Amherst
INFORMATION TECHNOLOGY

Major Incident Management

Enterprise IT Process Document

2022

Overview

The purpose of this procedure is to clearly define and communicate severity levels, priorities, roles, and processes to successfully implement the Amherst **Major Incident** (MI) initiative and gain a shared understanding of priorities, roles, and processes.

Contents

What is a Major Incident?

Major Incidents cause serious interruptions to business activities and must be solved with great urgency.

Major Incident Examples

SYSTEM	INCIDENT
Yardi Voyager	• Inability to close monthly invoice registers • Inability to collect rent

Roles and Responsibilities

Incident Manager: The person responsible for overseeing the resolution of the incident.

Technical Lead: A senior-level technical professional tasked with figuring out what is broken and why, deciding the best course of action, and running the tech team.

Communications Lead: Responsible for communicating with internal and external customers affected by the incident.

Customer Support Lead: The person in charge of making sure incoming tickets and phone calls about the incident get a prompt, proper response.

Social Media Lead: A social media professional, in charge of communicating about the incident on social channels.

Problem Manager: The person responsible for going beyond the incident's resolution to find the root cause and any changes that need to be made to avoid future issues.

Definitions

Incident Model

An Incident Model has pre-defined steps to deal with a particular type of Incident. This is a way to ensure that routinely occurring Incidents are handled efficiently and effectively.

Incident Prioritization Guideline

The Incident Prioritization Guideline describes the rules for assigning priorities to Incidents, including the definition of what constitutes a Major Incident. Since Incident Management escalation rules are usually based on priorities, assigning the correct priority to an Incident is essential for triggering proper escalations.

NOTE*: The Incident Prioritization Guideline requires further development.*

Incident Record

A set of data with all details of an Incident, documenting the history of the Incident from registration to closure. An Incident is defined as an unplanned interruption or reduction in the quality of an IT service.

Incident Status Information

A message containing the present status of an Incident, sent to users. Status information is typically provided to users at various points during an Incident's lifecycle.

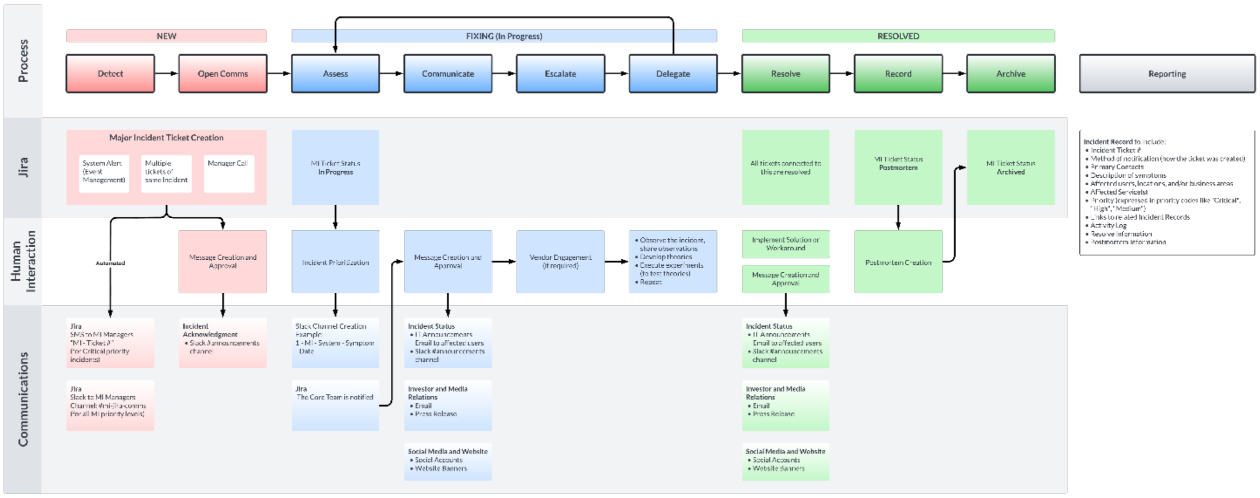
Major Incident Postmortem

A Major Incident Postmortem takes place after a Major Incident has occurred. The postmortem review documents the Incident's underlying causes (if known) and the complete resolution history. It also shows opportunities for improving the handling of future Major Incidents.

