Crisis Management Guideline

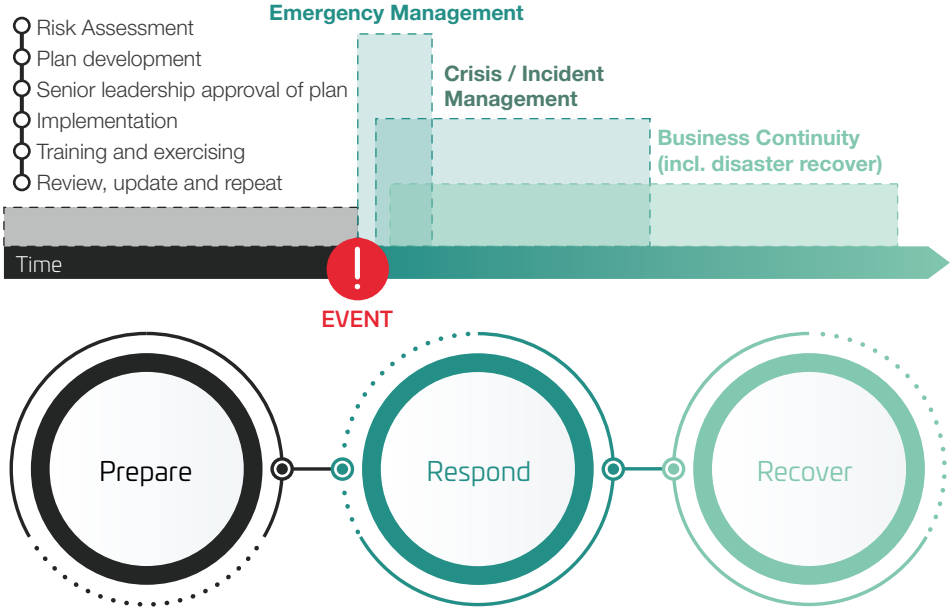**Introduction to Best Practice**

Introduction

Crises are the most serious challenge facing any organisation. While crises may be caused by a range of different events the common factor is that they present organisations with complex challenges that could have far-reaching and very damaging consequences, particularly if an organisation is perceived as having failed to prepare for, manage or effectively recover from a crisis. In the worst case a crisis may threaten the continued viability or existence of an organisation.

This Crisis Management Guideline, which draws from and is aligned with an internationally recognised standard for best practice (BS 11200:2014 Crisis Management Guidance and Good Practice), aims to provide insureds with a basic introduction to the core tenets of crisis management.

Embedding Crisis Resilience

Effective crisis resilience consists of several activities and inter-connected disciplines. Some of the most critical activities should be undertaken before an incident occurs, for example undertaking risk assessments to then inform crisis and emergency management team planning, training and exercising.

If an adverse event occurs one or all of three disciplines may then commence, albeit not necessarily simultaneously and to varying degrees of duration and intensity – emergency management, crisis management and business continuity.

Emergency Management

Crisis / Incident Management

Business Continuity (incl. disaster recover)

- Risk Assessment
- Plan development
- Senior leadership approval of plan
- Implementation
- Training and exercising
- Review, update and repeat

Time

!
EVENT

Prepare

Respond

Recover

Senior management buy-in and support is critical to successfully developing, implementing and maintaining an effective crisis resilience programme, as well as a commitment to appropriate resourcing.

Definitions

In its simplest form crisis management is the development and application of an organisational capability to deal with crises. Organisations use different definitions when talking about crisis management, emergency management and business continuity. This guideline uses definitions taken from the BS 11200:2014 Crisis Management Guidance and Good Practice standard.

Emergency

An unplanned situation with the potential to cause limited damage that can be managed through existing plans and procedures using local resources at the point of the event

An emergency is an adverse situation - likely contained at site-level and without wider implications for an organisation - that can be managed by on scene personnel and an Emergency Management Team (EMT) using the resources and plans readily available to them, escalating where additional support or management input is required.

Incident

Adverse event that might cause disruption, loss or emergency, but which does not meet the organisation's criteria for, or definition of a crisis

Where a serious adverse event occurs that does not meet the definition of a corporate level crisis then an Incident Management Team (IMT) might convene as a regional or operating unit level in place of or in addition to a Crisis Management Team (CMT) at corporate level.

Crisis

An abnormal or unstable situation that threatens the organization's strategic objectives, reputation and/or viability

A crisis involves a significant and ongoing event which manifests itself at a strategic level and requires a Crisis Management Team to convene at a senior management level.

Business continuity

The capability of an organisation to continue delivery of products and services at acceptable pre-defined levels following a disruptive incident

Business continuity refers to pre-defined actions that are taken to limit and control business disruptions (for example, business critical IT systems / data), and to recover from them within an acceptable timeframe and cost.

