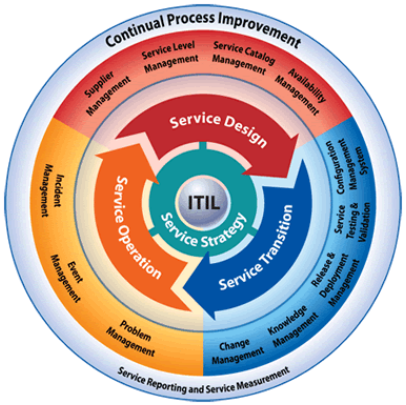
Major Incident Management Training



IT Service Management

Texas Health Resources

What is a major incident?

A major incident is primarily defined by impact and urgency.

- If an incident has an impact on the enterprise, a site, or a department and requires critical or high urgency to resolve, it is considered major.

If an incident is impacting a critical application or service, it is considered a major incident.

- The list of critical applications and services can be found in ITSM site.

  http://team.txhealth.org/teams/ITS/ITSM/Lists/Application/AllItems.aspx

Priority Assessment Matrix (Urgency + Impact / 2) rounded to the higher priority		Urgency			
		1 – Critical	2 – High	3 – Average	4 – Low
Impact	1 – Enterprise	P1	P1	P2	P2
	2 – Site/Dept	P1	P2	P2	P3
	3 – Multiple users	P2	P2	P3	P3
	4 – User	P2	P3	P3	P4

Examples of priority 1 (P1) incidents:

1. Disruption or degradation in critical network infrastructure
   a) Examples are: VLAN, LDAP, AD, DNS, NETAPP or storage systems
2. Disruption or degradation in a critical application
   a) Examples: CareConnect and Outlook
3. Location-wide (hospital, clinic) utility failure
   a) Examples: circuits and telephone systems
4. Virus outbreak
5. Disruption or degradation in 2 or more tier 2 high priority applications

More examples of a major incident

- All or a majority of the users of a tier 1 service, or two or more tier 2 services, cannot access that service. No workaround is available.
- Multiple users experience a server, application or database freeze.
- A network outage, affecting core or distribution layers, or key routers and firewalls.
- A non-redundant network device or multiple devices at the core distribution layer are unavailable.
- Specific outage scenarios, particularly those directly impacting patient care.
- Clusters or redundant devices failover with some amount of downtime to end-users, although the system remains available with an increased risk of failure.
- A production server in a clustered environment where failover is not immediate.
- A critical application has current users logged in, but it is rejecting new user logins.
- A non-redundant production server is unavailable.

What's expected of you?

DO:

If you are having a problem with an application or a service, or are experiencing a network outage or slowness, contact the Service Desk **immediately**.

If you are working on a problem that has the potential to become a major incident, contact the Service Desk **immediately** for consultation on whether a major incident threshold has been reached.

DON'T:

Send out a mass email or yammer asking if others are having problems

Continue to work on the problem without escalation to service desk

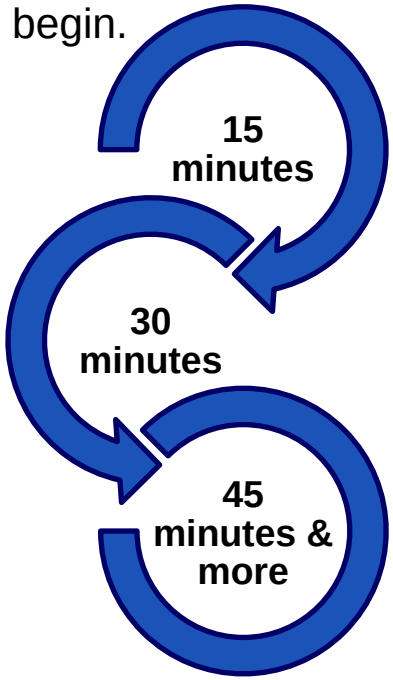
“The First Fifteen”

The first fifteen minutes are critical within the major incident cycle.

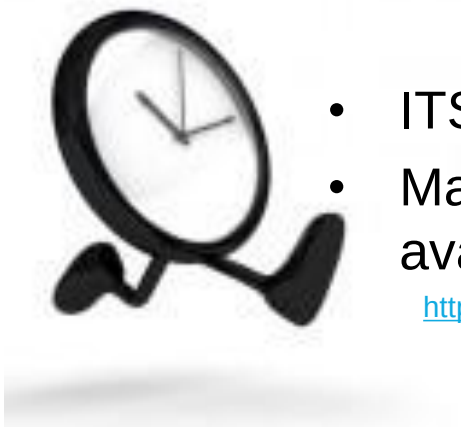
- During “the First Fifteen,” the initial triage takes place. Subject matter expert teams should have internal conversations on how to manage the first fifteen minutes of an incident for the services they manage.
- It is critical to begin immediate trouble shooting, fault isolation and restoration activities.
- It is important that the incident impact is evaluated so appropriate resources are brought together and escalation activities begin.

