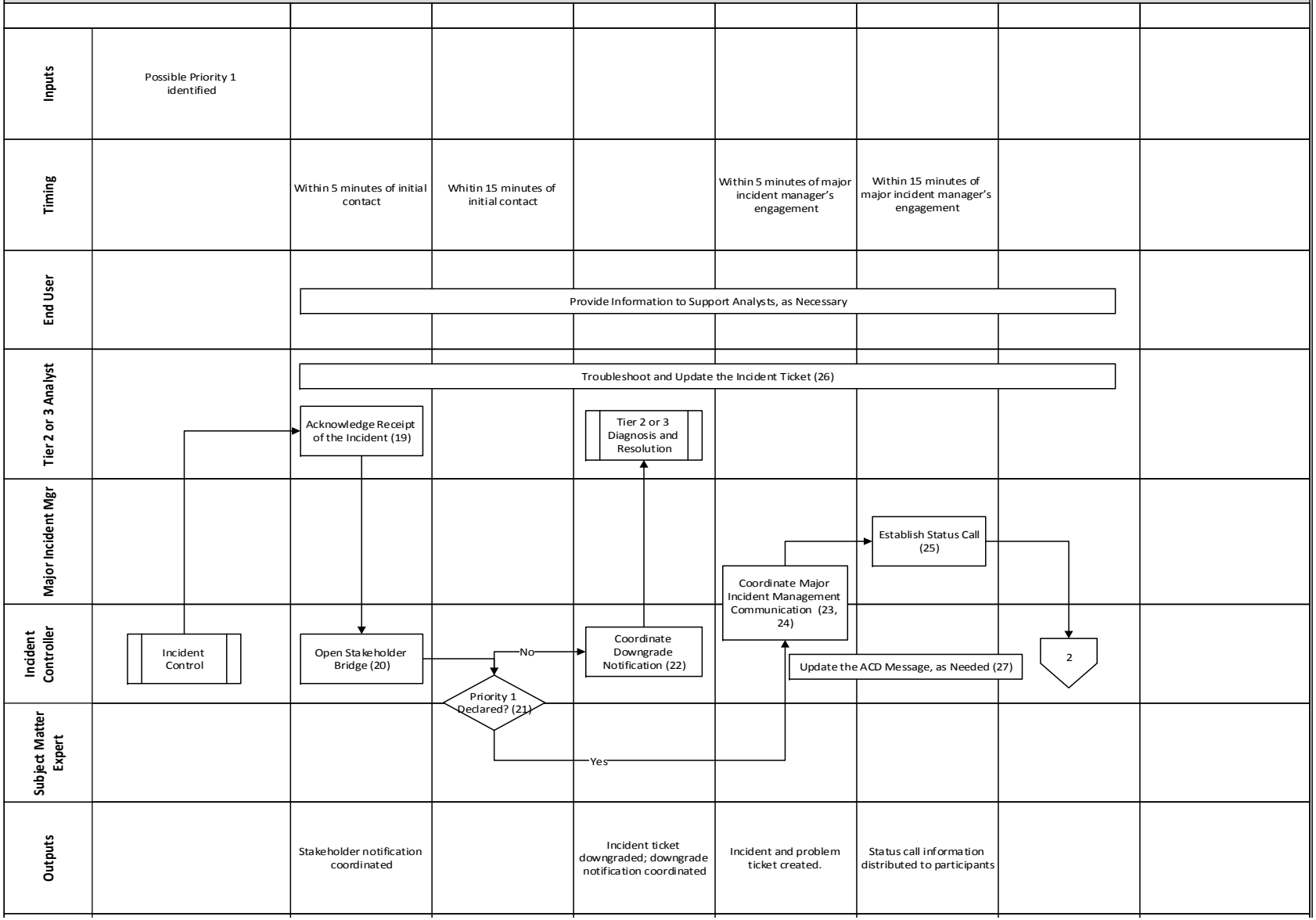
Incident Management: Tier 2 or 3 Diagnosis and Resolution 1