Potential causes of a crisis

Natural disasters /environmental events / spills

Instability

Serious life safety or security event

Organizational misdeeds

Cyber compromise

Major business interruption event

What are organisations trying to protect?

Every organisation will have a different view of what constitutes a crisis and what it will seek to protect should one occur. Most organisations however will be seeking to protect their:

- ✓ **People** – the wider public and employees

- ✓ **Environment** – operating, social and natural

- ✓ **Assets** – intellectual and physical

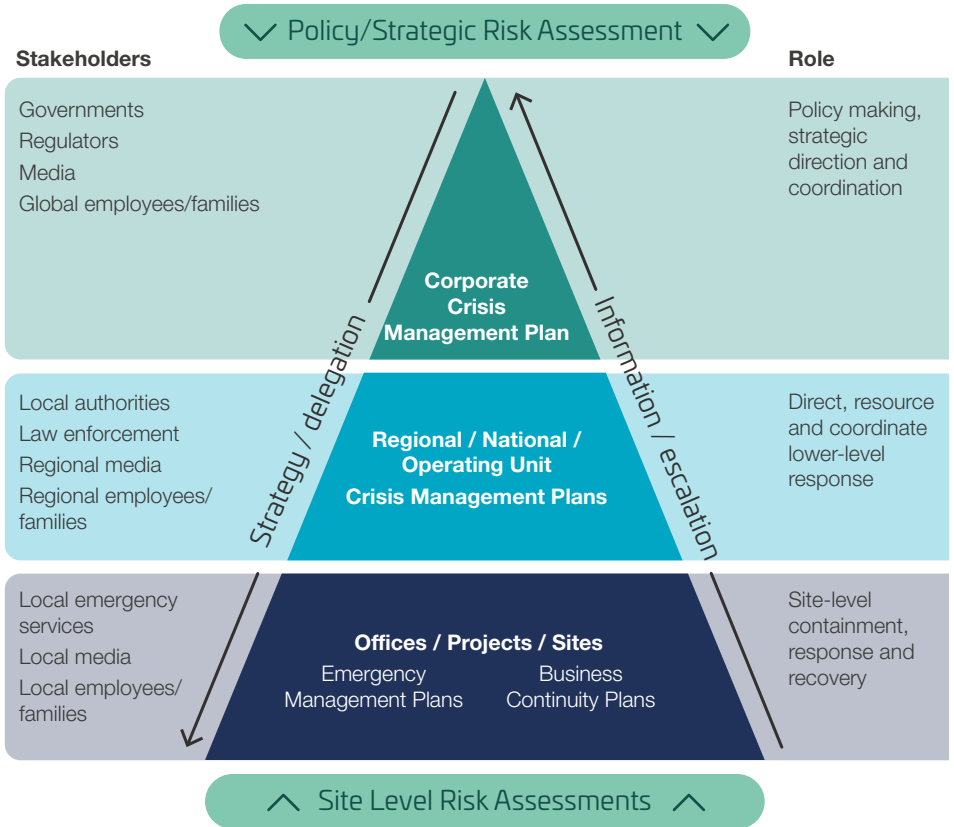- ✓ **Reputation** – brand and organizational standing with wider society

- ✓ **Stakeholders** – customers, partners, communities, investors, regulators

Crisis management structure

Every organisation is different meaning it is necessary to determine in advance the appropriate structure for managing crises (and by extension the different levels of crisis plans and teams required).

An example structure is shown below:

Policy/Strategic Risk Assessment

Stakeholders		Role
Governments Regulators Media Global employees/families	**Corporate Crisis Management Plan**	Policy making, strategic direction and coordination
Local authorities Law enforcement Regional media Regional employees/families	**Regional / National / Operating Unit Crisis Management Plans**	Direct, resource and coordinate lower-level response
Local emergency services Local media Local employees/families	**Offices / Projects / Sites** Emergency Management Plans — Business Continuity Plans	Site-level containment, response and recovery

Strategy / delegation

Information / escalation

Site Level Risk Assessments

Best practice

A number of key principles are at the heart of building effective crisis resilience, as demonstrated by organisations that have responded effectively to crises:

- **Risk-based:** any crisis resilience programme should be risk-based, in other words predictated on a dynamic risk assessment at each level of the organisation's crisis management structure (including an enterprise-level risk register).

- **Buy in:** crisis resilience programmes are most effective where there is clear organisational 'buy in' with appropriate commitment, leadership and subsequent programme implementation starting with senior management.

- **Organisational policy:** the approach to crisis management within an organisation should be established in a policy document which details the overall approach to crisis management, aims and objectives, the crisis management structure, and a summary of the key decision-making structures that apply.

