information technology

IT Major Incident Management

UCSF

Major Incident Handling Phases

A Major Incident is an event significantly impacting IT operations with widespread ramifications affecting multiple IT clients.

Four key phases:


Phase 1 – Detection, Invoke Major Incident Process


Phase 2 – Escalate to Major Incident P2


Phase 3 – Escalate to Major Incident Critical

(Medical Center IT-911 or Campus ITS P1)


Phase 4 – Closure/Stabilization

information technology

Phase 1 - Detection

A Major Incident is identified. Issues are reported through various channels:

- IT Operations
- Alerts sent from monitored systems
- Customers contacting the Service Desk

Phase 2 – Escalation to P2

A system or infrastructure component is fully or partially affected causing impact to clinical or business operations.

Multiple technical resources may be convened, customers are notified or engaged and a plan is developed to solve the problem.

Phase 3 – Escalation to P1 Critical

Campus P1 or Medical Center IT-911

Highest level of escalation. An event causing extreme negative impact to business operations and/or jeopardizing patient care.

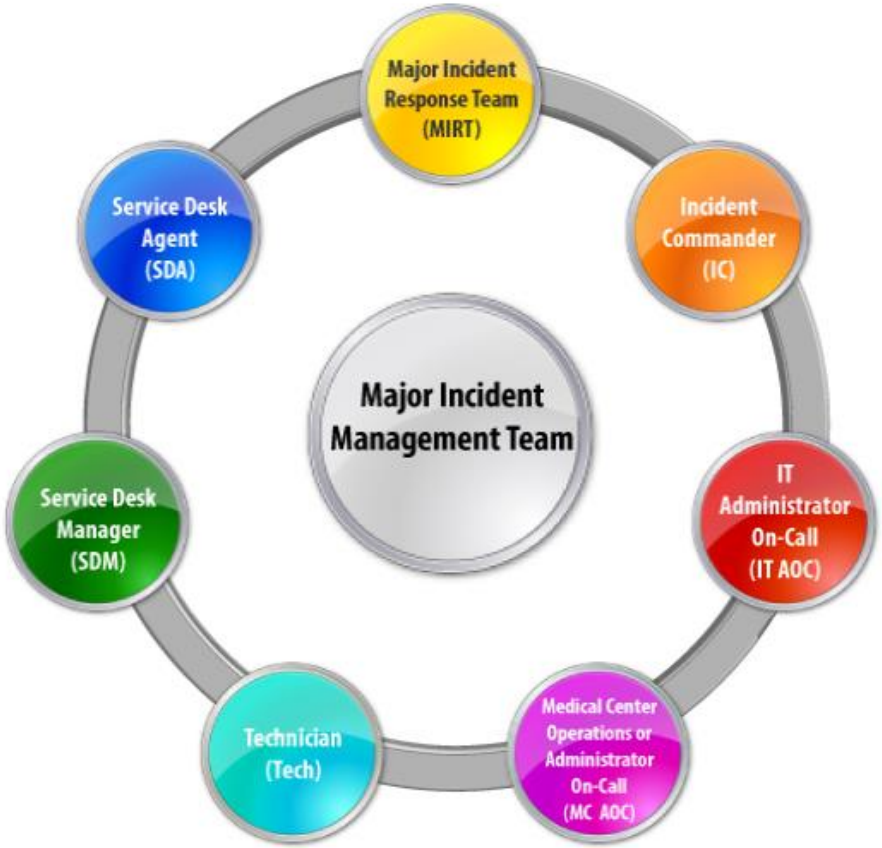
IT Executive leadership are actively engaged to coordinated key decisions and communication.

Phase 4 - Closure/Stabilization

Stabilization is achieved, recovery steps are validated and status is communicated to close the loop with everyone involved.

Important details are documented in the incident work-log as the basis for post-event or root-cause analysis.

Major Incident Team



information technology

Service Desk Agent (SDA)

Point of coordination for all incoming incident information and outgoing communications.

Service Desk Manager (SDM)

Primary point of contact within the Service Desk. Responsible for making sure potential MIs are escalated, resources are alerted, and end-users notified.

Technician

Technical Resource responsible for identifying and resolving incident. Responsible for providing regular updates to the Service Desk Staff.

Major Incident Response Team (MIRT)

Technical team tasked with identifying and resolving incident.

Incident Commander (IC)

Individual in command of the MI and responsible for escalating to the next level, if necessary. The IC drives the MI to resolution. This role is typically held by the manager (or designee) of the affected system or infrastructure component. It can also be assumed by the security manager in the event of that the incident involves a breach.