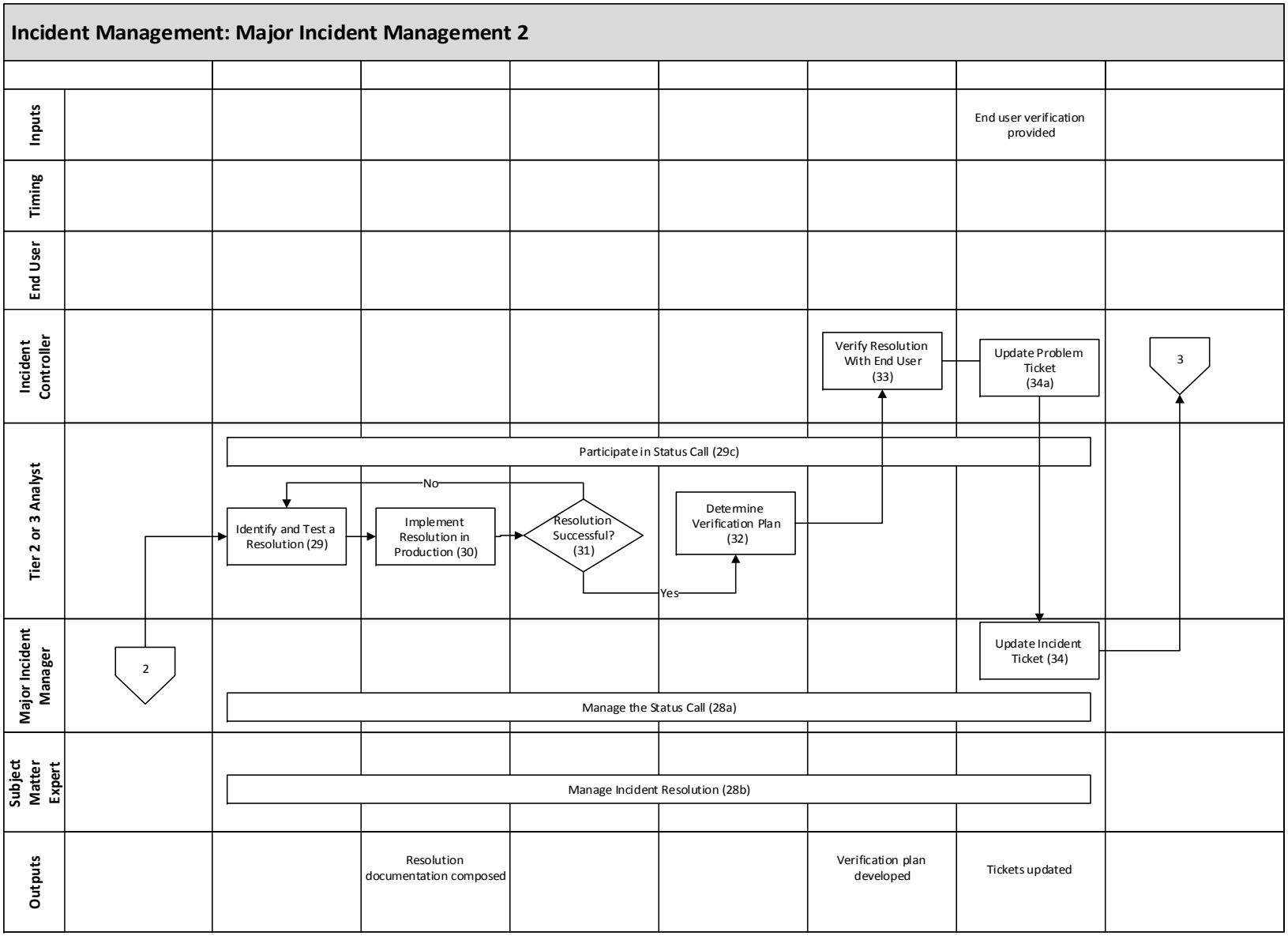
Incident Management: Tier 2 or 3 Diagnosis and Resolution 2