- **Systemic:** Organisations should adopt a structured approach with regards the design, roll out, implementation and ongoing maintenance of their crisis resilience capability.

- **Planning, training, exercising and review:** any effective crisis resilience programme should be supported by a regular programme of training, exercising, audit and review. This should be progressive, ultimately to incorporate the testing of interoperability of plans and teams at different tiers of the crisis management structure.

Principles of effective crisis management

Recognised best practice is that an organisation's preparation for, response to and recovery from a crisis should be consistent with the following principles (BSI Crisis Management Guidance for Developing a Strategic Capability, 2018):

- Seek understanding of the situation.
- Achieve control as soon a possible.
- Communicate effectively, internally and externally, and with empathy.
- Be prepared with clear, universally understood structures, decision making processes, roles and responsibilities.
- Build situational awareness through good information management and coordinated working.
- Have a clear and well-rehearsed decision-making and action driving process in line with core values ad objectives of the organisation.
- Implement effective leadership at akll levels of the organisation.
- Ensure people with specific crisis management roles are familiar with relevant plans and process and competent through appropriate training and exercising.
- Maintain a comprehensive record and policy log of all decisions taken, including the facts known at the time, any assumptions made and the basis for those assumptions.
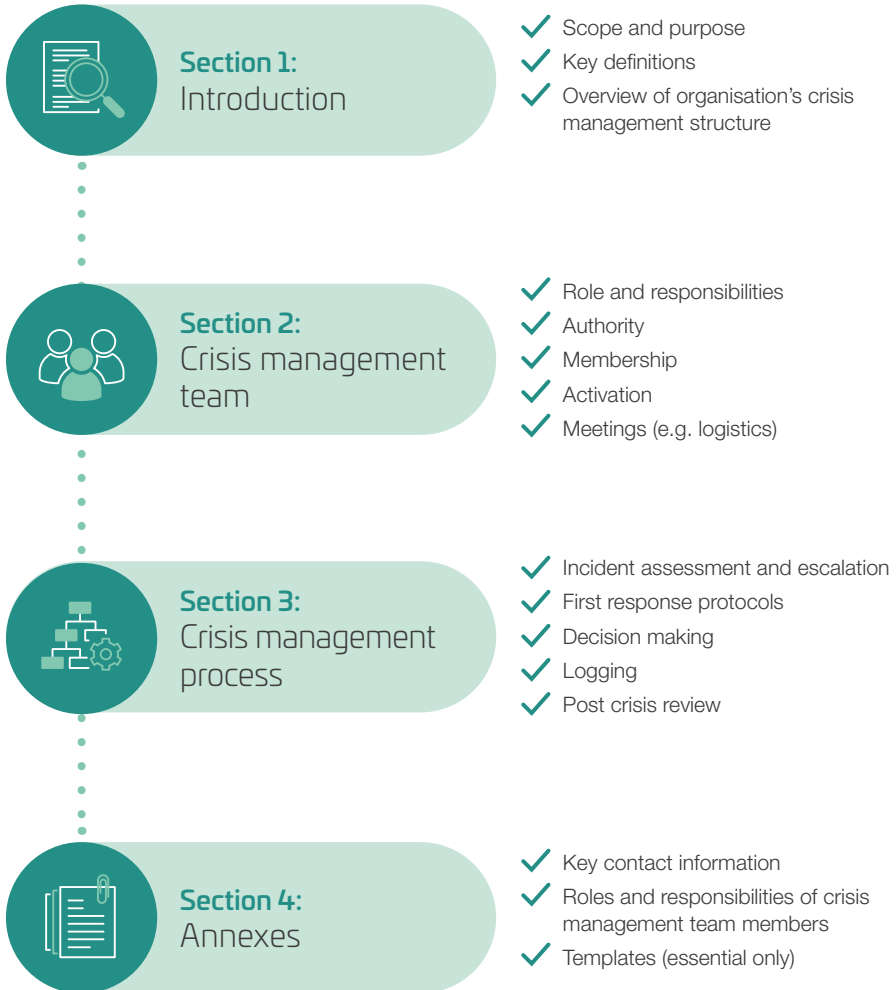- Learn and evolve from experience of actual events, successes and failures.

