Managing Critical Moments

Resources to support your organisation's response to crisis.

Contents

Introduction

Business Resilience when managing critical moments comprises of a number of different resilience disciplines including Incident Management, Emergency Management, Crisis Management, Business Continuity Management and IT Disaster Recovery:

- Incident Management focuses on the escalation and management of events which fall outside existing processes and/or systems; or, are considered by the organisation as warranting special management attention;
- Emergency Management focuses on the immediate response to an incident to manage time critical threats to the lives and safety of individuals; the protection of assets under threat; and, the risks of broader environmental impacts;
- IT Disaster Recovery/IT Service Continuity focuses on the response and recovery of IT systems and assets from significant outages, failures or degraded service;
- Business Continuity Management focuses on the capability of the organisation to continue delivery of products or services at acceptable, predefined levels – despite disruptive incidents – and to recover these services to a business as usual position; and
- Crisis Management focuses on the management of strategic impacts of incidents, such as severe financial losses; reputational damage; and / or, compromise to the organisations ability to achieve its strategic objectives or fulfil its mission.

These arrangements are typically built from facts and analysis collated in the form of a Business Impact Analysis, and are supported by Crisis Communications arrangements which spans all five disciplines.

While these resilience disciplines are discrete functions with distinct scopes, organisations must ensure that these functions operate effectively in concert, given the high likelihood of an incident triggering multiple arrangements concurrently. Where managed together, such as through a consolidated Organisational or Operational Resilience program, efficiencies may be achieved in staffing, response resources and shared functions (e.g. communications).

Executive Guide

Executive Considerations

Immediate Considerations

The (Not So) Basics

Many clients tell us that several key resources can make incident responses significantly easier if the following is in place:

- Up-to-date staff and critical third party contact lists (mobile phone is best).
- A clear approach to contacting staff during incidents, which includes a mix of personal and broadcast communications spanning multiple channels (email, automated SMS, call trees, town hall / all hands meetings).
- A plan which defines when, who, where and how a co-ordinated response will be initiated.

Priorities

Priorities for managing incidents vary significantly from organisation to organisation. It is important that wherever possible, your organisation's priorities are documented and well understood by the management team.

For example - based on our company values, we prioritise our staff safety and wellbeing – meaning an initial step in all our responses is to account for staff whereabouts, with operational impacts only being addressed once we have initiated an appropriate response to support those affected.

Longer Term Considerations

The Right Team

Crisis Management is a discipline which teams must learn and practice, to enact a smooth and coordinated response. A response to a crisis often requires managers and executives to lead with multiple styles, concurrently. For example, operational functions may require a high degree of decisiveness, whereas strategic decisions may warrant broad stakeholder consultation and nuanced communication. Many leaders take time to adjust to this change.

If possible, we recommend investing in the training and development of several potential leaders who may be able to guide and/or support the function of a management team if required. If the organisation does not have the ability to do this, we recommend appointing different leaders to manage operational and strategic impacts – while ensuring regular communication and collaboration between both groups takes place. This will assist in making sure each level of the response receives the appropriate focus where required.

Flexible Working Arrangements

Flexible working arrangements and technology supporting these practices provide organisations with a unique opportunity to distribute technology loads – minimising peak demand on hardware; minimising the impact of site or transport disruptions; and critically, providing staff with the space and time to manage other responsibilities related to family and community impacts around their work.

These practices cannot be implemented overnight, and retaining productivity through the transition takes both planning and careful change management. We recommend initiating a conversation around how remote working would be used if required with your technology, risk, human resources and operations team ahead of time to understand the likely challenges and opportunities. Further, staff should be clear on how remote working practices could be called upon if needed ahead of time.

Readiness Checklist

Where to begin

While one crisis might be over, future impacts from related, or separate events is still possible. We recommend all of our clients take proactive steps to ensure you are prepared to manage potential impacts both efficiently and effectively.