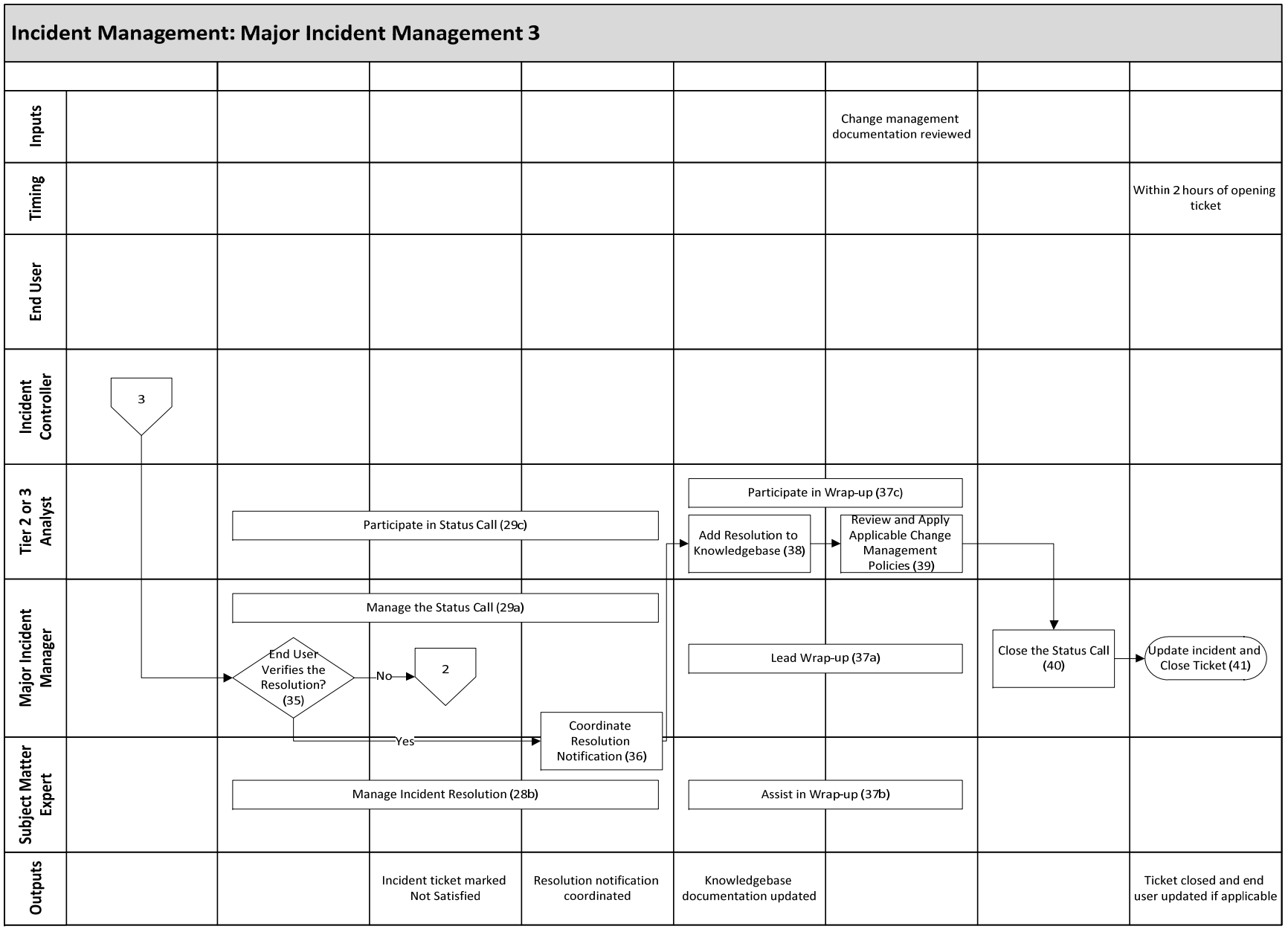


Incident Management: Major Incident Management 1



Incident Management: Major Incident Management 2




Incident Management: Major Incident Management 3
Inputs
Timing
End User
Incident Controller
Tier 2 or 3 Analyst
Major Incident Manager
Subject Matter Expert
Outputs
Change management documentation reviewed
Within 2 hours of opening ticket
3
Participate in Status Call (29c)
Participate in Wrap-up (37c)
Add Resolution to Knowledgebase (38)
Review and Apply Applicable Change Management Policies (39)
Manage the Status Call (29a)
End User Verifies the Resolution? (35)
No
2
Yes
Coordinate Resolution Notification (36)
Lead Wrap-up (37a)
Close the Status Call (40)
Update incident and Close Ticket (41)
Manage Incident Resolution (28b)
Assist in Wrap-up (37b)
Incident ticket marked Not Satisfied
Resolution notification coordinated
Knowledgebase documentation updated
Ticket closed and end user updated if applicable

Work Instructions

Step	Description	Owner	ARCI	
1	End user calls, e-mails, chats or self-service reports an incident to the service desk.	End User	**A**	End User
			R	End User
			C	Tier 1 Analyst
			I	
2	Gather end user information and interaction description. Verify that end user and service recipient information is available. If not, add relevant content.	Tier 1 Analyst	**A**	Tier 1 Analyst
			R	Tier 1 Analyst
			C	End User
			I	
3	Determine whether the interaction is valid. If it is not, terminate the interaction.	Tier 1 Analyst	**A**	Tier 1 Analyst
			R	Tier 1 Analyst
			C	End User
			I	
4	Determine whether the interaction is a service request. If it is, initiate request fulfillment.	Tier 1 Analyst	**A**	Tier 1 Analyst
			R	Tier 1 Analyst
			C	End User
			I	
5	Determine whether the interaction is a request for change. If it is, initiate change management.	Tier 1 Analyst	**A**	Tier 1 Analyst
			R	Tier 1 Analyst
			C	End User
			I	
6	Assess the impact of the incident using the NUIT policy as described in the definitions section at the end of this document: • Campus Wide Impact • Departmental Impact • Office Impact • Single User Impact Note: Automated tickets opened by monitoring tools default to priority 3. The tier 1 analyst must evaluate the true impact and update the initial priority as needed.	Tier 1 Analyst	**A**	Tier 1 Analyst
			R	Tier 1 Analyst
			C	
			I	
7	Assess the urgency of the incident using the NUIT policy as described in the definitions section of this document: 1. Immediate 2. Critical 3. Elevated 4. Routine Note: Automated tickets opened by monitoring tools default to priority 3. The tier 1 analyst must evaluate the true urgency and update the initial priority as needed.	Tier 1 Analyst	**A**	Tier 1 Analyst
			R	Tier 1 Analyst
			C	
			I	
8	Determine whether the incident is a known error and whether a workaround is available. If the incident is not a known error or there is no known workaround, refer the incident to incident control.	Tier 1 Analyst	**A**	Tier 1 Analyst
			R	Tier 1 Analyst
			C	
			I	Incident Controller

