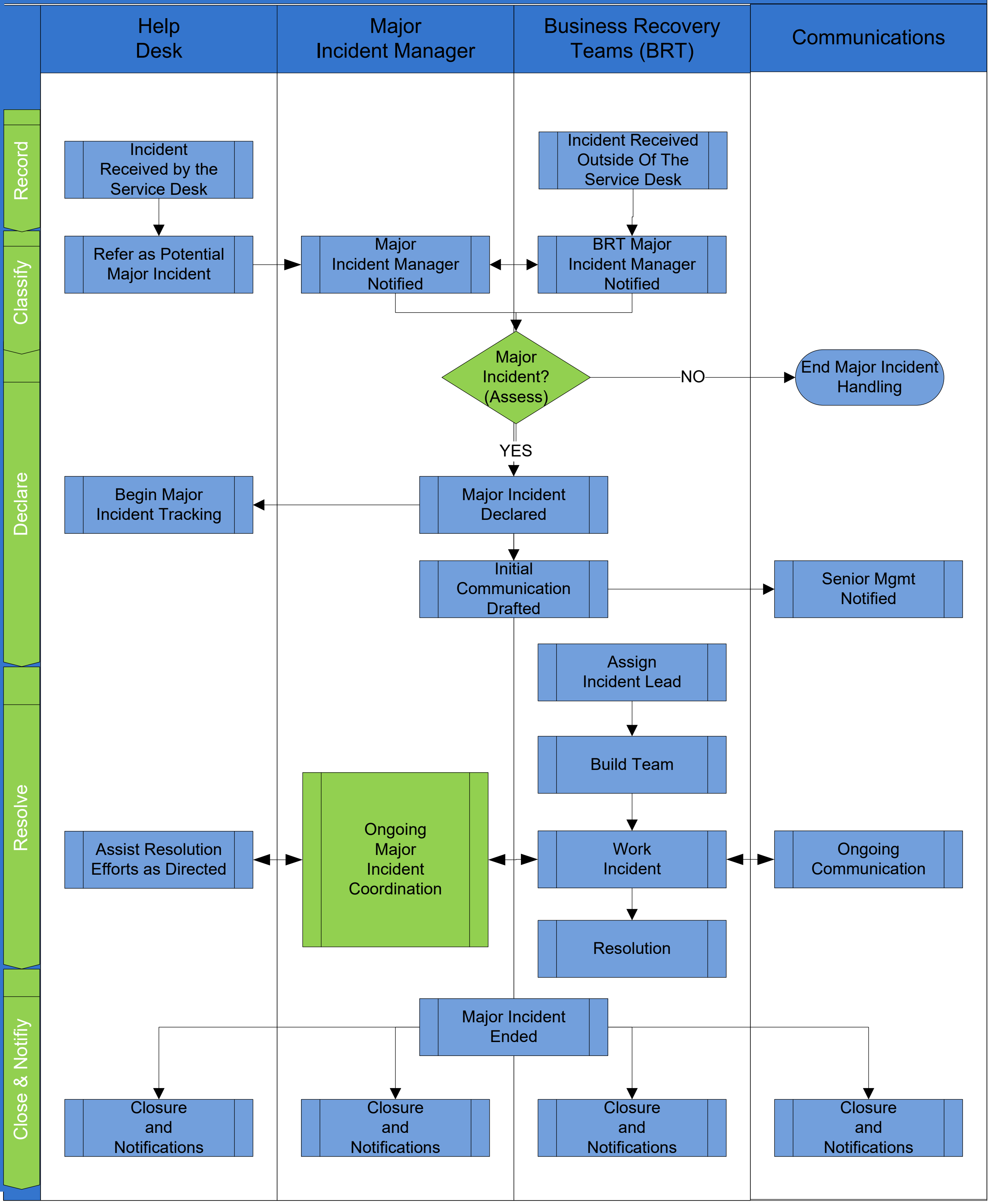
Major Incident Handling

Tuesday, October 01, 2019

A Major Incident Handling Plan Model


Help Desk
Major Incident Manager
Business Recovery Teams (BRT)
Communications
Record
Classify
Declare
Resolve
Close & Notifiy
Incident Received by the Service Desk
Incident Received Outside Of The Service Desk
Refer as Potential Major Incident
Major Incident Manager Notified
BRT Major Incident Manager Notified
Major Incident? (Assess)
NO
End Major Incident Handling
YES
Begin Major Incident Tracking
Major Incident Declared
Initial Communication Drafted
Senior Mgmt Notified
Assign Incident Lead
Build Team
Assist Resolution Efforts as Directed
Ongoing Major Incident Coordination
Work Incident
Ongoing Communication
Resolution
Major Incident Ended
Closure and Notifications
Closure and Notifications
Closure and Notifications
Closure and Notifications

Return to MIH Process

Major Incident -- (Service Operation) The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Major Incident Handling Process (MIH)

1.0 (Record) Incipient Event tracking.

- **1.1 An Incident is reported or recorded that appears to be of a high enough severity to warrant MIH consideration, or**
- **1.2 Help Desk staff note pattern of tickets or events and start linking them with other similar tickets or events that have the potential to collectively be considered as a Major Incident.**
- **1.3 An Incident may also be received outside of the Help Desk by another Service Delivery Team (VPD for example)**
- **1.4 Regardless of how the Incident is received, the Incident team handling the Incident should contact the appropriate Major Incident Manager and appraise him or her of their concerns / observations.**
    - *1.4.1 At many Help Desks organizations the role of Major Incident Manager is assigned to the Help Desk Supervisor – though in larger organizations with high volumes a separate role may be necessary. For organizations without a Help Desk, this Role generally falls to the Incident Management Process Owner. In all cases it is important that the Major Incident Manager is given the authority to manage incidents effectively through first, second and third level resolution silos as they will be responsible for internal and cross-company coordination in the event of a Major Incident. It should also be noted that a Major Incident may involve more than one Major Incident Manager.*

Return to MIH Process

Major Incident -- (Service Operation) The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Major Incident Handling Process (MIH)

2.0 (Classify) Major Incident Classification.

- **2.1 The Major Incident Manager performs an initial assessment of the Incident data. If the Major Incident Manager decides that an escalation is not warranted at this time the Help Desk or Incident Team will manage these events as incidents and monitor for any changes that may occur which would warrant further escalation.**