1 Be clear on management roles and responsibilities

Understanding key management and support roles for Crisis Management is central to an efficient and effective response. We recommend identifying and agreeing which key staff will lead your response efforts, each supported by an appropriately qualified and experienced alternate/back-up wherever possible. Organisations need to consider:

- Who will lead the Crisis and/or Incident Management Team? Note: Ideally, CEOs (or equivalents) should not chair or co-ordinate meetings due to common, competing demands during the incident (i.e. public representation, liaison with key stakeholders, regulators, etc.)
- Are critical functions represented in the team? For example: Legal, Technology, Operations, Finance, Insurance/Risk, Communications, Human Resources

2 Agree your organisational priorities

Crises must be managed in line with your organisational values – being to true to these is an important part of your response, particularly in your internal and external communications. Beyond prioritising people, many organisations face challenges in defining priorities for a response while experiencing the pressures of a crisis. Organisations need to consider:

- Is reliably poor service more important than an unreliable service?
- Could operating without typical resources jeopardise quality or safety? Or create unintended consequences which are worse than the incident itself (unmanageable backlogs or excessive credit risk)?

3 Know your exposure, and how impacts may manifest in your organisation

Many organisations do not have visibility of their most time-critical processes, key resources/inputs, interdependencies or their tolerances for disruptions to these. Additionally, many organisations are unsure how a severe disruption may manifest for them.

At an absolute minimum, executive groups should agree on a prioritised sequence for resource and process restoration following a disruption.

Refer to page 16 for a guide to a temporary Business Impact Assessment.

4 Plan to contact your staff quickly, and through multiple channels

During an incident, you may need to rapidly alert staff of safety-critical issues; or distribute messages and instructions to teams across the organisation as part of your response.

This requires careful planning and rehearsal for all businesses, particularly where communication is reliant on personal information. When an intermediary is involved (such as call trees), complexity in the delivery of the communications, and the opportunity for introducing risks of inconsistent messaging across key staff is greatly heightened.

If possible, we strongly recommend the use of multi-channel, rapid notification systems capable of SMS, Automated Phone Calls (text to voice) and email. At a minimum, key managers across the business should be able to rapidly contact their team when required.

Readiness Checklist

5 Update your plans, strategies and contact lists

While management decision making is a central part of any response, prepared resources serve to expedite responses and provide critical inputs to the process – namely, situational awareness and business intelligence. These inputs can assist with the sequencing, prioritisation and delegation of response actions in a timely manner – as well as the rapid analysis of impacts, including the identification of affected stakeholders.

Consider the following when reviewing your plan:

- Are you clear on when you will activate your plan?
  What is your threshold for activation, or tolerance for impact?
- How will you assemble the right people and resources to facilitate a response?
  Which communication mechanisms will you use, and what do you need with you to make informed decisions?
- How will you communicate with key stakeholders?
  How do you intend to communicate in the early stages of your response? (e.g. Templates, key messages, frequency)
- Does your plan balance the competing demands of:
  - Operations (including quality and continuity)
  - Reputation, Brand and Public Trust
  - Organisational Strategy, and
  - Risk and Compliance?
- Does your plan consider de-escalation of the incident, including the management of:
  - Outstanding actions
  - Financial accounting
  - Lessons learned; and
  - The management of protracted operational impacts (e.g. backlogs)?

6 Test your arrangements

By far the most effective thing an organisation can do to prepare for an event is to rehearse their response. At a basic level, this can involve management discussing a severe, yet plausible scenario; and, applying the resources they would expect to use in the event of a crisis – such as plans. These tests must include individuals with identified roles in the response, and ideally their back-ups.

We recommend choosing scenarios which create impacts to technology, third parties, people and critical assets (e.g. buildings, plant and specialist equipment), including discussion of:

- How the event may impact the organisation and its key stakeholders.
- How the event should be identified, and escalated to management.
- What external support is available, and how to access it if required.
- How to manage communications and engagement with key stakeholders.
- How to manage operational impacts, especially disruptions and/or service degradations.
- At what point (if any) the continuation of business functions/operations was no longer viable, and suspending business activities was preferable.