By thirty minutes of a major incident, if there is no resolution, it is vital that communications to the customers occur.

- Incident Manager on Duty contacts the Director on Duty.
- Incident Manager on Duty contacts the Service Manager .
- Director on Duty determines if further communication is required.



Major Incident Management Process

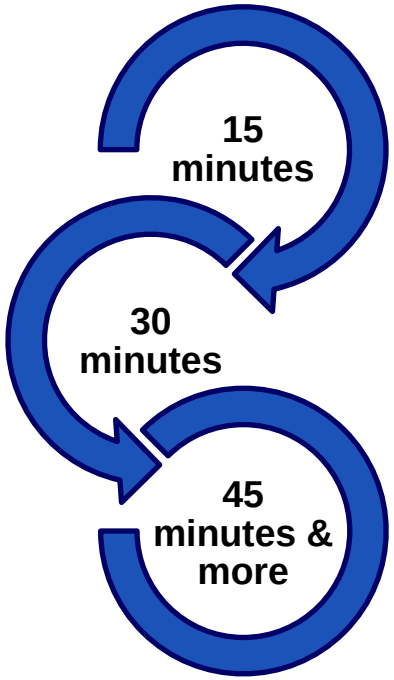


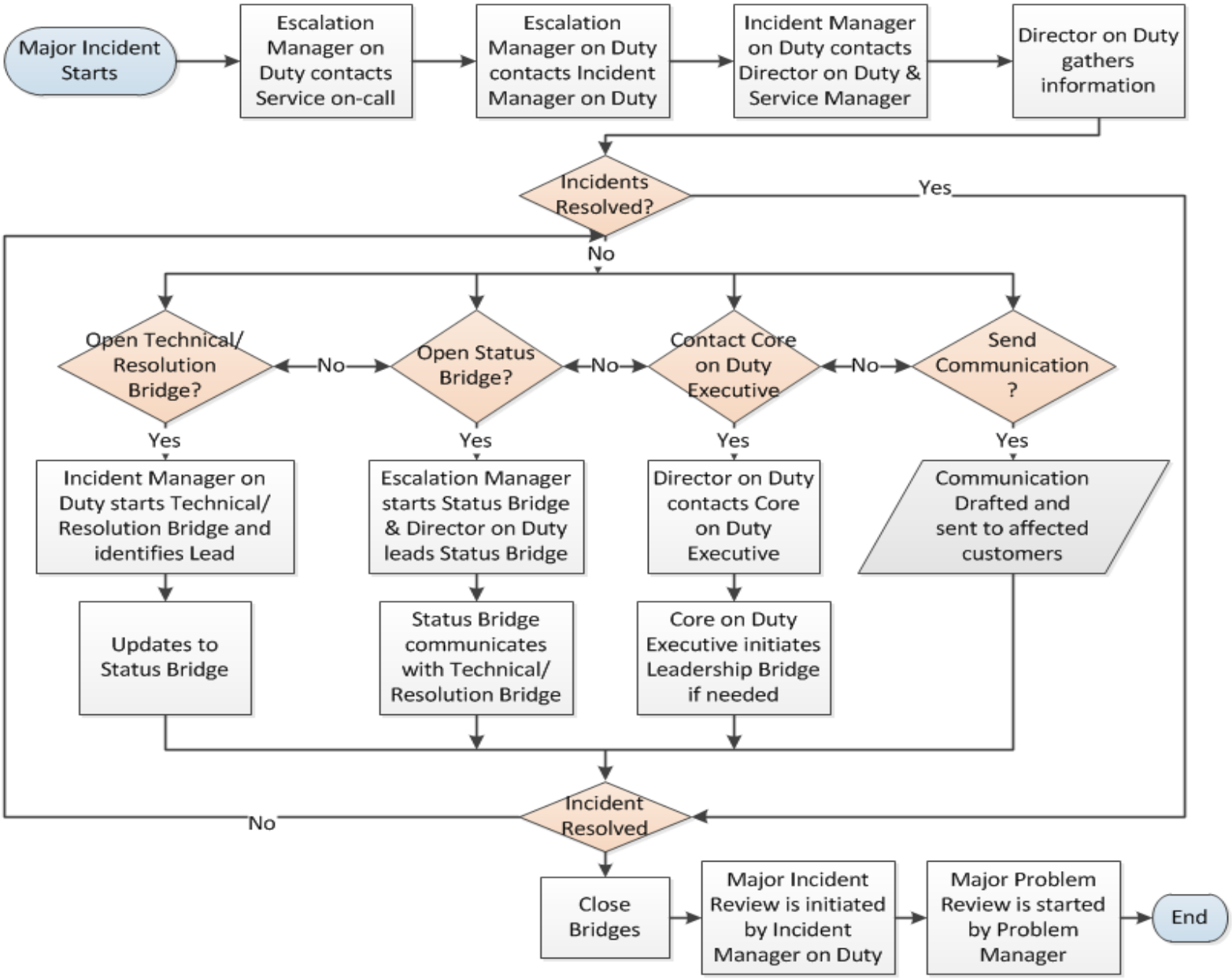
- ITS has defined processes for managing Major Incidents
- Major Incident Management Process documentation is available on the ITSM SharePoint site.