- **2.2 If the Major Incident Manager believes based upon his or her assessment that a potential Major Incident exists, the Major Incident Manager will invoke Major Incident Handling and refer the Incident to his or her counterpart in the appropriate Business Recovery Team (BRT) for further review.**
  - ○ *2.2.1 For the purpose of this document and process, the term "Business Recovery Team" or "BRT" denotes any team or teams, internal or external, which would be appropriate to lead the resolution efforts of the potential or identified Major Incident. The BRTs are not just limited to IT or Internal organizations. For example: a major networking outage may involve (one or both) the internal Network team and the external Internet Service Provider (ISP). Conversely a Major Incident which required a BCP/DR type response (Business Continuity / Disaster Recovery) could include multiple internal and external IT teams and may also include non-IT teams such as Risk Management, Legal, Police, Fire, and others. For the proper execution of this process these teams' roles and escalation criteria must be clearly defined and this information must be made available to the Major Incident Manager in a format that is easily accessible and insures its accuracy and currency.*
- **2.3 The Major Incident Manager and BRT discuss the facts as they are known. If the BRT has defined specific Major Incident classification criteria those policies or guidelines should be used to determine the final decisions and next steps. In the absence of specific BRT policies or guidelines the following criteria can be used to help with decision making.** See Also "Assess"
  - ○ *2.3.1 Risk: Low, Med, High – What is the Risk to the organization if this Incident is not resolved? For example a virus that only causes customer aggravation would have a low risk while one that destroyed or stole data would be viewed as high.*
  - ○ *2.3.2 Scope: Limited, Broad, Global – Who or what does this Incident affect? One individual or system? Multiple users, systems or business groups? Majority of users, systems or business groups worldwide?*
  - ○ *2.3.3 Potential Impact – Finally, consider the potential Impact to employees or the business? Loss of life or limb? Significant financial loss or Brand damage? Regulatory or legislative breaches?*
- **2.4 Once a decision has been made it should be communicated without delay. If a Major Incident is declared move to step 3. If a Major Incident is not to be declared end the process here. Under no circumstances ever should a Major Incident be declared without City participation, regardless of who the resolver team is.**

