Major Incident Handbook for Services

Hotline 617-496-2831

July 2015

Questions? Contact IT Service Management at itsm@harvard.edu.
Major Incidents: Overview
Incident Priority Levels

**University digital emergency**

**Operational**

- **Crisis**
  - Major: < 0.1%
- **Critical**
  - High: ~ 5%
- **Normal**
  - ~ 95%

Unplanned service interruption or degradation that disrupts teaching, learning, research, and/or administration.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial assessment or limited impact</td>
</tr>
<tr>
<td>2</td>
<td>Known solution or working toward a solution</td>
</tr>
<tr>
<td>3</td>
<td>Significant impact with no known solution</td>
</tr>
</tbody>
</table>
See something, say something…

• If you think there may be a major incident, call the hotline.
• If in doubt, err on the side of calling; don’t wait!

Provide as much information as possible to facilitate the process:

• Incident start time
• Services or applications impacted
• Impact to users or University functions
• Teams need for troubleshooting
• Initial diagnosis or current actions, if any
Goals of Major Incident Process

• Minimize negative impact to the institution and its mission.

• Restore normal service as quickly as possible.
  – Implement workaround, if it enables a faster resolution.
  – Balance service restoration (incident management) with gathering root cause information (problem management).

• Marshal necessary staff and resources for resolution.

• Communicate appropriately and promptly.
  – Internal: HUIT, including senior leadership as required
  – External: Users and stakeholders
  – For security incidents, different protocols may be necessary.

• When possible, preserve forensics for further analysis.
Major Incident: High-Level Process and Steps

ASSESS

Declaration of MI
• Triggered by Service Desk reporting, event monitoring, and/or individual
• Preliminary information gathering regarding incident (Incident Coordinator)

Initial Coordination
• Initial assessment and categorization of MI (Service/Offering Owner)
• Convene service/offering owner and technical team on conference bridge (Incident Coordinator)
• Notify HUIT staff (Incident Coordinator) and users (Service/Offering Owner)

CONTAIN

Investigation and Diagnosis
• Marshaling of appropriate troubleshooting resources (Service/Offering Owner)
• Ongoing communication (Service/Offering Owner)
• Escalation as needed (Service/Offering Owner or Incident Coordinator)
• Vendor management as needed (Service/Offering Owner)
• Implement temporary workaround or permanent solution (Service/Offering Owner)

RESOLVE

Resolution and Closure
• Validation that all services are operational, including downstream (Service/Offering Owner)
• Gathering of all key information, e.g., end time, actions, root cause when known (Service/Offering Owner and Incident Coordinator)
• Final communication, including HUIT Alert notification of resolution (Incident Coordinator)
• Trigger problem review and After Action Review
## Major Incident Categories and Flow

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Incident Leader Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial assessment or limited impact with risk of escalation</td>
<td>Informed</td>
</tr>
<tr>
<td>2</td>
<td>Known solution or working toward a solution</td>
<td>Involved, if extended duration</td>
</tr>
<tr>
<td>3</td>
<td>Significant impact with no known solution</td>
<td>Leading</td>
</tr>
</tbody>
</table>

