MAJOR INCIDENT HANDLING

A MANDATORY REQUIREMENT OF ORGANIZATIONAL RISK MANAGEMENT

*it***SMF** Canada Dinner Seminar Event – Oct 26, 2011

Presenter: Braun Tacon

WWW.MajorIncidentHandling.com

*it*SMF CANADA

MIH
Major Incident Handling

Presentation Abstract

Anyone who has ever flown on a commercial airliner has experienced a Major Incident Handling plan. From the steward and stewardess droning on about seat belts and oxygen masks, to the pilots in the cockpit reviewing checklist after checklist, to the little cards in the seatbacks ahead of you detailing exit locations and water landing procedures, all of these are examples of Major Incident planning in support of the airline's Risk Management goals and objectives. Plans such as these not only make good sense but are critical requirements driven by fiduciary responsibility, moral obligation, and legislative and safety mandates.

That said, many organizations continue to do business with no Major Incident Handling plan in place as part of their overall Organizational Risk Management strategy. Worse yet, when it comes to addressing that gap, far too many choose to remain in denial leaving Major Incident planning for the proverbial, "…next fiscal year."

This does not need to happen. All that is required is some forethought and a common sense approach to planning and documentation. The goal of this presentation is to clearly demonstrate why a Major Incident Handling plan is a core business requirement in today's world. To provide you some tools that you can use as a starting point for creating your own Major Incident plan and to show you how relatively simple actions like creating flowcharts, procedures along with solid testing can bring big returns to the organization's overall risk posture. This in turn allows for an increased risk appetite, creating opportunities for a more a dynamic, agile, and competitive business strategy.

Purpose / Goals

- To **demonstrate** that **Major Incident Handling is** a **mandatory** requirement of an effective Risk Management Portfolio

- To **propose a business case** that demonstrates this in such a way that is not easily rebutted

- To **provide tools and techniques** to help you begin to use Major Incident Handling Planning in your own Service Design and Operations Lifecycle

Why Are We Talking About This?

- Major Incidents Happen
- What Constitutes a Major Incident?

Major Incidents Happen

- Sometimes they are caused by technological and / or human failures
  - Timeline of RIM Blackberry Outages Including the Global Outage of Oct 10th 2011 (Most Significant in Time/Impact in RIM History)
- Sometimes they are a result of natural forces beyond any human control
  - History of Tohoku Japan Earthquake and Tsunami of March 2011
- Major Incidents can also be the result of criminal or other nefarious behavior
  - Stuxnet: A Demonstration of the Use of Malware for Industrial Subversion and Espionage

What constitutes a Major Incident?

- There are many definitions for the term Major Incident in the common lexicon. Regardless of what definition you assign to the phrase this much is certain:
  - Major Incidents are unpredictable
  - Major Incidents are statistically probable
  - Dealing with any Major Incident demands a plan
  - Any plan should be tailored to your specific industry, discipline, and needs

Major Incidents: Why Plan?

Would you…

- Participate in the sport of parachute jumping without a reserve parachute?
- Go open water diving without a reserve air supply or a buddy?
- Fly in a jetliner that did not have capability to deploy oxygen masks in an emergency?
- **In all probability you would not. Why?**

Major Incidents: Why Plan?

