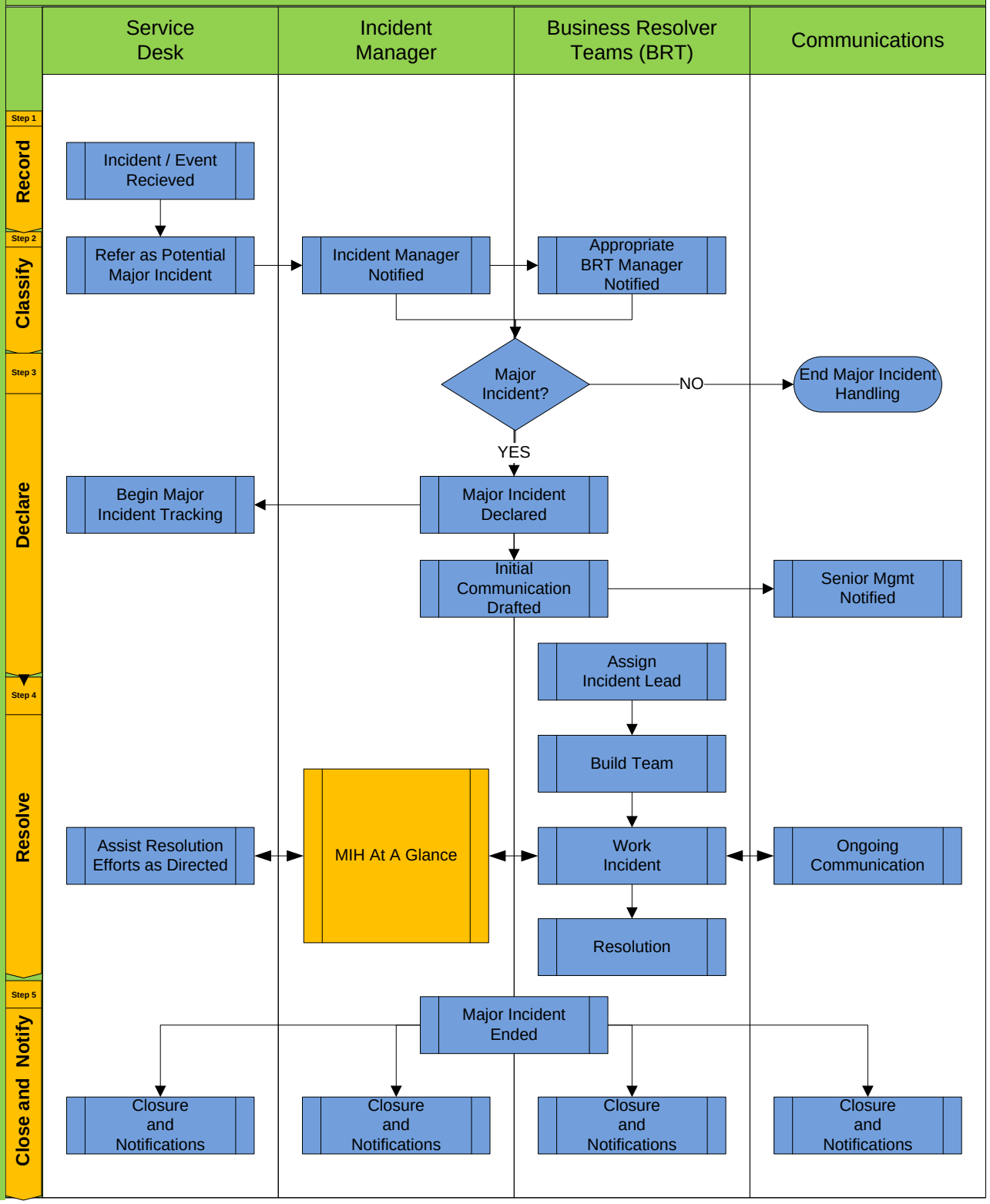
Major Incident Handling

Friday, February 10, 2012

A Major Incident Handling Plan Model



Major Incident Handling

Return to MI Process

Friday, February 10, 2012

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 (MI)	**Role**	**Inputs**	**Outputs**
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 MI consideration, **or**			
• 1.2 Service Desk staff note a pattern of tickets or events and start linking them with similar tickets or events that have the potential to collectively be considered as an MI.			
• 1.3 SD staff contact the Incident Manager and appraise him or her of their concerns / observations.			
○ 1.3.1 In many organizations the role of Incident Manager is assigned to the Service Desk Supervisor – though in larger organizations with high volumes a separate role may be necessary. The BRTs should also insure they have somebody fill the Role of Incident Manager for Major Incidents. In all cases, it is important that the Incident Manager's are given the authority to manage incidents effectively through first, second and third level resolution silos.			