**Time-boxed:**
Assess category status every 30 minutes
# Key Roles in Major Incident Management

<table>
<thead>
<tr>
<th>Area of Leadership</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Leadership</strong></td>
<td><strong>Incident Leader</strong> (Member of SLT; typically MD of affected service)</td>
</tr>
<tr>
<td></td>
<td>• Owns progress during category 2 or 3 Major Incident</td>
</tr>
<tr>
<td></td>
<td>• Communicates with CIO/DCIO, other senior HUIT staff, and key stakeholders (e.g., deans)</td>
</tr>
<tr>
<td><strong>Service and Technical</strong></td>
<td><strong>Incident Manager</strong> (Service/Offering Owner)</td>
</tr>
<tr>
<td></td>
<td>• Qualifies incident</td>
</tr>
<tr>
<td></td>
<td>• Leads troubleshooting</td>
</tr>
<tr>
<td></td>
<td>• Marshalls resources for troubleshooting and resolution</td>
</tr>
<tr>
<td></td>
<td>• Accountable for communication with users and IT stakeholders</td>
</tr>
<tr>
<td></td>
<td>• Determines when incident has been resolved</td>
</tr>
<tr>
<td></td>
<td>• Conducts After Action Review and problem review</td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td><strong>Incident Coordinator</strong> (ITSM)</td>
</tr>
<tr>
<td></td>
<td>• Lead process facilitator</td>
</tr>
<tr>
<td></td>
<td>• Initiates contact with service/offering owner</td>
</tr>
<tr>
<td></td>
<td>• Establishes conference bridge</td>
</tr>
<tr>
<td></td>
<td>• Provides initial communication (e.g., HUIT alerts &amp; website, end users if predefined for affected service)</td>
</tr>
<tr>
<td></td>
<td>• Documents material technical, communications, and related information in ticket</td>
</tr>
</tbody>
</table>
# Major Incident Communications

<table>
<thead>
<tr>
<th>HUIT</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Declaration</strong></td>
<td></td>
</tr>
<tr>
<td>• Ticket created (Incident Coordinator)</td>
<td>• HUIT website and Twitter (Incident Coordinator)</td>
</tr>
<tr>
<td>• HUIT alert - New (Incident Coordinator)</td>
<td>• Service Desk phone message</td>
</tr>
<tr>
<td>• Updates to UCIO/DCIO, if category 2 or 3 (Incident Leader)</td>
<td>• End users and stakeholders (Service/Offering Owner)</td>
</tr>
<tr>
<td><strong>Assess and Contain</strong></td>
<td></td>
</tr>
<tr>
<td>• Updates every 30 minutes to Incident Coordinator and, if applicable, Incident Leader (Service/Offering Owner)</td>
<td>• As necessary, update end users and stakeholders (Service/Offering Owner)</td>
</tr>
<tr>
<td>• Updates to UCIO/DCIO, if category 2 or 3 (Incident Leader)</td>
<td></td>
</tr>
<tr>
<td>• HUIT alert – Category Change (Incident Coordinator)</td>
<td></td>
</tr>
<tr>
<td><strong>Resolve</strong></td>
<td></td>
</tr>
<tr>
<td>• Declaration of resolution to Incident Coordinator and, if applicable, Incident Leader (Service/Offering Owner)</td>
<td>• HUIT website and Twitter (Incident Coordinator)</td>
</tr>
<tr>
<td>• HUIT alert - Resolved (Incident Coordinator)</td>
<td>• End users and stakeholders (Service/Offering Owner)</td>
</tr>
<tr>
<td>• Updates to UCIO/DCIO, if category 2 or 3 (Incident Leader)</td>
<td></td>
</tr>
</tbody>
</table>
Major Incidents: Process and Procedures
Declaration of Major Incident

**Triggers**

<table>
<thead>
<tr>
<th>End Users</th>
<th>Sudden flood of tickets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staff</strong></td>
<td>Preventative measure, alerts, vendor notifications</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria</th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Urgency</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intolerance for delay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk of Escalation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>into more widespread issue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Size of Population</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Responsible for declaration:
- Incident Manager
- If above unavailable, Incident Coordinator

Declare Major Incident, if two criteria are M / H.
Initial Coordination

- Incident Coordinator convenes service/offering owner and technical team on conference bridge.

  The Conference Bridge is critical for efficient troubleshooting and centralized communications.

- All required resource should join within **15 minutes**.
  - If no response, Incident Coordinator escalates to Service Owner and/or Director/MD.

- Once service/offering owner (or proxy) joins, s/he leads call.

- Initial discussion on bridge:
  1. Articulate issue.
  3. Review recent changes.

- Open separate, technical bridge, if needed.