Step	Description	Owner	ARCI	
9	Apply workaround if available. If the workaround fails, refer the incident to incident control. If the workaround succeeds, update and close the ticket.	Tier 1 Analyst	**A**	Tier 1 Analyst
			R	Tier 1 Analyst
			C	End User
			I	Incident Controller
10	Evaluate the incident by validating the assessment. If the incident should be abandoned, update and close the ticket.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	
			I	
11	If incident is a possible Priority 1, coordinate assessment activities. Go to step 19. For standard incidents, refer the ticket to an appropriate tier 2 or 3 team.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	Tier 2 Analyst/ Tier 3 Analyst
			I	Major Incident Manager
12	Isolate and diagnose the incident. If diagnosis fails, or if no resolution is available for the diagnosed cause, determine whether the incident should be reassigned. If not, continue to diagnose the incident. If the incident should be reassigned, refer the ticket back to the incident controller for reevaluation.	Tier 2 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	Incident Controller
13	Determine whether a change is required to resolve the incident. If so, initiate change management.	Tier 2 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	
14	Apply and verify a resolution. If the resolution was not successful, determine whether the incident should be reassigned. If not, continue to diagnose the incident. If the incident should be reassigned, refer the ticket back to the incident controller for reevaluation.	Tier 2 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	Incident Controller
15	If the initial tier 2 or 3 analyst could not diagnose or resolve the incident, reevaluate the ticket and reassign to another tier 2 or 3 group.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	
			I	Tier 2 Analyst
16	Verify the resolution with the end user.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	End User
			I	Tier 2 Analyst
17	Determine whether a problem has been generated by the incident. If so, initiate problem management.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	
			I	Tier 2 Analyst

Step	Description	Owner	ARCI	
18	Update the incident and close the ticket. Incident management is complete.	Tier 2 Analyst	**A**	Tier 2 Analyst
			R	Tier 2 Analyst
			C	
			I	End User
19	Acknowledge receipt of the incident by assigning the incident ticket to the appropriate tier 2 or 3 analyst. Note: If the assignment group recognizes the cause to be a known error with a standard resolution that can be quickly implemented, they will notify the incident controller and no status call will be scheduled. In this situation, the tier 2 or 3 analyst assumes the responsibility of coordinating update and resolution notifications with the incident controller as needed, including assisting in documenting the impact.	Incident Controller	**A**	Incident Controller
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	Major Incident Manager
			I	Incident Controller
20	Simultaneously to the tier 2 or 3 analyst receiving and working the incident, incident controller kicks off the priority 1 assessment process by coordinating the stakeholder bridge for incident assessment. To avoid confusion, the initial notification will contain minimal detail.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	Tier 2 Analyst/ Tier 3 Analyst
			I	Stakeholders
21	The Incident Controller is to work with the SME to establish consensus that the priority has been assessed correctly. The Incident Controller is required to follow the standard definitions of urgency and impact in determining the priority.	Incident Controller	**A**	SME
			R	Incident Controller
			C	Stakeholders
			I	
22	If the Incident Controller determines that the incident is not priority 1, the incident controller will work to organize a downgrade notification, and the incident will be worked via the standard incident process. If the incident is downgraded to a priority 2 or less, the incident controller will close the stakeholder bridge and coordinate community notification.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	SME
			I	Management Stakeholders
23	Engage the major incident manager, providing the incident details (including IM ticket number) and if needed assist in developing the initial notification.	Incident Controller	**A**	Incident Controller
			R	Incident Controller Major Incident Manager
			C	
			I	Management Stakeholders
24	Coordinate communication and community notification activities.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager
			C	
			I	Management Stakeholders

Step	Description	Owner	ARCI	
25	Establish a technical bridge to permit support teams to work in parallel on incident resolution.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager
			C	
			I	SME Incident Controller Tier 2 Analyst Tier 3 Analyst
26	Troubleshoot the incident, attempting to determine its root cause.	Tier 2 Analyst / Tier 3 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	
27	Update ACD (Automated Call Distribution) message as needed. If an incident can be expected to produce a high volume of calls to the service desk, the incident controller can work with the service desk to record a message to be played at the beginning of the ACD menu before the callers hears any menu options.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	
			I	End User
28a	Manage status call process: • Request additional resources to join call as identified by SME • Verify the tier 2 or tier 3 team updates incident • Escalate within Northwestern University or service partner organizations, when required, to gain additional focus and resources to permit timely resolution within service levels • Monitor who is on the call • Coordinate distribution of update notifications regularly to communicate incident status. If no status call is scheduled, monitor ticket for troubleshooting actions/progress and contact SME or tier 2 or 3 analyst for status as needed.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager
			C	
			I	