Return to MIH Process

Tuesday, October 01, 2019

Major Incident -- (Service Operation) The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Major Incident Handling Process (MIH)

Major Incident Assessment Criteria (Impact, Scope, and Urgency):

In figure 1, each **IMPACT** and **URGENCY** column can earn from 0 to 3 points. For example, an Incident may have a Scope impact of 3, a Goodwill impact of 0, an Operations impact of 1, and an Urgency of 2, and thus score a 6:

	IMPACT	IMPACT	IMPACT	
Points	Scope	Goodwill	Operations	URGENCY
3 points each	Affects > 50% of users	Areas inside and outside of the company may be affected negatively	Interferes with core business functions OR loss or potential loss of mission critical data	Event underway and it cannot be stopped or changed AND immediate action is needed to resolve the issue
2 points each	Affects >10 but < 50 users OR no more than 50% of all users	The company may be affected negatively	Interferes with non-core activities OR functions that do not affect the entire company	Event scheduled to occur but not enough time remains to prevent the occurrence of an issue
1 point each	Affects < 10 users OR no more than 25% of all users	Business unit may be affected negatively	Interferes with normal completion of work OR tasks are more difficult but not impossible to complete	Event can be postponed OR is far enough away in time to allow response without loss of productivity
0 points each	Affects a single user	Goodwill unchanged	Interferes with recreational OR non-business related use	No scheduled completion time is required and normal work can continue until responding

Figure 1 Priority Scoring Matrix

Next, look at the priority codes (Critical, High, Medium, Low) and establish a value range for each. In this case a score of 12 means Critical; 9-11 means High; 5-8 means Medium; and 0-4 means Low. Following our example with a score of 6, this incident would receive a priority of Medium:

Note: ANY Incident with a Priority Value of 12 or above (Critical) must be immediately referred to the Incident Manager as an Actual Major Incident. Values from 9-11 (High) should be referred to the Incident Manager as a Potential Major Incident.

Values below 9 (Medium and Low) are not to be considered for Major Incident Handling and will be managed via the normal Incident Management process

Score	Priority Code	Response	Timeframes
12	Critical	An immediate and sustained effort using all available resources until resolved. Major Incident Handling is invoked.	Immediate action/resolution as soon as possible.
9-11	High	Technicians respond immediately, assess the situation, and may interrupt other staff working low or medium priority jobs for assistance.	Action within 1 hour/resolution within 1 business day.
5-8	Medium	Respond using standard procedures and operating within normal supervisory management structures.	Follow normal Incident Management procedures
0-4	Low	Respond using standard operating procedures as time allows.	Follow normal Incident Management procedures

Figure 2 Priority Assignment Matrix

Return to MIH Process

Tuesday, October 01, 2019

Major Incident -- (Service Operation) The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Major Incident Handling Process (MIH)

3.0 (Declare) Major Incident Declared.

- **3.1 After reviewing the Incident data, a decision is made to formally declare a Major Incident.**
- **3.2 Initial communication to Senior Management and Stakeholders is drafted and sent.**
- **3.3 Service Desk is notified and instructed to begin Major Incident tracking if appropriate.**
- **3.4 A Center of Operations is established and serves as the focal point for coordination of ongoing activities and communications for the duration of the Major Incident event.**
    - *3.4.1 When activities involve more than one organization or site there may be a need for multiple centers.*
- **3.5 A communication plan is developed and a schedule and methodology for future updates is communicated.**
    - *3.5.1 Communication plans should consider the need for multiple methods of communication. For example a bridge number for conference calls and a second line for immediate communications or discussions with individual responders. Finally there may be a need for alternative or confidential communications when the situation or conditions dictate.*
- **3.6 All of the steps detailed above are critical for an effective Major Incident response but they should not take precedence over managing the immediate situation. Good judgment is required and the order and timing of the actions taken will ultimately be determined by the specifics and urgency of the Major Incident.**

Return to MIH Process

Major Incident -- (Service Operation) The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Major Incident Handling Process (MIH)

4.0 (Resolve) Resolution Efforts Begin.