**NB:** Activity on bridge should focus **primarily** on service restoration. Root cause is important, but should generally remain secondary. Whenever possible, preserve forensic information in support of further analysis and After Action Review.
Conference Bridge Phone Numbers and Access

Join the Bridge:
866-890-3820 or 334-323-7229

<table>
<thead>
<tr>
<th>Bridge</th>
<th>Leader</th>
<th>Participant</th>
</tr>
</thead>
<tbody>
<tr>
<td>MI Bridge</td>
<td>71284835#</td>
<td>38793366#</td>
</tr>
<tr>
<td>Secondary Bridge</td>
<td>58775889#</td>
<td>86065154#</td>
</tr>
<tr>
<td>Tertiary Bridge</td>
<td>52545874#</td>
<td>42832588#</td>
</tr>
</tbody>
</table>

Conference Bridge Features

**LEADER**
- *2  Begin / end recording
- *7  Lock / unlock conference
- 72#  Roll call
- 81#  Mute all lines
- 80#  Unmute all lines

**ANYONE**
- *0  Operator
- *6  Mute / unmute your line
Major Incident Classification

• Incident Manager (or proxy) provides initial classification.
  – Based on reported and actual user impact, event monitoring, availability of known solutions, and potential to become a crisis.
  – If Incident Manager unreachable, this assessment defaults to the Incident Coordinator.

• Preliminary assessment should be made and then updated every 30 minutes (may be longer, depending on investigation needed).
  – It is better to err on the side of caution and, if appropriate, downgrade to Critical during or after the incident.

• If no possible solution is identified within 2 hours, MI category should be upgraded.

• Incident Manager may adjust classification, as additional information is gathered, based on time of year and/or business needs, etc.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Incident Leader Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial assessment or limited impact with risk of escalation</td>
<td>Informed</td>
</tr>
<tr>
<td>2</td>
<td>Known solution or working toward a solution</td>
<td>Involved, if extended</td>
</tr>
<tr>
<td>3</td>
<td>Significant impact with no known solution</td>
<td>Leading</td>
</tr>
</tbody>
</table>
Information Security Incidents

• Notify Information Security Operations of any incidents that may pertain to information security (e.g., system compromise, compromise of administrative credentials).

• Incidents with a significant information security component should be handled differently from the standard Major Incident protocol.
  – In the case of system and/or account compromise, sufficient time must be allotted for accurate and detailed assessment of the scope of the incident.
  – Communications outside of – or even internal to – HUIT are often limited (e.g., no ticket in ServiceNow, no posting on HUIT status page) to avoid “tipping off” the perpetrator (either through our own or public channels) and minimize anxiety.

• For these incidents, the CISO (or designate) acts as Incident Leader.
Initial Communication of a Major Incident

- Incident Coordinator creates ticket in ServiceNow
  - Primary channel for internal updates on progress
- Communications chain initiated for category 2 (extended) or category 3:
  Incident Manager → Incident Leader → DCIO/CIO
- Incident Coordinator notifies HUIT staff
  - HUIT alerts
  - HUIT website (status.huit.harvard.edu)
  - Twitter (@HUITAlerts)
- Update of Service Desk phone message with any specific steps/information
- Incident Manager notifies users and stakeholders
Investigation and Diagnosis

Guiding Principles & Procedures

- Pursue multiple leads and parallel work streams as appropriate.
- Avoid combining seemingly-related incidents.
  - Continue to troubleshoot as separate incidents until it’s confirmed they are related.
- Review change calendar to identify any potential causes or impact.
- Follow troubleshooting checklists; leverage workflows or service maps (if available).
Investigation and Diagnosis

**Incident Manager** (aka Service/Offering Owner)
- Technical investigation and diagnosis
- Marshaling of appropriate troubleshooting resources
  - Launch 2nd conference bridge for technical discussions, if needed; coordinate between two conferences to ensure timely updates
- Vendor management as needed
- Ongoing status updates for communication needs

**Incident Coordinator**
- Documentation of all material technical, process, communications, and related information in ticket
- Additional HUIT Alerts, if MI category changes

**Incident Leader**
- Hourly updates to CIO/DCIO and key senior-level stakeholders
Technical Escalation

- Escalations raise involvement and awareness of incident to more advanced skill sets or senior decision-making levels.
- Incident Manager is accountable for the overall escalation process.
- Current level notifies the next level no later than the hour indicated below.