Step	Description	Owner	ARCI	
28b	Manage incident resolution: • Identify appropriate personnel to participate in status call and notify major incident manager • Coordinate update/resolution notifications with the major incident manager as needed • As appropriate add groups (or individuals) or release groups (or individuals) to/from the call. • As needed, communicate initial troubleshooting steps to additional resources as they join the bridge Note: Transferring ownership to another SME: If an incident is initially reported as impacting one service, but during troubleshooting it is determined that a different service is impacted, this may call for the original SME to transfer ownership to a different SME. Similarly, if an incident is determined to be caused by an infrastructure component and that component error impacts multiple critical services, the SME role may be transferred to the SME for that infrastructure component. To transfer ownership: 1. The original SME should request that the SME for the other service or infrastructure component join the status call. 2. The original SME should brief the other SME, explaining how they reached the conclusion that a transfer of ownership would be appropriate. 3. The other SME must then agree that transfer is appropriate and will then take ownership of the incident.	SME	**A**	SME
			R	SME
			C	
			I	Major Incident Manager
28c	Participate in status call and update ticket with troubleshooting actions and progress: • Every 60 minutes for priority 1 Note: If another team will implement the resolution, the incident ticket should be reassigned to that assignment group.	Tier 2 Analyst / Tier 3 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	Major Incident Manager
29	Identify a resolution, document the resolution, and test the resolution on a non-production environment if it makes sense, time permits, and a duplicate environment exists.	Tier 2 Analyst / Tier 3 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	SME Major Incident Manager Incident Controller
			I	

Step	Description	Owner	ARCI	
30	Implement the resolution in the production environment.	Tier 2 Analyst / Tier 3 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	SME Major Incident Manager Incident Controller
			I	
31	Determine if the resolution was successful and appears to have restored the service. If the resolution did not restore service, return to troubleshooting.	Tier 2 Analyst / Tier 3 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	Major Incident Manager
32	Work with the participants on the call to determine an appropriate verification plan. Most commonly, the incident controller will be engaged to contact the end users who reported the incident or appropriate standard business contacts. For major platform outages it may be necessary to verify that all dependent services have been restored. In such situations the major incident manager will develop a plan for verification, and the incident controller will support them by engaging the identified resources as needed.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager
			C	Incident Controller
			I	
33	Contact the end user to verify that service has been restored. Should the incident controller be unable to reach someone that can verify service has been restored they will re-join the status call and work with the participants to identify an approach to verifying.	Incident Controller	**A**	Incident Controller
			R	Incident Controller
			C	End User
			I	SME

Step	Description	Owner	ARCI	
34	If the resolution was successful and service was restored, notify the major incident manager and status call participants that service appears to have been restored. The incident ticket should be closed and the resolution steps documented in detail in the corrective actions. This will allow for all associated interactions to be closed, thus notifying affected end users. Once an after action review is complete, the ticket may be reopened to append appropriate information. Note: Incidents are not left open to monitor ongoing performance of an issue, while a root cause is being determined, or to support a permanent solution or other follow-up activities when a temporary solution has restored service. When service has been restored, the incident must be closed. Note: In the event that service is partially restored, and the impact no longer justifies a priority 1 incident, the ticket will be downgraded appropriately by the tier 2 analyst.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager
			C	Tier 2 Analyst/ Tier 3 Analyst
			I	
34a	During wrap-up activities the Tier 2 Analyst will record known errors and relevant service restoration details in the problem ticket.	Tier 2 Analyst	**A**	Tier 2 Analyst
			R	Tier 2 Analyst
			C	SME
			I	Major Incident Manager
35	If the end user does not agree that service has been restored, a reassessment of the original deficiency must take place and troubleshooting must continue.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager
			C	
			I	
36	Coordinating with the SME, notify management and stakeholders that the incident has been resolved.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager SME
			C	
			I	Management Stakeholders

Step	Description	Owner	ARCI	
37a	Lead the team on the status call through wrap-up activities that include the following: • Remind the tier 2 or 3 analyst to file any SCRs for emergency changes that were undertaken during the incident • Identify immediate follow-up actions required and assign ownership. Immediate follow-ups are intended to be only those that must occur prior to the end of the next business day. Other follow-up actions may be determined and tracked by problem management process.	Major Incident Manager	**A**	Major Incident Manager
			R	SME Major Incident Manager Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	
37b	Assist the major incident manager in leading wrap up activities.	SME	**A**	SME
			R	SME Major Incident Manager Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	
37c	Participate in wrap-up activities.	Tier 2 Analyst / Tier 3 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	SME Major Incident Manager Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	
38	Add resolution to the knowledgebase if applicable.	Tier 2 Analyst / Tier 3 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	
			I	Incident Controller
39	After conferring on status call and implementing a solution, all applicable change management policies should be reviewed and conducted as appropriate. The change management policy allows an emergency change to be implemented before the SCR is opened. The status call participants, specifically the major incident manager, approve this change as part of the call. The SCR still is required to be processed after the incident is resolved. See the change management process documentation for more details.	Tier 2 Analyst / Tier 3 Analyst	**A**	Tier 2 Analyst/ Tier 3 Analyst
			R	Tier 2 Analyst/ Tier 3 Analyst
			C	SME Major Incident Manager
			I	