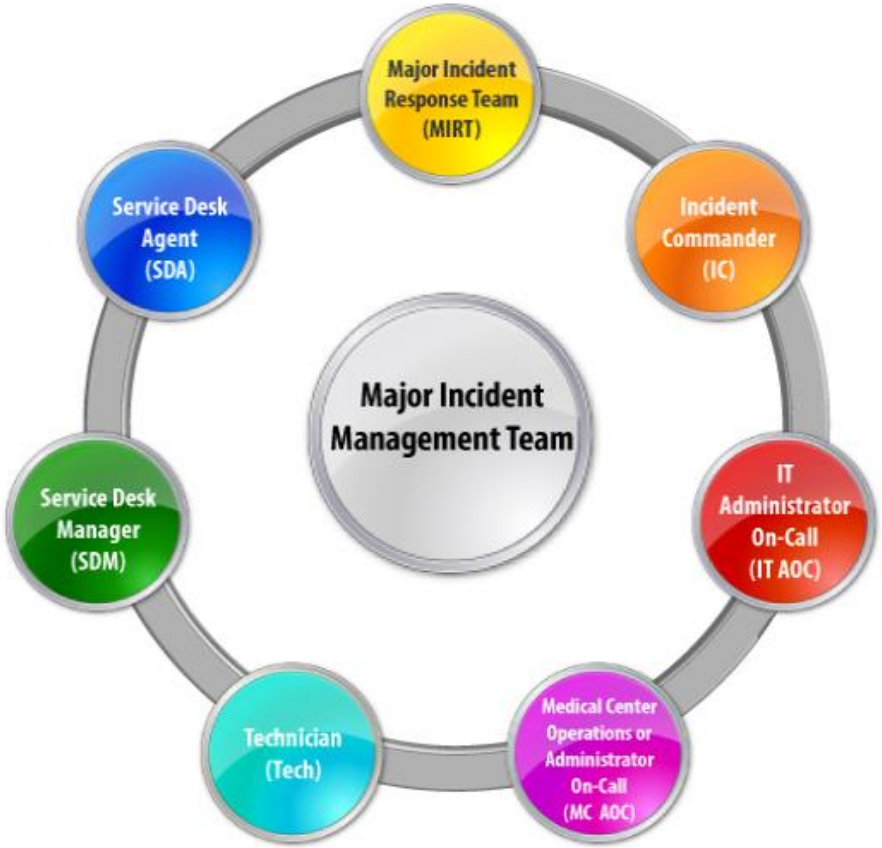
IT Administrator On-Call (IT AOC)

Director who is designated on-call and is engaged when an incident escalates to a crisis. The IT AOC is responsible for providing an enterprise perspective and making sure key leadership and other stakeholders are notified or involved.

MC Administrator On-Call (MC AOC)

Administrator On-Call responsible for providing an operational perspective into the issue and facilitating communication within the Medical Center or throughout the enterprise. The MC AOC is also responsible for initiating the Medical Center Command Center in the event that a widespread disaster occurs and cutover to Disaster Recovery processes are needed.

Major Incident Team



information technology

Detection

Who	What	Action
Tech SDA	Identify a potential Major Incident	1
Tech	Begin Incident Investigation	2
SDA	Notify Service Desk Manager	3
Tech	Confirm the issue is system wide	4
SDM	Invoke Major Incident Process	5

Escalation to Major Incident P2

Who	What	Action
Tech	Notify Incident Commander	6
IC	Open Technical Bridge	7
IC	Coordinate Remediation Effort And Initiate Work Plan	8
SDA	Prepare Frontend Service Desk Message for Inbound customer calls	9
IC	Initiate Service Desk Communication Process	10
IC	Escalate to Major Incident Priority 1 - Critical	11

Escalate to Priority 1 (P1) CRITICAL

Who	What	Action
IC	Initiate Priority 1 Conference Bridge • Campus – ITS P1 • Med Center – IT-911	12
SDM	Update Incident to P1	13
SDA	Notify IT AOC	14
IT AOC	**Decision:** to Notify CIO	15
IC	**Decision**: to Cutover to Disaster Recovery	16
IC	Continue Remediation	17

information technology

Major Incident Process

http://it.ucsf.edu/sites/it.ucsf.edu/files/major_incident_process_83112.pdf

- Major Incident Definitions
- Process Definition
  - Process Flow
  - RACI – *who is*
    - Responsible
    - Accountable
    - Consulted
    - Informed
- Major Incident Checklist