Crisis management plans

Current
Up to date, trained and exercised against, and based on a dynamic risk assessment

Concise
Concise enough to be reviewed in less than 15 minutes with focus on key processes and details

Communicated
To those with any role or responsibility in the plan or crisis management team

Clear
No extraneous detail or content so they are actually useful in a crisis

Consistent
With the organisation's wider structures and other crisis and emergency plans

Organisations should ensure that crisis management plans are simple and easy to use as follows:

Information relating to policy, or detailed emergency procedures or recovery plans (e.g. kidnap response or crisis communications plans), should be contained elsewhere or exist as separate documents.
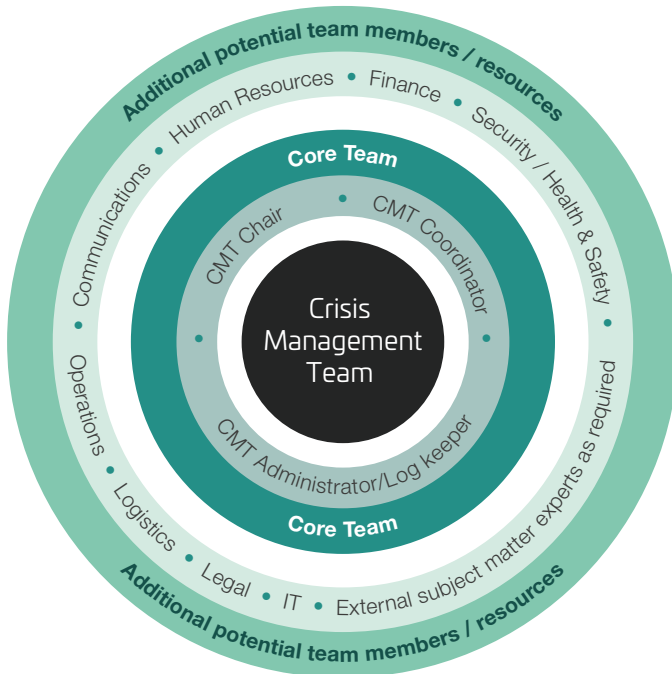
Below is a generic structure but any plan should be configured to the specifics of the organisation:

Section 1:
Introduction

- ✓ Scope and purpose
- ✓ Key definitions
- ✓ Overview of organisation's crisis management structure

Section 2:
Crisis management team

- ✓ Role and responsibilities
- ✓ Authority
- ✓ Membership
- ✓ Activation
- ✓ Meetings (e.g. logistics)

Section 3:
Crisis management process

- ✓ Incident assessment and escalation
- ✓ First response protocols
- ✓ Decision making
- ✓ Logging
- ✓ Post crisis review

Section 4:
Annexes

- ✓ Key contact information
- ✓ Roles and responsibilities of crisis management team members
- ✓ Templates (essential only)

Crisis management teams

A Crisis Management Team (CMT), irrespective of what level of an organisation it is convened at, should be limited to essential individuals only to allow for rapid decision making, with a focus on a member's role on the team rather than their position in the organisation.

The composition of a CMT will vary according to the organisation and the crisis scenario, but would normally consist of a core team that is supplemented by additional relevant functions and resources the incident requires:

Additional potential team members / resources

Human Resources • Finance • Security / Health & Safety • External subject matter experts as required • IT • Legal • Logistics • Operations • Communications

Core Team

CMT Chair • CMT Coordinator • CMT Administrator/Log keeper

Crisis Management Team

Business continuity

The objective of Business Continuity Management (BCM) is to limit and control business disruptions following an event, and to recover from them by restoring normal operations within an acceptable timeframe and at reasonable cost. Business continuity will cover and/or link to a spectrum of other plans (for example IT disaster recovery plans, and crisis management and emergency management plans).

In line with Business Continuity Institute (BCI) Good Practice Guidelines 2018 edition and this Standard, Business Continuity Plans (BCPs) should be prepared for all of an organisation's services, sites and infrastructure. Before a BCP can be prepared however, a Business Impact Analysis (BIA) and Risk Assessment should be completed.

Key stages in business continuity planning

Undertake a documented Risk Assessment process that systemically identifies, analyses and evaluates the risk of disruptive events to the organisation

Identify key business functions (e.g. IT or finance)

Business functions undertake a BIA to identify risk scenarios and the critical processes required to meet miminum service levels to ensure business continues

Functions review critical processes against each scenario to determine mitigating activities required to maintain service levels
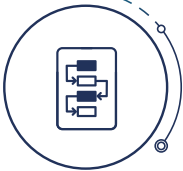
Using outputs from the BIA and Risk Assessments, develop Recovery Plans to include within a BCP.

Convex Insurance UK Limited

52 Lime Street, London EC3M 7AF
+44 203 886 0560

Convex Re Limited

Point House, 6 Front Street, Hamilton HM 11, Bermuda
+1441 232 0112

Convex Europe S.A.

37 Boulevard Joseph II,2ème étage,
L-1840 Luxembourg,Grand-Duchy of Luxembourg
+352 27 86 22 76

convexin.com