Major Incident (Core) Team

A dynamically established team of IT managers and technical experts, usually under the leadership of the Incident Manager, formulated to concentrate on the resolution of a Major Incident.

Process



Process
Jira
Human Interaction
Communications
NEW
FIXING (In Progress)
RESOLVED
Detect
Open Comms
Assess
Communicate
Escalate
Delegate
Resolve
Record
Archive
Reporting
Major Incident Ticket Creation
System Alert (Event Management)
Multiple tickets of same Incident
Manager Call
MI Ticket Status In Progress
All tickets connected to this are resolved
MI Ticket Status Postmortem
MI Ticket Status Archived
Incident Record to include:
• Incident Ticket #
• Method of notification (how the ticket was created)
• Primary Contacts
• Description of symptoms
• Affected users, locations, and/or business areas
• Affected Service(s)
• Priority (expressed in priority codes like "Critical", "High", "Medium")
• Links to related Incident Records
• Activity Log
• Resolve Information
• Postmortem Information
Automated
Message Creation and Approval
Incident Prioritization
Message Creation and Approval
Vendor Engagement (If required)
• Observe the incident, share observations
• Develop theories
• Execute experiments (to test theories)
• Repeat
Implement Solution or Workaround
Message Creation and Approval
Postmortem Creation
Jira SMS to MI Managers "MI - Ticket #" (for Critical priority incidents)
Jira Slack to MI Managers Channel: #mi-jira-comms (for all MI priority levels)
Incident Acknowledgment • Slack #announcements channel
Slack Channel Creation Example: 1 - MI - System - Symptom Date
Jira The Core Team is notified
Incident Status • IT Announcements Email to affected users • Slack #announcements channel
Investor and Media Relations • Email • Press Release
Social Media and Website • Social Accounts • Website Banners
Incident Status • IT Announcements Email to affected users • Slack #announcements channel
Investor and Media Relations • Email • Press Release
Social Media and Website • Social Accounts • Website Banners

The Major Incident Process Flowchart can be viewed **HERE**.

New

In the “New” stage of the Major Incident process, an incident is detected and reported by a person or system. Then, initial communications are sent to gather the Major Incident Team and to acknowledge the incident to affected users. Initially, the Major Incident ticket has a “New” status, in the support ticketing system.

Detect

First, an incident is detected by our technology (Events through Event Management), customer reports (Customers, Social Media), or our End-Users. When a support technician creates a Major Incident ticket (based on multiple tickets reporting the same incident) the technician will be responsible for logging the incident into our system and identifying a severity level.

Detection Methods

The methods for detecting a Major Incident include (but are not limited to):

- **System alerts** – software systems can alert the support project of pre-specified incidents
  NOTE*: This detection method is in development.*
- **Multiple tickets** – multiple tickets of the same incident, recognized by support technicians
  NOTE*: This detection method is in development.*
- **Manager call** – a technical professional, assigned to a system encountering an incident, initiates a Major Incident

Open Comms

Once an incident ticket is created, a notification goes out to the on-call professional responsible for that service.

An alert will go out, including information on the severity and priority of the incident and a summary, making it clear — immediately — whether this is the top priority or can wait if another incident is in progress.

Jira automation

Automation in the IT support project supports sending messages via SMS and Slack. In the case of a Major Incident with a Critical priority, Major Incident Managers will receive a text message detailing the summary of the incident. For all Major Incident tickets, Major Incident Managers will receive an automated Slack message in a Slack channel dedicated to organizing a response to Major Incidents (#mi-jira-comms).