It is a fact that parachutes seldom fail, but when they do a reserve is needed

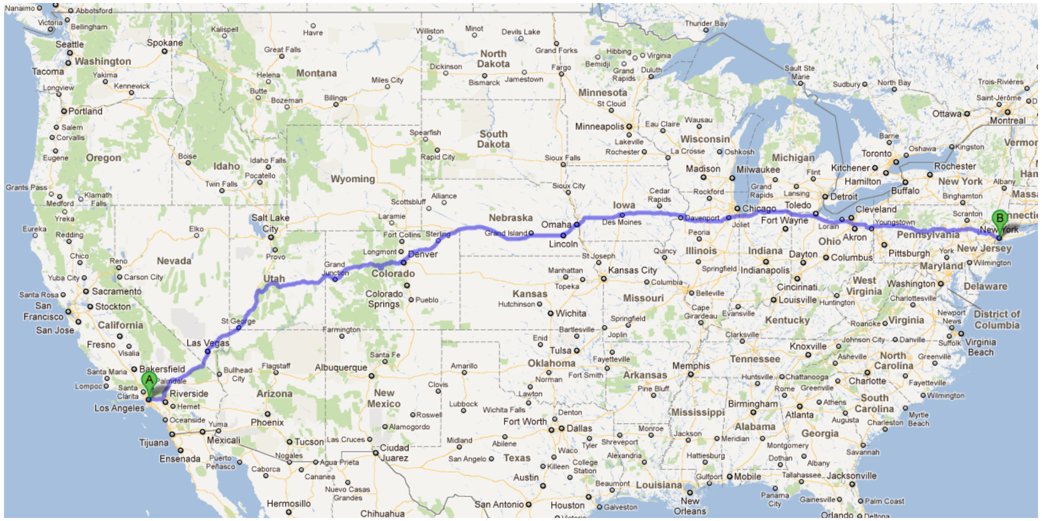
Most diving fatalities are caused by insufficient air or situations that require a buddy's assistance

At the altitudes that jetliners fly, a loss of cabin pressure is certain death without supplemental oxygen

Plans such as these are nothing more than "**common sense**"

Major Incident Handling – Planning Your Trip?

Building a Major Incident Handling Plan is much like planning a cross-country trip. You'll need to know where you are going, but you will also need to know how to get there



My Trip – Where Am I Going

My Trip – How To Get There

1. Head **southeast** on **W 1st St** toward **S Main St**

2. Take the 1st left onto **N Main St**

3. Take the 2nd right onto **W Aliso St**

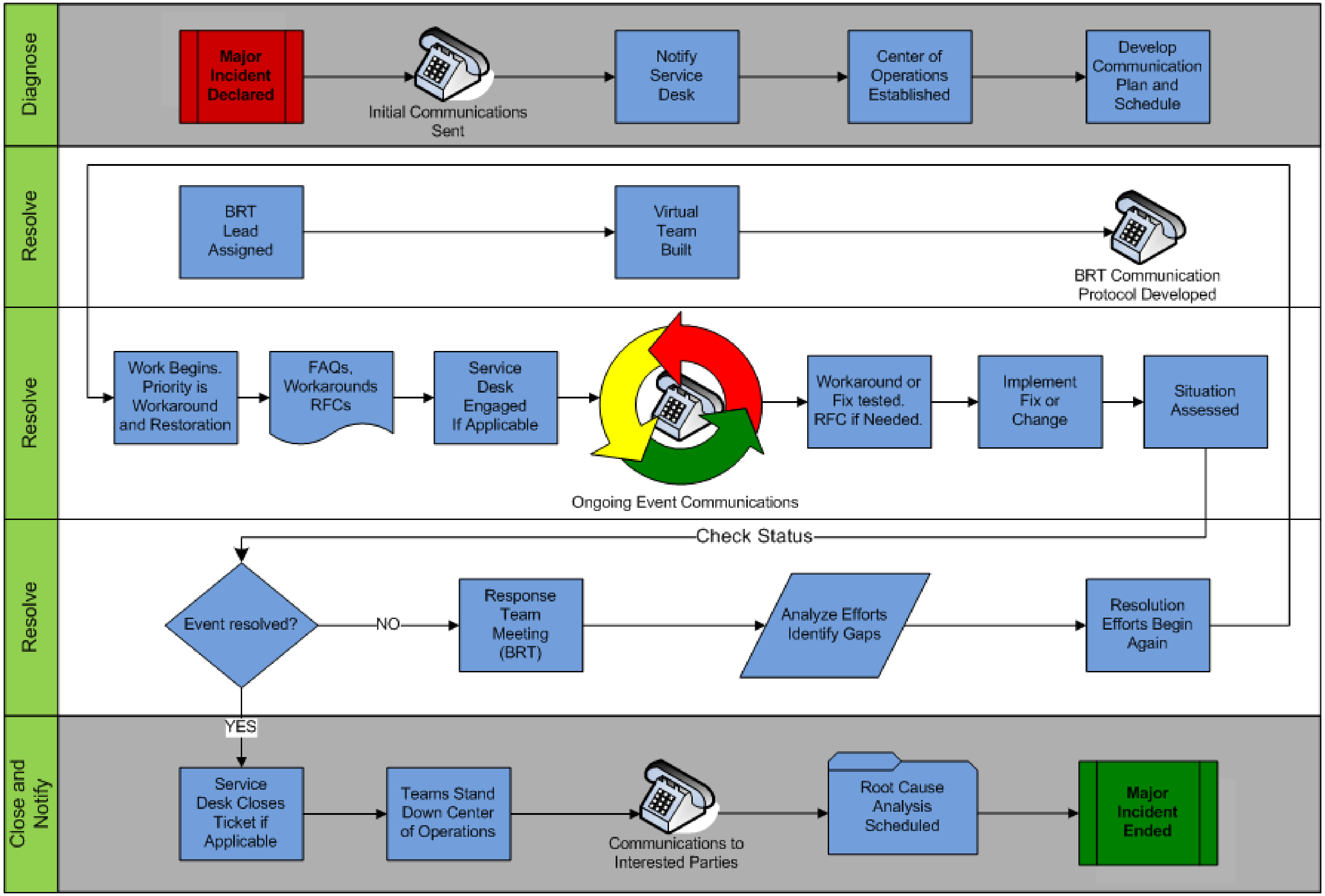
4. Merge onto **US-101 S** via the ramp on the left to **Interstate 10 Fwy E/Interstate 5 Fwy S**