Step	Description	Owner	ARCI	
40	Close the status call line.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager
			C	
			I	
41	Close the incident ticket. Incident management is complete. If residual impact exists that no longer justifies a priority 1 impact, open a new incident ticket at the appropriate priority level for the remaining impact.	Major Incident Manager	**A**	Major Incident Manager
			R	Major Incident Manager
			C	
			I	

Roles and Responsibilities

Role	Responsibility
End User	• Report incident(s) to the service desk • Answer questions and test as needed • Confirm resolution
Tier 1 Analyst	• Verify user profile • Use knowledge base to troubleshoot the incident and to determine priority • Log and dispatch the ticket to the appropriate assignment group • Engage incident controller to validate priority

Incident Controller	• Validate priority assignment by tier 1 or 2 analyst, as needed
	• Notify assignment group that a priority 1 ticket has been assigned to them using on-call database
	• If not already done by tier 1 analyst:
	  • Engage the major incident manager
	  • Provide the major incident manager with sufficient detail to develop initial high-level notification
	• Assist the major incident manager, as needed, throughout incident
	• Upon request from the major incident manager, contact the end user to confirm a resolution

Role	Responsibility
Tier 2 Analyst	• For incidents identified through automated alerts, perform initial evaluation to determine an incident is a priority 1 • Notify the major incident manager and incident controller of a new priority 1 incident when appropriate • Acknowledge assignment of incident within 15 minutes of notification • Troubleshoot and fix the incident • Participate in the technical bridge • Provide timely updates to the incident ticket (every 60 minutes for priority 1). All actions taken during troubleshooting and resolution should be documented in the incident ticket in service manager • After conferring with technical bridge, implement approved resolution following all applicable change management policies • Resolve the ticket and document the resolution: Provide a detailed technical description of the resolution in the Action/Resolution tab, which will be posted to the journal. Provide a clear description of the resolution in laymen's terms on the Closure tab. • If no status call is opened, it becomes the responsibility of the tier 2 or 3 analyst to coordinate update and resolution notifications with the major incident manager as needed, including assisting in documenting impact
Tier 3 Analyst	• Acknowledge assignment of incident within 15 minutes of notification • Troubleshoot and resolve the incident • Participate in technical bridge • Provide timely updates to the incident ticket (every 60 minutes for priority 1). All actions taken during troubleshooting and resolution should be documented in the incident ticket in service manager • After conferring with technical bridge, implement resolution following all applicable change management policies • Resolve the ticket and document the resolution. Provide a detailed technical description of the resolution in the Action/Resolution tab, which will be posted to the journal. Provide a clear description of the resolution in laymen's terms on the Closure tab. • If no status call is opened, it becomes the responsibility of the tier 2 or 3 analyst to coordinate update and resolution notifications with the major incident manager as needed, including assisting in documenting impact

Role	Responsibility
Major Incident Manager	• Manage process for all priority 1 technical issues • Final escalation point for initial evaluation of incident priority • Establish a status call line to permit support teams (service partners and NUIT support teams, if required) to work in parallel on incident detection and resolution • Monitor who is on the call • Restrict participation on the status call line to personnel who are critical to restoring service • Maintain a log of events • Coordinate the sending of messages regularly to NUIT management teams, as well as stakeholders, to communicate incident status • Escalate within service partner organizations or Northwestern, when required, to gain additional focus and resources to permit timely resolution within service levels • Contact appropriate personnel as identified by SME • Coordinate with SME to ensure proper documentation of incident and that immediate follow-up actions are identified • Engage the SME's manager
Subject Matter Expert (SME)	• Manage resolution of incident • Identify appropriate personnel to participate in bridge and notify major incident manager • Coordinate update/resolution notifications with the major incident manager as needed • Determine need for management status calls and participate on calls as needed • As appropriate add groups (or individuals) or release groups (or individuals) to/from the call • As needed, provide recap of troubleshooting steps already taken • Coordinate with major incident manager to ensure proper documentation of incident and follow-up actions identified

Business Continuity Controller	• For priority 1 incidents that impact business continuity:
	  • Lead management status calls
	  • Ensure any additional communication needed for NUIT leadership occurs

Priority Classification

Overview

At the highest level, the priority of an incident is determined based on the impact to the University and the urgency of restoration. The descriptions provided in this document are intended to provide very subjective guidelines for assessing the priority of incidents. The goal of these definitions is that every individual in Northwestern's information technology environment interprets each standard in the same manner so that as much subjectivity as possible is removed. In this way, we can ensure that a priority 1 ticket means the same thing to everyone at all levels and in all departments. Standardizing these definitions ensures the most efficient use of resources and fairness across the entire support spectrum.