Major Incident Handling

Return to MI Process

Friday, February 10, 2012

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 (MI)	**Role**	**Inputs**	**Outputs**
2.0 (Classify) Major Incident Classification.			
• 2.1 The Incident Manager performs an initial assessment of the Incident data. If the Incident Manager decides that an escalation is not warranted at this time the Service Desk will manage these events as incidents and monitor for any changes that may occur which would warrant further escalation.			
• 2.2 If the Incident Manager believes based upon his or her assessment that a potential MI exists, the Incident Manager will invoke Major Incident Handling and refer this as a potential MI to the appropriate Business Recovery Team (BRT) for further review.			
○ 2.2.1 For the purpose of this document and process, the term "**Business Resolver Team**" or "**BRT**" denotes any team either separately or in combination that would be appropriate to lead the resolution efforts of the Potential or identified Major Incident. The BRTs are not just limited to Internal organizations. For example: for a major networking outage the Vendor Network teams could be the responsible party while for a Major Security Incident Internal Information Security would lead. Conversely a major incident which required Disaster Recovery might be managed jointly by the Internal and external Disaster Recovery teams. **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 Incident Manager in a format that is easily accessible and insures its accuracy and currency.**			
• 2.3 The Incident Managers and BRT discuss the facts as they are known. **If the BRT has defined specific MI 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:			
○ 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 MI is declared move to step 3. If a MI is not to be declared end the process here. **Under no circumstances ever should an Internal MI be declared without Internal participation, regardless of who the Resolver team is.**			

Friday, February 10, 2012

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 (MI)	**Role**	**Inputs**	**Outputs**
3.0 (Declare) Major Incident Declared.			
• 3.1 After reviewing the Incident data, the Incident Managers and the BRT decide on a course of action and formally declare a MI.			
○ 3.1.1 Initial communication to Senior Management and Stakeholders is drafted and sent.			
○ 3.1.2 Service Desk is notified and instructed to begin MI tracking as appropriate.			
○ 3.1.3 A Center of Operations is established and serves as the focal point for coordination of ongoing activities and communications for the duration of the MI event.			
▪ 3.1.3.1 When activities involve more than one organization or site there may be a need for multiple centers.			
○ 3.1.4 A communication plan is developed and a schedule and methodology for future updates is communicated.			
▪ 3.1.4.1 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.			
○ 3.1.5 All of the steps detailed above are critical for an effective MI 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 MI.			

Major Incident Handling

Return to MI Process

Friday, February 10, 2012

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 (MI)	**Role**	**Inputs**	**Outputs**
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 Incident Managers 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 Incident Manager / 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 Incident Manager 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 MI closure and keeping all teams, Senior Management, and Stakeholders appraised of MI status and estimated time of Resolution.			
• 4.6 Incident Managers 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 or RFCs as requested or needed.			
○ 4.6.4 Insures the currency, accuracy, and completeness of MI tracking and communications.			
• 4.7 Resolution begins.			
○ 4.7.1 Workarounds and RFCs are tested.			
○ 4.7.2 Fixes and Changes are implemented.			
○ 4.7.3 Situation is 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.			

Friday, February 10, 2012

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 (MI)	**Role**	**Inputs**	**Outputs**
5.0 (Close and Notify) Closure efforts begin.			
• 5.1 Incident Managers and BRT agree to close MI.			
○ 5.1.1 Service Desk closes MI ticket(s) and performs communications as directed.			
○ 5.1.2 Incident Managers insure all parties are apprised of closure status and works with BRT to stand down MI Center of Operations and Resolution activities.			
○ 5.1.3 BRT insures all parties are apprised of closure status and works with Incident Manager to stand down MI Center of Operations and Resolution activities.			
○ 5.1.4 Event Closure communications are sent to all interested parties.			
○ 5.1.5 Root Cause Analysis is scheduled and the schedule communicated.			

Major Incident Handling At A Glance

Go Back

Friday, February 10, 2012