Tools & Resources

Crisis Management Meeting Agenda

1	**Initiation**	• Record attendance • Confirm roles and responsibilities • Confirm other resources/staff required for meeting
2	**Assessment**	• Time & Location • Incident Overview & Chronology • Critical impacts - People - Community/Environment - Operations - Stakeholders - Technology • Expected resolution horizon • Emerging issues • Progress - Actions taken - Actions in progress - Pending actions/needs - New requests for assistance - New problems
3	**Objectives**	Setting clear SMART goals for the meeting, and for the response. *Refer to the Strategic Impact Assessment*
4	**People**	• Staff, contractor and client safety and wellbeing • Employee assistance required • Resourcing needs for critical activities • Conditions, fatigue, travel, leave and pay
5	**Community**	• Community impacts • Assistance required • Resourcing needs for community support
6	**Clients & Customers**	• Client impacts • Operational resilience (incl. Business Continuity for service delivery) • Additional assistance required • Resourcing support
7	**Resources**	• People • Technology • Facilities • Specialist Assets • Third Parties • Impacts • Availability • Opportunities • Support requirements
8	**Operations**	• Continuity • Recovery • Resumption of Business as Usual
9	**Technology**	• Impacts • Performance
10	**Risk**	• Compliance • Insurance • Risk management in altered conditions/processes
11	**Communications**	• Stakeholders • Key messages
12	**Actions**	• Next steps • Action owners • Other business

Situational Awareness Report

The following template may be used to help assess the impacts of an incident, in conjunction with your organisation's risk management approach. This template may also be used at regular intervals to monitor changes, and re-assess impacts as they evolve.

Our Crisis Management Team use this template as a starting point for all meetings.

Incident Assessment Form	
Incident Date:	**Date of evaluation:**
Incident Summary:	
Person/s conducting evaluation:	

Assess Disruption

Consider the following	Details
Immediate: • What is the disruption? • How long has the issue lasted? • Which activities of the business are impacted? • Have any workarounds been employed? • Is the root cause known?	
Next Steps: • What will be done to fix the issue? • How long do we anticipate until the disruption stops its effect? • What resources are required to fix the issue?	

Determine Impacted Teams

(e.g. Department, Branch, Business Units)

Team(s)	Activities Impacted

Escalate

Action	Completed
Escalate disruption event to relevant parties.	◻
If required, activate Business Continuity Plan	◻

Strategic Impact Assessment

The following template may be used to help assess the strategic impacts of an incident, and set goals for recovery and response activities.

This template is often transcribed onto a whiteboard and filled in using post it notes. The board is visible to the entire Crisis Management Team, and is revisited periodically to track, adjust and celebrate progress.

	People & Community	Reputational Damage	Financial Loss	Legal & Compliance	Operations & Strategy
	• Staff • Customers • Suppliers • External	• Internal • Product • Key Staff	• Customers • Insurance • Grants	• Compliance • Litigation • Mandatory Reporting	• Operations • Customers • Supply Chain • Viability
Organisational Impact					
Stakeholders					
What do we know?					
What don't we know?					
What do we need to know?					
Owner & Action Timeframes	Name: Time:	Name: Time:	Name: Time:	Name: Time:	Name: Time:
Where do we want to be in 4 hours?					
Where do we want to be in 8 hours?					
Where do we want to be in 24 hours?					
Where do we want to be in 48 hours?					

Disruption Management Log

The following template may be used to track key events, decisions and actions taken by the management team in response to an incident. It is important to maintain standard meeting practices and governance activities even when the circumstances feel different.

Our Crisis Management Team often delegate the use of this log to an executive support staff member, or member of the legal team to ensure management team members can fully engage in the conversation.