<table>
<thead>
<tr>
<th>NLT* Hour</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting</td>
<td>Admins, Engineers, Developers, etc.</td>
</tr>
<tr>
<td>Begins</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Sr. Tech. Engineers and Architects</td>
</tr>
<tr>
<td>4</td>
<td>Vendor (if applicable)</td>
</tr>
</tbody>
</table>

*No Later Than
Resolution and Closure

• Resolution
  – Incident Manager validates all services are operational, including those downstream
  – Incident Coordinator gathers all key information (e.g., end time, actions, root cause when known) and includes in ticket

• Incident Closure
  – Final communication, including HUIT Alert notification of resolution
  – Problem review and After Action Review for all involved
    • Occurs following Tuesday during Problem Management meetings
    • Confirm/update root cause
    • Address any open issues or concerns
    • Identify necessary mitigation and next steps, including owners and timelines
After Action Review Template

• Incident #
• Duration
  – Start date
  – End date
  – Total time
• Affected Systems
• Symptoms
• Chronology and Summary of Events
• Workaround/Solution

• Root Cause Analysis
  – Technical
• Process & Communication Review
  – What went well?
  – What can be improved?
• Next Steps
  – Preventative measures to prevent recurrence
  – Recommendations
Major Incidents: Roles & Responsibilities
Code of Conduct

• **Remember to Act according to the HUIT Values** (i.e. user-focused, collaborative, innovative, and open), especially during these critical periods.

• **Report Issues**: Call the hotline at 617-496-2831!
  – “See something, say something.”
  – Avoid calls to the Service Desk or individual staff.
  – **For crisis**, calls may be made directly to the ESF leader.

• **Respond Quickly** when contacted by the Incident Coordinator.
  – Call into the bridge as soon as possible, but no later than 15 minutes after notification.

• **Respect the Process** to ensure efficient resolution and maximum collaboration.
  – Limit conference bridge to essential staff: Avoid unnecessary participants, which may impede progress and clear communication.
Code of Conduct

• Ensure Timely Access to Appropriate Staff (Yourself or Others).
  – Maintain and share up-to-date lists of on call information, staff (including vacation and back-up coverage), and phone numbers.
  – Provide readily available access to needed technical expertise (especially during times of escalation or transition).
  – Dedicate your own or your team’s time as warranted and attention to ensure speedy service restoration.

• Coordinate Internal Communications: Material troubleshooting, communications, and decisions should be communicated/validated on conference bridge and in the ticket.
Incident Manager Responsibilities

Service/Offering Owner or proxy is accountable for the restoration of an interrupted or degraded service.

- Confirm and classify Major Incident, based on organizational impact.
- Lead troubleshooting effort:
  - Identify, marshal, and deploy technical resources.
  - Lead discussion on primary conference bridge (and coordinate with technical bridge, if applicable).
- Approve proposed fix or workaround.
- Confirm resolution of Major Incident.
- Accountable for communications with stakeholders and end-users.
- Responsible for After Action Review:
  - Review and validate record of events.
  - Determine and implement preventative measures and next steps.
Additional Responsibilities for Service Owners

To optimize service restoration and prevent future Major Incidents, these activities should be well defined for the MI process:

Vendor Management

• Manage relationships with vendors and set response expectations.
  – Review of vendor contracts for incident response times
  – Enforcement of contracts breaches
  – Process to review root causes of incidents

Relationship Management

• Predefine business impact of services for different levels of outages.

Configuration Management

• Document and map service components and relationships for troubleshooting.
Technical Teams Responsibilities

Any HUIT technical resource (Infrastructure, Development, Operations, etc.) that receives alerts or escalations or has a role in restoring normal operations.