5. Slight left onto **San Bernardino Fwy** (signs for **San Bernardino/Interstate 10 E**)

6. Continue onto **I-10 E**

7. Take exit **58A** to merge onto **I-15 N/Ontario Fwy** toward **Barstow/Las Vegas** Continue to follow I-15 N

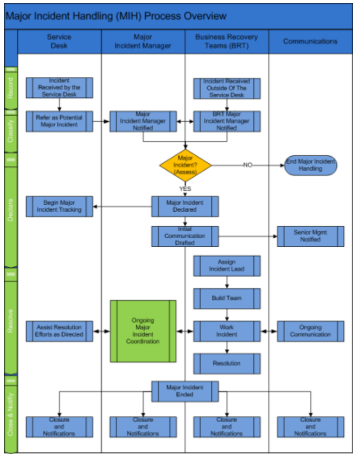
Major Incident Handling – Where Am I Going?

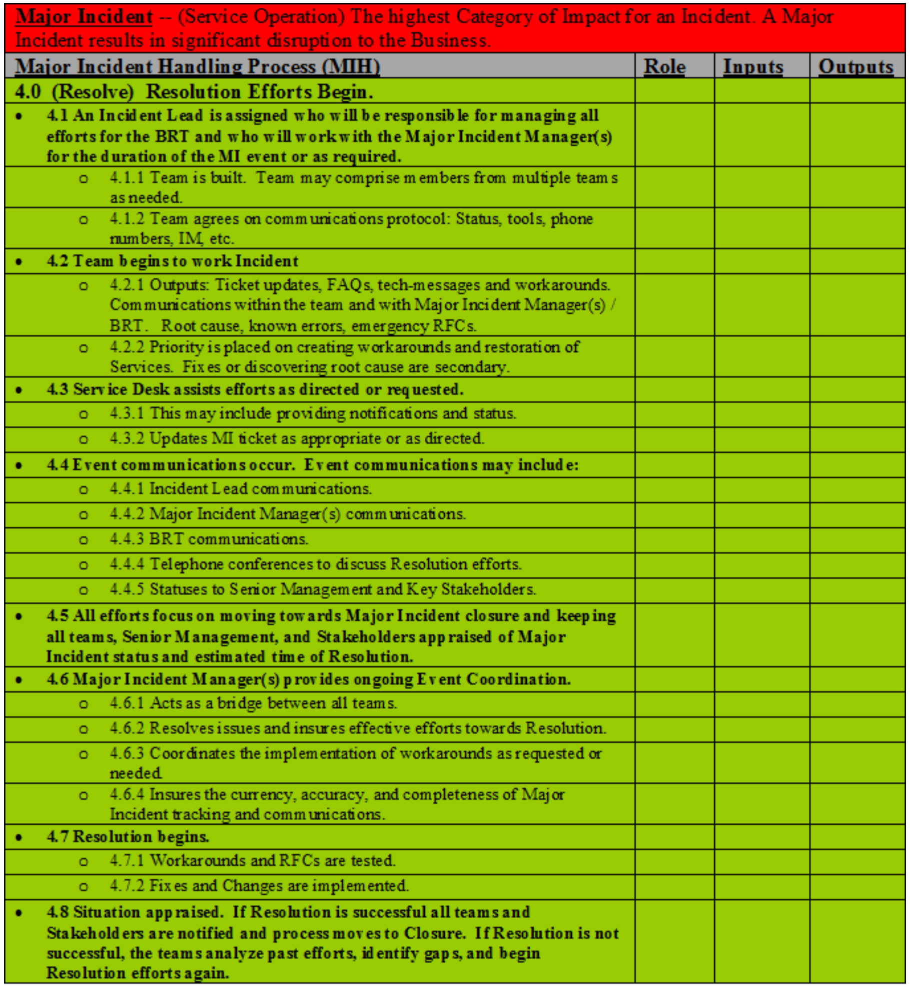

Diagnose
Major Incident Declared
Initial Communications Sent
Notify Service Desk
Center of Operations Established
Develop Communication Plan and Schedule
Resolve
BRT Lead Assigned
Virtual Team Built
BRT Communication Protocol Developed
Resolve
Work Begins. Priority is Workaround and Restoration
FAQs, Workarounds RFCs
Service Desk Engaged If Applicable
Ongoing Event Communications
Workaround or Fix tested. RFC if Needed.
Implement Fix or Change
Situation Assessed
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

itSMF CANADA

MIH Major Incident Handling

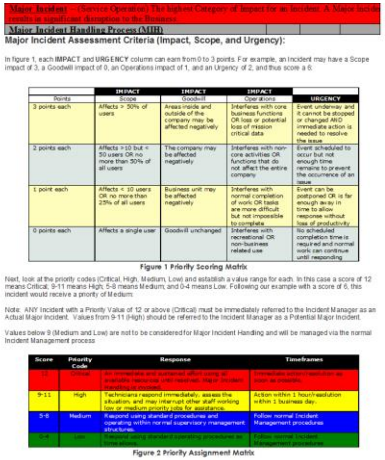
Major Incident Handling – How To Get There?


Major Incident Handling (MIH) Process Overview
Service Desk
Major Incident Manager
Business Recovery Teams (BRT)
Communications
Record
Classify
Declare
Resolve
Close & Notify
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



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)	**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 Major Incident Manager(s) for the duration of the MI event or as required.**			
o 4.1.1 Team is built. Team may comprise members from multiple teams as needed.			
o 4.1.2 Team agrees on communications protocol: Status, tools, phone numbers, IM, etc.			
• **4.2 Team begins to work Incident**			
o 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.			