Event Log			
Event Description			
Date and Time	**Actioned By**	**Event / Decision / Task**	**Recorded by**
14:00	*J. Smith*	*E: Reviewed impact assessment.* *D: Prioritise IT recovery over building repairs.* *T: J. Smith to liaise with CIO.*	*J. Nguyen*

Communications Planner

Many businesses find stakeholder management particularly complex during crises due to the variety of messages, stakeholder interests/needs and the volume of communication required to support an effective response. This template may be used to ensure coverage of key stakeholder groups; plan key messages; and allocate roles and responsibilities to key staff. Where possible, always engage with your communications team to help centrally coordinate your communications.

Stakeholder	Communication Method	Key Message	Responsibility	Timeframe
Example: Employees	1. Town Hall Meeting 2. Management Calls 3. Broadcast Emails	• Confirm Wellbeing • Situation Updates • Changed Conditions • Actions Required • Identify Other Needs • Identify Other Impacts	1. CEO 2. Line Managers 3. Human Resources	1. Fortnightly 2. Weekly 3. Daily

Always consider your communication principals:

1. Centrally Managed - One Source of truth
2. Leadership Voice & Ownership
3. Accuracy
4. Transparent
5. Timely & considered
6. Consistent
7. Clear Roles & Responsibilities
8. Manage the impact of Communications

Communications Ledger

This template assists with the tracking of communications by managers and is particularly useful in handovers between managers over the course of an incident.

Given the numerous stakeholders our business has, our Crisis Management Team use this to help schedule key executive activities, and to ensure coherency in external communications over the duration of the incident.

Date / Time	Communication Method	Recipients	Key Message/s	Next Update Due

Post Incident Report

Learning from incidents is just as important as effective management. This Post Incident Report can assist with identifying improvement opportunities and reporting on outcomes to key stakeholders – such as a board.

Post Incident Review	
Incident Summary	
Incident Date	
Person/s conducting evaluation	
Date of evaluation	

Agenda	Feedback
Key actions taken	
Strengths	
Opportunities for Improvement	

Key Actions	Owner
People	
Process	
Resources	
Technology	

Basic Business Impact Assessment

Understanding how an incident may manifest in your organisation, and your tolerances for outages is an important step in planning for a response and/or recovery.

This template does not replace a Business Impact Assessment, but may assist organisations as a temporary measure in the absence of one.

Step One:

Create a seven column list per the example below.

Step Two:

List business processes in the left-most column

Step Three:

List your organisation's tolerance for disruption to each process in the third column.

If this process was not operational, how long could it be suspended until an irreversible and/or severe impact would be sustained? (This is often referred to as a Maximum Allowable Outage, or Maximum Tolerable Period of Disruption)

Step Four:

In the third to seventh columns, list critical dependencies for each process, including:

- Other processes
- Key staff
- Technology
- Third Parties
- Assets (e.g. buildings, plant and specialist equipment)

Step Five:

Where dependencies appear multiple times, mark the lowest Maximum Allowable Outage value of any reliant process in brackets beside it.

		Dependencies				
Process	MAO	Other Processes	Key Staff	Technology	Third Parties	Assets
Example: Stakeholder Comms	*2 Hours*	*N/A*	*Media Officer Spokesperson*	*SocialMonitor Email Contacts CRM*	*MediaMonitor MailDelivery+*	*High-Spec Design PC*
Example Payroll	*13 Days*	*Treasury (4 hrs)*	*Payroll Officer CFO HR*	*E-Bank ERM System Timesheet+ Email (2 hrs)*	*A-Bank ABC Staffing*	*Bank Token PC*

For ease of use, you may wish to plot processes and dependencies on timelines based on the urgency and priority of their recovery.

Contacts

For further information regarding Resilience support for your organisation, please contact:

Akhilesh Tuteja
Partner and Head
Risk Consulting - KPMG in India
Co-Leader Global Cyber Security
T: +91 98710 25500
E: atuteja@kpmg.com

Ritesh Tiwari
Partner and Head
Risk Consulting Markets
KPMG in India
T: +91 85888 62899
E: riteshtiwari@kpmg.com

KPMG.com.au