- **4.1 An Incident Lead is assigned who will be responsible for managing all efforts for the BRT and who will work with the Major Incident Manager(s) for the duration of the MI event or as required.**
  - *4.1.1 Team is built. Team may comprise members from multiple teams as needed.*
  - *4.1.2 Team agrees on communications protocol: Status, tools, phone numbers, IM, etc.*
- **4.2 Team begins to work Incident**
  - *4.2.1 Outputs: Ticket updates, FAQs, tech-messages and workarounds. Communications within the team and with Major Incident Manager(s) / BRT. Root cause, known errors, emergency RFCs.*
  - *4.2.2 Priority is placed on creating workarounds and restoration of Services. Fixes or discovering root cause are secondary.*
- **4.3 Service Desk assists efforts as directed or requested.**
  - *4.3.1 This may include providing notifications and status.*
  - *4.3.2 Updates MI ticket as appropriate or as directed.*
- **4.4 Event communications occur. Event communications may include:**
  - *4.4.1 Incident Lead communications.*
  - *4.4.2 Major Incident Manager(s) communications.*
  - *4.4.3 BRT communications.*
  - *4.4.4 Telephone conferences to discuss Resolution efforts.*
  - *4.4.5 Statuses to Senior Management and Key Stakeholders.*
- **4.5 All efforts focus on moving towards Major Incident closure and keeping all teams, Senior Management, and Stakeholders appraised of Major Incident status and estimated time of Resolution.**
- **4.6 Major Incident Manager(s) provides ongoing Event Coordination.**
  - *4.6.1 Acts as a bridge between all teams.*
  - *4.6.2 Resolves issues and insures effective efforts towards Resolution.*
  - *4.6.3 Coordinates the implementation of workarounds as requested or needed.*
  - *4.6.4 Insures the currency, accuracy, and completeness of Major Incident tracking and communications.*
- **4.7 Resolution begins.**
  - *4.7.1 Workarounds and RFCs are tested.*
  - *4.7.2 Fixes and Changes are implemented.*
- **4.8 Situation appraised. If Resolution is successful all teams and Stakeholders are notified and process moves to Closure. If Resolution is not successful, the teams analyze past efforts, identify gaps, and begin Resolution efforts again.**

Major Incident Handling

Return to MIH Process

Tuesday, October 01, 2019

Major Incident -- (Service Operation) The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Major Incident Handling Process (MIH)