Incident acknowledgment

Once we have confirmed the actual incident, communication with our customers and employees becomes a top priority. Therefore, the following should be focused on for the initial communication:

“The goal of first internal communication is to focus the incident response on one place and reduce confusion. The goal of external communication is to tell customers that you know something is broken and you are looking into it as a matter of urgency.”

Speedy, accurate communication helps build and keep customer trust.

Acknowledgment of the Major Incident will occur in the Slack #announcements channel.

Fixing (in progress)

In this stage of the Major Incident process, actions to resolve the incident are started. The Major Incident ticket will transition to “In Progress” status, in the support ticketing system.

Assess

The incident manager has been alerted, and the communication channels are open—the next step: assessing the incident itself.

We will start the process with a series of questions the team has to answer:

- What is the impact on Amherst’s customers and End-users?
- What are customers/End-users seeing?
- How many customers/End-users are affected? (Some? All?)
- When did the incident start?
- How many support cases have been opened about this incident?
- Do other factors affect the severity level or priority or change how we approach the incident? (E.g., security concerns, social media PR crises, etc.)

Once we have answered these questions, we can move forward with diagnostics and proposed fixes or change the priority level of an incident, as needed.

Incident prioritization

Some of the key characteristics that make these Major Incidents are:

- The ability of significant numbers of customers and/or key customers to use services or systems is or will be affected.
- The cost to customers and/or the service provider is or will be substantial, both in terms of direct and indirect costs (including consequential loss).
- The reputation of the Service Provider is likely to be damaged.

AND

- The amount of effort and/or time needed to manage and resolve the incident is likely to be large and agreed service levels (target resolution times) will probably be breached.

A Major Incident is also likely to be categorized as a critical or high-priority incident.

Dedicated Slack channel creation

Major Incident Managers will create a Slack channel dedicated to immediate communication with the Major Incident (Core) Team. Slack channels created for this purpose will follow strict naming guidelines.

“1-mi-system-symptom-date”

The breakdown of the Slack channel name is:

- “1” – an integer assignment of the first, second, and so on, of major incidents in progress
- “mi” – Major Incident
- “system” – the system affected (e.g., Yardi)
- “symptom” – a word referring to the symptoms of the incident
- “date” – date the incident is assessed

Core Team curation

The Major Incident Manager determines the best team members to serve as the Major Incident (Core) Team.

The Major Incident Manager uses a feature of the support project system to send standardized SMS messages to all the identified team members.

Communicate

As the details of the Major Incident are determined by the Core Team, messages will be crafted to inform the affected users of the status of the incident. Communication of the incident serves to limit the intake of new (individual) tickets about the Major Incident. Communications may also be sent to the Tier 1 and 2 service desk staff with directions about how best to handle correspondence with end-users about the incident.

Incident Status

Major Incident status messages will be sent using the following channels:

- IT Announcements email
- #Announcements (Slack channel)

VoiceEng (telephony)

As appropriate, the voice engineering (VoiceEng) staff will update prompts in the Enterprise Support phone line to notify end-users of the ongoing incident.
NOTE*: This process requires further development.*

Investor and Media Relations

As appropriate, investor and media relations messages will be created and distributed by corporate communications specialists. Methods include email and press releases.
NOTE*: This process requires further development.*

Social Media and Website

As appropriate, messages for customer-facing channels will be created by Social Media Lead(s), to be distributed via social media accounts and with banners on websites.
NOTE*: This process requires further development.*

Escalate

Incident Escalation

Sometimes, an incident is resolved quickly by the on-call team. But, in cases where that does not happen, the next step is to escalate the issue to another expert or group of experts better suited to resolving this specific incident.

Vendor Engagement

The Major Incident Manager is tasked to engage vendors, as necessary, based on pre-defined contracts.
NOTE*: This process requires further development.*

Delegate

Once the issue has been escalated to someone new, the Incident Manager delegates a role to them; these roles must be pre-set and trained upon, so team members can quickly understand what is expected of them.