End User Knowledge of Priority

End users should not request an upgrade or downgrade in priority; they should simply provide the most accurate impact and urgency information to the analyst, who, using the definitions provided, assigns the impact and urgency to the interaction. End users should not be told the priority of tickets since they may not understand the priority determinations. Furthermore, promoting a ticket based upon an end user's 'emotion' negatively impacts those resources which might otherwise be needed elsewhere.
Standardizing definitions and making them as objective as possible represents the most equitable distribution of resources and promotes a level of fairness for end user regardless of a end user's status or emotion. If an end user is unhappy about the timeliness of an issue, the requested resolution date can be altered without affecting the impact, urgency, or priority.

Assessment Process

- For incidents initiated via calls to the service desk: The tier 1 analyst will assess the impact and urgency using the definitions below. The service manager tool will then calculate the priority using the matrix documented below.
- For incidents auto-generated from monitoring tools, the ticket will be opened with a default priority 3. The tier 2 analyst is responsible for re-assessing the impact and urgency and updating the ticket accordingly.

End User Escalation Processes

A ticket can only be escalated or downgraded if the current assessment, based upon the impact and urgency definitions, is no longer accurate.

Changing Priority (Impact and Urgency)

- It is understood that over time the impact and/or urgency of an incident may change, which would in turn change its priority.
- Only select individuals may authorize changes in impact and urgency within the system. Only representatives from the service operations center (SOC) and service desk may upgrade an incident to a P1.
- The practice of downgrading an incident for the purpose of monitoring an issue after service has been restored is prohibited by policy. Once service is restored, whether via temporary or permanent solution, the incident must be closed.
- An incident may not be upgraded to bypass the change management process.

Urgency

Urgency is an indication of how long the resolution of the incident can be delayed

- Speed needed to resolve incident
- Extent the business can bear delay in resolution or completion

Urgency is defined according to the following rubric:

Urgency Value	Definition
1: Immediate (Service Restoration Target = four hours)	• End users are unable to complete their work, and • There is no viable workaround, and • Service restoration must be completed immediately or significant loss of revenue, reputation, or productivity will occur, and

	• The event threatens Northwestern's ability to meet operational goals or • The safety of Northwestern students, staff, faculty or capital equipment is threatened	
2: Critical (Service Restoration Target = eight hours)	• End users are unable to complete their work, and • There is no viable workaround, and • Service restoration must be completed within one business day or there is potential for significant loss of revenue, reputation, or productivity or • Service Restoration in excess of one business day will have a direct impact on Northwestern's ability to meet operational goals	
3: Elevated (Service Restoration Target = two business days)	• End users are able to complete their work using a workaround or • End users are unable to complete their work using a workaround. However, service restoration can be delayed by up to two business days without significant loss of productivity or operational goals	

Impact

Impact is the effect on the business due to the loss of the service. Impact is assessed as follows:

Impact Value	Definition
1: University / Campus / School	• Service interruption potentially affects one or multiple University campuses, or • All users of the service specified are affected regardless of location, or • All users of an entire school are affected
2: Building / Department	• Localized service interruption affecting a specific but entire department of users, or • All users affected by the service interruption are confined to a building or geographical location
3: Multiple Users	• Service interruption affects users across departments or geographical locations, but does not affect everyone in those locations
4: Single User	• Service interruption affects only one person

Priority

Once impact and urgency are assessed, priority is calculated according to the following table:

		Impact			
		1 University / Campus / School	**2 Building / Department**	**3 Multiple Users**	**4 Single User**
Urgency	**1: Immediate**	1	1	2	3
	2: Critical	2	2	2	3
	3: Elevated	3	3	3	4
	4: Routine	4	4	4	4

The calculated priority of the incident is used to determine the order incidents should be worked in. Higher priority incidents should take precedence over ones with lower priority. Regardless of priority, the restoration goal for any incident should be to meet the service restoration target determined by the incident's urgency.

Communication Timelines

The priority determines the expected communication timeline for an incident.

Priority 1 Incidents (Service Restoration Target is four hours)

Within five minutes of initial assignment from tier 1

- The incident controller initiates contact to tier 2 or 3 assignment group
- The service desk or incident controller notifies the major incident manager

Within five minutes of the major incident manager's engagement

- The major incident manager initiates contact to the SME and establishes a status call

Within 10 minutes of attempted contact

- The tier 2 or 3 assignment group acknowledges contact, either by calling the incident controller or joining the status call
    - ➢ If not acknowledged, the incident controller escalates to next contact or next level
- The SME acknowledges contact by calling the major incident manager or joining the status call
    - ➢ If not acknowledged, the major incident manager escalates to an alternate SME or next level

Within 15 minutes of the major incident manager's engagement

- The major incident manager coordinates the distribution of an initial management and stakeholder notification

Every 60 minutes (minimum)

- The tier 2 or 3 team updates incident ticket
- The major incident manager coordinates the distribution of updated management and stakeholder notifications

Priority 2 Incidents (Service Restoration Target is eight hours)

Within 15 minutes of initial contact from tier 1

- The tier 2 or 3 assignment group acknowledges contact
    - ➢ If not acknowledged, the incident controller escalates to next contact or next level