- Identify and escalate a Major Incident to Incident Coordinator.
- Participate in conference bridge, if appropriate.
  - Join bridge within 15 minutes of HUIT alert or on-call contact.
  - If not available, an alternate should be pre-identified and easily accessible.
- Understand technical landscape, including:
  - Technical or service dependencies, such as downstream effects
  - Recent changes
- Troubleshoot and work to resolve incident in accordance with internal procedures.
- Help document incident details and any material steps taken to resolve underlying problem.
- Provide regular updates to the Incident Manager and/or Incident Coordinator on status of investigation and resolution of incident.
Service Desk and SOC Ops Responsibilities

These frontline resources, including after hours, may be the first to identify a Major Incident.

- Identify Major Incidents and escalate to the Incident Coordinator.
- Track individual tickets/calls, relating them to the main/master incident.
- Communicate with end users, individually via calls and email and/or generally through an updated incoming message.
- Provide technical information to the bridge as appropriate or requested.
- Help document incident details and any material steps taken to resolve the underlying problem.
Incident Coordinator Responsibilities

Facilitates the major incident process through coordination, documentation, and communication.

• Initiate and participate in primary conference bridge, adhering to timelines and guiding principles.

• Open a Major Incident ticket and maintain ongoing record of events.

• Maintain update and escalation intervals and associated communications with technical resources, service owners, and management.

• Ensure that internal communications about a Major Incident are conducted in a timely manner, including:
  – HUIT alerts at the beginning and resolution
  – HUIT website postings (statuspage.io)
  – Twitter

• Create an associated Problem Record.
Incident Leader Responsibilities

- Supervises service restoration at a high level.
- Accountable for communicating with CIO, DCIO, and key senior-level stakeholders.
- Facilitates availability of appropriate troubleshooting resources (e.g., clearing calendars, removing barriers).
- Oversees decisions about restoration activities that affect other non-impacted services.
- Has discretion to mobilize resources across HUIT (e.g., other service areas).
- If warranted, with CIO/DCIO, invokes assessment of incident as Crisis.

Owns progress towards service restoration during category 2 (extended) or category 3 Major Incident.
## RACI Matrix for Key Roles during Major Incidents

<table>
<thead>
<tr>
<th>Activity</th>
<th>Incident Leader (category 2/3)</th>
<th>Incident Coordinator</th>
<th>Service / Offering Owner</th>
<th>Service Desk</th>
<th>SOC Operations</th>
<th>Technical Resource</th>
<th>Technical Line Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Identification</td>
<td>C</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Initial Coordination</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Conference Bridge + Open Ticket</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Initial Communications</td>
<td>R</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>C/R</td>
<td>C/R</td>
<td>A</td>
<td>C/R</td>
<td>C/R</td>
<td>C/R</td>
<td>C/R</td>
</tr>
<tr>
<td>Technical Investigation &amp; Diagnosis</td>
<td>R</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Escalation</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Ongoing Communication</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Incident Documentation</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>C/R</td>
<td>C/R</td>
<td>C/R</td>
<td>C/R</td>
</tr>
<tr>
<td>Resolution</td>
<td>C/R</td>
<td>C/R</td>
<td>A</td>
<td>C/R</td>
<td>C/R</td>
<td>C/R</td>
<td>C/R</td>
</tr>
<tr>
<td>After Action Review</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>
Appendix
Major Incident and Crisis Workflow

- **Crisis Declared**
  - Determine if Crisis
  - MI Declared
    - Assess / Contain / Resolve
      - MI Closed
      - MI AAR
  - Crisis Closed
  - Crisis AAR
Template: HUIT Alerts Email

Subject: [huit-alerts] INC##### - Description

Major Incident Status:
Category: NEW field
Time Reported:
Incident Start:

Customer / Business Impact:

Services Affected:

Major Incident Conference Bridge: 866-890-3820,,38793366#
**Representatives from technical and service owner groups are expected on the call bridge for incident assessment within 15 minutes of HUIT alert.

Group(s) Responsible:

Service Owner Group: IT Service Management (ITSM)

Status updates: HUIT Service Status Dashboard
ServiceNow: Incident url

Current Actions:

*Incident Coordinator Name*
HUIT Incident Management
617-496-2831