Sometimes major incidents require a single incident manager and a small team. Other times, a situation may call for multiple tech leads or even multiple incident managers. The original incident manager is tasked with deciding when that is the case and bringing on the right people.

Sending follow-up Comms

As the Major Incident progresses, another round of communication outside the tech team will help keep customers and employees calm, trusting, and well-informed.

Review

Unfortunately, when it comes to incident resolution, there is no one-size-fits-all; therefore, at this stage of the process, we take the time to:

- Observe what is going on, share and confirm observations with the team
- Develop theories about why it is happening (and how we can fix it)
- Develop and execute experiments that prove or disprove our theories
- Repeat

Throughout this process, the incident manager keeps a close eye on how things are going. *Are team members overtasked? Does someone need a break? Do we need to bring in a fresh set of eyes?* More delegation happens as needed.

Resolved

When the current or imminent business impact has ended.

The emergency has passed, and the team transitions into clean-up and postmortem.

The Major Incident ticket will transition to “Resolved” status, in the support ticketing system, during the Resolved phase.

Resolve

Tickets resolved

When the Major Incident ticket is resolved, the support system will automatically resolve all the tickets listed as “*is caused by*” the Major Incident. The following information should be included in the records for the tickets associated with a Major Incident:

- Protocol
    - Person in charge (Major Incident Manager)
    - Support Group (Major Incident Team)
    - Time and Date
- Description of the Incident
- Documentation of applied Workarounds
- Documentation of the root cause of the Service interruption
- Documentation of the applied resolution to eliminate the root cause
- Date of the Incident resolution

Communicate

Incident Status (Resolution)

Major Incident resolution messages will be created, approved, and sent using the following channels:

- IT Announcements email
- #Announcements (Slack channel)

Investor and Media Relations

As appropriate, investor and media relations messages will be created and distributed by corporate communications specialists. Methods include email and press releases.
NOTE*: This process requires further development.*

Social Media and Website

As appropriate, messages for customer-facing channels will be created by Social Media Lead(s), to be distributed via social media accounts and with banners on websites.
NOTE*: This process requires further development.*

Record

Postmortem

The Major Incident ticket will transition to “Postmortem” status, in the support ticketing system.

We want to do everything we can to ensure an incident does not reoccur. The next step is a blameless postmortem designed to show the cause of an incident and help us mitigate our risk in the future.

The Major Incident Manager's report (postmortem) must include the following information:

- Adherence to agreed Service Levels
    - Agreed Service Levels

    - Attained Service Levels
        - Vendor(s) service level adherence
- Recent Major Incident Information
    - Type of event
    - Causes
    - Countermeasures for the elimination of the Incident
    - Measures for the future avoidance of similar occurrences
- Anticipated potential future Incidents (e.g., downtimes to services)
- Statistical evaluations
    - Number of Incidents
        - Over time
        - According to categories (if applicable)
    - Resolution times
- Technical analysis of the Major Incident
    - Description
    - Applied resolution strategy
        - Elimination of the root cause
        - Workaround
- Adherence to Communication expectations
    - Record of Communications to customers

Archive

The Major Incident ticket will transition to “Archived” status, in the support ticketing system, during the Archive phase.

The support ticketing system features a Dashboard dedicated to tracking the status of, and the high-level details of ongoing and archived Major Incidents. The archive of Major Incidents can also be referenced using typical Jira search methods.

Reporting

Incident Records must include:

- Incident Ticket #
- Method of notification (how the ticket was created)
- Primary Contacts
- Description of symptoms
- Affected users, locations, and/or business areas
- Affected Service(s)
- Priority (expressed in priority codes like "Critical", "High", and "Medium")
- Links to related Incident Records
- Activity Log
- Resolve Information
- Postmortem Information

Document Versions

Version	Revision Summary	Author	Date
0.1	Draft	Jeffrey Miller	9/18/2022
0.2	Refined and developed content	Jeffrey Miller, Luke Bowman	10/6/2022
0.3			