Within 30 minutes of initial assignment from tier 1

- The tier 2 or 3 team coordinates the distribution of a NWU Comp Announce posting and a targeted communication to impacted service area (as appropriate)

Within one hour of attempted contact

- The tier 2 or 3 team updates incident ticket with relevant status

Every two hours (minimum)

- The tier 2 or 3 team updates incident ticket relevant status and coordinates the distribution of NWU Comp Announce posting and a targeted communication to impacted service area (as appropriate)

Priority 3 Incidents (Service Restoration Target is two business days)

Within one hour of initial assignment from tier 1

- The incident controller initiates contact to tier 2 or 3 assignment group

Within four hours of attempted contact

- The tier 2 or 3 assignment group acknowledges contact
    - ➢ If not acknowledged, the incident controller escalates to next contact or next level

Every business day (minimum)

- The tier 2 or 3 team updates incident ticket

Priority 4 Incidents (Service Restoration Target is five business days)

Within one hour of initial assignment from tier 1

- The incident controller initiates contact to tier 2 or 3 assignment group

Within one business day of attempted contact

- The tier 2 or 3 assignment group acknowledges contact
    - ➢ If not acknowledged, the incident controller escalates to next contact or next level

Every two business days (minimum)

- The tier 2 or 3 team updates incident ticket

Key Terms and Definitions

Term	Definition

ARCI	A Roles and Responsibilities matrix used to define who is: **A**ccountable: t*he buck stops here* - only one **A** can be assigned to a task **R**esponsible: *the doer* – there can be more than one **R** across a task **C**onsulted: prior to making a decision or taking an action **I**nformed: after decision is made
Business Partner	A University advisory group or committee that assists in determining business requirements, obtaining funding, and providing strategic guidance to NUIT.
Change Advisory Board (CAB)	A team whose goal is to provide cross-functional visibility to all standard change requests (SCRs), to assist the change management team in the assessment and prioritization of SCRs, and to ultimately approve or deny SCRs.
Change Management	The process used to ensure that any modifications to the NUIT environment are performed in a controlled and approved manner.
End User	A user of NUIT systems, including, but not limited to, students, staff, and faculty.
Impact	The effect on the business due to the loss of the service. Levels of impact are defined as follows: 1. University, Campus, or School 2. Building(s) or Department(s) 3. Multiple Users 4. Single User
Incident	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Incident Controller	A role within the service desk responsible for the overall health and control of the incident management process. This individual acts as an internal escalation point for tier 1 analysts to assist in determining impact and urgency.
Incident Management	A process whose goal 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.
Major Incident Manager	An individual accountable for the activities and resources required to resolve escalated incidents and responsible for management of the process and facilitating communication.
Mean Time to Repair (MTTR)	The mean elapsed time from the occurrence of an incident to the restoration of service. Elapsed time is defined as the time between the open time and closed time of an incident.
On-Call List	A list of support contacts for a particular service. The on-call list for NUIT resources is recorded in the IT service manager tool.
Operational Goals	The fundamental objectives of the University, primarily education and research, as enumerated by the University's mission statement.
Priority	The degree of the attention that an incident or service request should be given for handling and resolution. Priority is calculated from the impact and urgency.

Problem	A condition identified from multiple incidents, or from a single significant incident, indicative of a single error, for which the cause is unknown.
Problem Management	A process whose goal is to minimize the adverse impact of incidents and problems on the business that are caused by errors within the IT infrastructure and to prevent recurrence of incidents related to these errors. To achieve this goal, problem management seeks to find the root cause of incidents and initiate actions to improve or correct the situation.
Resolution	The restoration of service. This may be a workaround.
Service Desk (SD)	Single point of contact (SPOC) between the end user and the service. Responsible for the incident control provided by incident management.
Service Manager	A tool implemented at Northwestern to facilitate service management. The current implementation is a repository for all service desk interactions, incidents (both from callers and alerts), service desk knowledge, and (*Tentative*) on-call support contacts.
Service Partners	Third-party vendors contracted to provide ongoing service delivery for NUIT (e.g., Google, Iron Mountain).
Standard Change Request (SCR)	A document that describes the requested change and why it is important. This can originate from problem reports, system enhancements, other projects, changes in underlying systems, and senior management.
Stakeholder	All people who have an interest in an IT service. This may include end users and partners.
Subject Matter Expert (SME)	An individual with a high-level of overall knowledge of the service impacted, both in terms of general architecture and business service provided.
Tier 2/Tier 3 Analysts	The assignment groups outside the service desk participating in the incident management process
Urgency	An indication of how long the resolution of the incident can be delayed, the speed needed to resolve incident, and the extent the business can bear delay in resolution or completion.
Workaround	An alternate operating method that can be implemented temporarily to allow the affected end users to continue working. Different levels of workaround exist. A workaround that allows end users to continue working with little if any reduction in ability to perform the function (for example, a redundant server) would result in closing an incident. A workaround that allows end users to continue working, but has significant impact on the ability to perform the function might result in downgrading a priority 1 incident to priority 2.