o 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.**			
o 4.3.1 This may include providing notifications and status.			
o 4.3.2 Updates MI ticket as appropriate or as directed.			
• **4.4 Event communications occur. Event communications may include:**			
o 4.4.1 Incident Lead communications.			
o 4.4.2 Major Incident Manager(s) communications.			
o 4.4.3 BRT communications.			
o 4.4.4 Telephone conferences to discuss Resolution efforts.			
o 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.**			
o 4.6.1 Acts as a bridge between all teams.			
o 4.6.2 Resolves issues and insures effective efforts towards Resolution.			
o 4.6.3 Coordinates the implementation of workarounds as requested or needed.			
o 4.6.4 Insures the currency, accuracy, and completeness of Major Incident tracking and communications.			
• **4.7 Resolution begins.**			
o 4.7.1 Workarounds and RFCs are tested.			
o 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 -- (Service Operation) The highest Category of Impact for an Incident. A Major Incide 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

itSMF CANADA

MIH Major Incident Handling

Major Incident Handling – WIFM?

What's In It For Me?

- In the advent of a Major Incident having a well developed, trained and tested Major Incident Handling Procedures and Plan document will go a long way to ensuring that when individuals are called upon to respond they know exactly what they are to do, and just as importantly, they know exactly what they are not to do

- *This is the reason why the people who sit in the exit seat on airliners are given a second safety briefing prior to takeoff*

Contact

Braun Tacon
Info@MajorIncidentHandling.com
WWW.MajorIncidentHandling.com