http://team.txhealth.org/teams/ITS/ITSM/SitePages/ITSM%20Reference%20Materials.aspx

What's expected of you?

Engage the Service Desk during the critical first 15 minutes so major incident management processes can be triggered.




Major Incident Starts
Escalation Manager on Duty contacts Service on-call
Escalation Manager on Duty contacts Incident Manager on Duty
Incident Manager on Duty contacts Director on Duty & Service Manager
Director on Duty gathers information
Incidents Resolved?
Yes
No
Open Technical/ Resolution Bridge?
No
Open Status Bridge?
No
Contact Core on Duty Executive
No
Send Communication ?
Yes
Yes
Yes
Yes
Incident Manager on Duty starts Technical/ Resolution Bridge and identifies Lead
Escalation Manager starts Status Bridge & Director on Duty leads Status Bridge
Director on Duty contacts Core on Duty Executive
Communication Drafted and sent to affected customers
Updates to Status Bridge
Status Bridge communicates with Technical/ Resolution Bridge
Core on Duty Executive initiates Leadership Bridge if needed
Incident Resolved
No
Close Bridges
Major Incident Review is initiated by Incident Manager on Duty
Major Problem Review is started by Problem Manager
End

Role	Responsibilities
Service Desk	• Determines Major Incident in progress • Provides information on calls from customers to Escalation Manager
Escalation Manager (Service Desk Lead)	• Contacts Incident Manager on Duty (IMOD) & Technical/Application On-Call • Gathers information from Service Desk on Major Incident • Starts Status Bridge and sends communications
Incident Manager	• Contacts Director on Duty (DOD) and Technical/Application Manager • Helps determine if incident is resolved • Helps determine if a Technical Resolution Bridge is needed • Starts Technical Resolution Bridge and determines technical lead • Helps determine if a Status Bridge is needed and provides updates to Status Bridge • Completes Major Incident Review
Service On-call	• Performs initial diagnosis and troubleshooting of the Major Incident • Involved in resolution of Major Incident
Service Manager	• Helps determine if a Technical Resolution Bridge is needed • Involved in resolution of Major Incident • Drafts communications
Director On Duty (DOD)	• Gathers information on Major Incident • Helps determine if incident is resolved • Helps determine if a Technical Resolution Bridge and a Status Bridge are needed • Responsible for Status Bridge • Contacts Core On Duty Executive • Approves/revises communications
Core Executive On Duty (CODE)	• Determines if Executive Leadership is contacted • Starts Leadership Bridge
Problem Manager	• Opens Problem Record • Completes Major Problem Review

On Duty Calendar: http://team.txhealth.org/teams/ITS/itsl/Lists/Director%20on%20Duty%20Calendar/calendar.aspx

For more information…

Major Incident Process Guide

http://team.txhealth.org/teams/ITS/ITSM/so/Major%20Incident%20Process%20Guide.doc

Priority Matrix and Service Targets

http://team.txhealth.org/teams/ITS/ITSM/so/Priority%20Matrix%20and%20Service%20Targets.docx

ITSM Material Reference Page:

http://team.txhealth.org/teams/ITS/ITSM/SitePages/ITSM%20Reference%20Materials.aspx

List of critical applications and services:

http://team.txhealth.org/teams/ITS/ITSM/Lists/Application/AllItems.aspx

On Duty Calendar:

http://team.txhealth.org/teams/ITS/itsl/Lists/Director%20on%20Duty%20Calendar/calendar.aspx