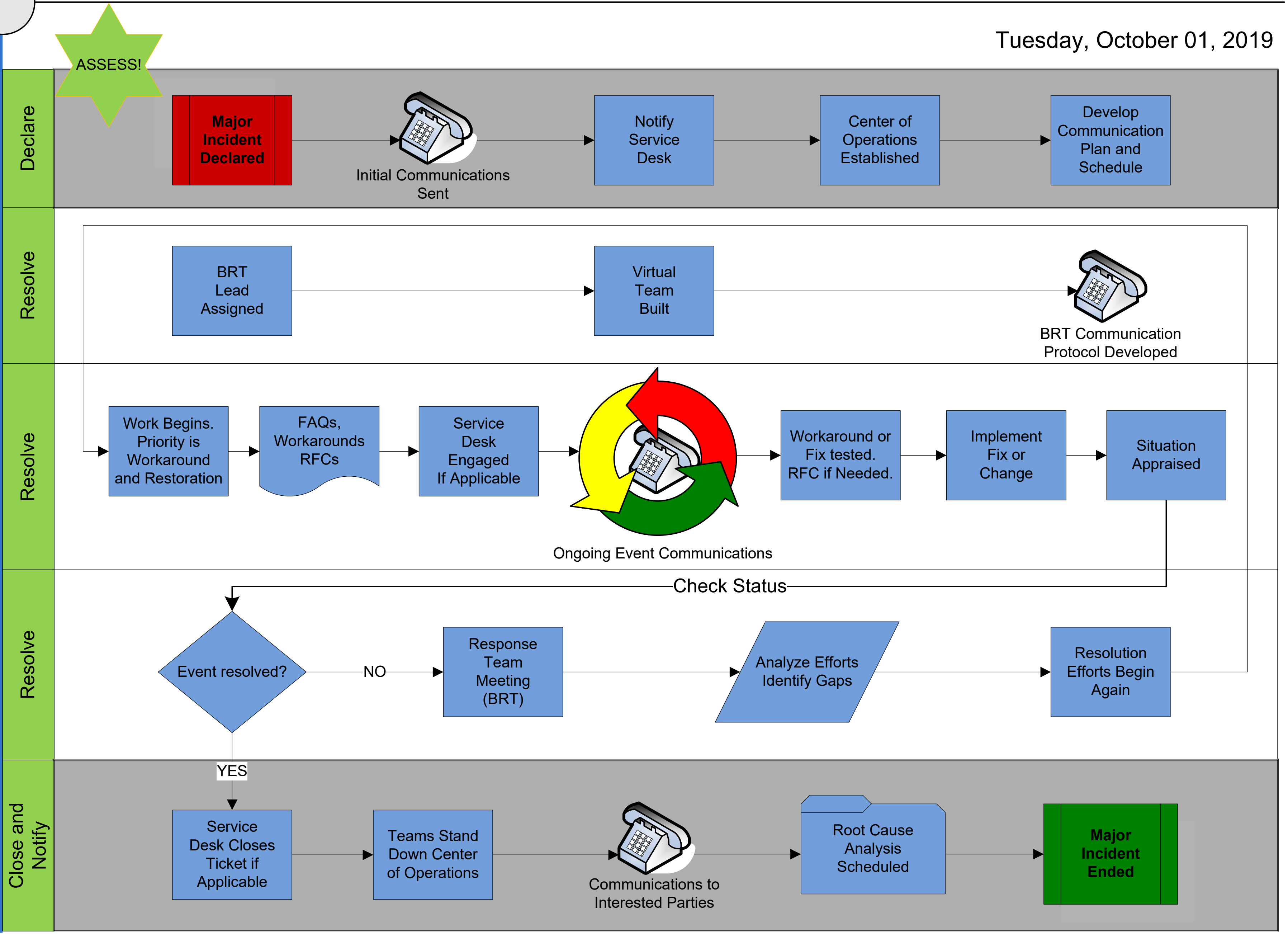
5.0 (Close and Notify) Closure efforts begin.

- **5.1 Major Incident Manager and BRT agree to close MI.**
- **5.2 Service Desk closes Major Incident ticket(s) and performs communications as directed.**
- **5.3 The Major Incident Manager insures all parties are apprised of closure status and works with BRT to stand down Major Incident Center of Operations and Resolution activities.**
- **5.4 BRT insures all parties are apprised of closure status and works with Major Incident Manager to stand down Major Incident Center of Operations and Resolution activities.**
- **5.5 Event Closure communications are sent to all interested parties.**
- **5.6 Root Cause Analysis is scheduled and the schedule communicated.**

Major Incident Handling

Return to MIH Process

Tuesday, October 01, 2019



Declare

ASSESS!

Major Incident Declared

Initial Communications Sent

Notify Service Desk

Center of Operations Established

Develop Communication Plan and Schedule

Resolve

BRT Lead Assigned

Virtual Team Built

BRT Communication Protocol Developed

Resolve

Work Begins. Priority is Workaround and Restoration

FAQs, Workarounds RFCs

Service Desk Engaged If Applicable

Ongoing Event Communications

Workaround or Fix tested. RFC if Needed.

Implement Fix or Change

Situation Appraised

Resolve

Check Status

Event resolved?

NO

Response Team Meeting (BRT)

Analyze Efforts Identify Gaps

Resolution Efforts Begin Again

YES

Close and Notify

Service Desk Closes Ticket if Applicable

Teams Stand Down Center of Operations

Communications to Interested Parties

Root Cause Analysis Scheduled

Major Incident Ended