Guidance Note

Crisis Management

The occurrence of a "sudden emergency situation" is by definition outside the control of an organisation. However, the response to such an event is not. How an organisation responds to a crisis may have more impact on their reputation, revenue, and resilience, than the crisis event itself.

In the same way that a person only has one chance to make a first impression, you only have one chance to manage your initial response to a crisis. If your first thoughts are "What do we do now?", then it's probably already too late.

A hard-earned reputation can be destroyed very quickly – as Gerald Ratner can testify. It is generally accepted that BP mishandled the corporate communication surrounding the Deepwater Horizon oil spillage. Whereas, Alton Towers received praise for it crisis communication and sensitive handling of a rollercoaster crash in 2015. The management of a crisis is often what people remember, rather than the details of the crisis event itself. Planning your response around likely scenarios is key to how you respond when a crisis does occur.

In managing a crisis, communication is vitally important.

"Be quick, honest, open and, in such circumstances, be compassionate in communications, these are the key principles of crisis management," says Julia Graham, deputy chief executive of Airmic, the UK's risk management body.

Crisis management planning is considered an important part of an organisations resilience and should be included in the framework of Business Continuity Planning and Enterprise Risk Management.

Crisis:

The British Standards Institution (BSI) defines crisis as an "abnormal and unstable situation that threatens the organisations strategic objectives, reputation or viability."

Crisis Management: - There are many definitions of Crisis Management, the simplest of which is - "The process by which a business or organisation deals with a sudden emergency situation."

Crisis Communication: - This is a sub-speciality of Crisis Management and can be defined as "The collection, processing and dissemination of information required to address the crisis situation".

ecclesiastical

There are effectively four elements to a Crisis Management Plan (CMP)

- Assessment
- Planning
- Execution
- Recovery

Assessment

Every organisation will face its own particular risks, although there will be some risks that are common to most organisations such as fire, flood and security. An open and honest analysis of the realistic worst-case scenarios is required. Some risk have potential to cause significantly more damage depending on the type of organisation. For example, reported embezzlement would be more detrimental to a charity organisation, than to a ball bearing factory.

Risks generally fall into six categories,

- **Strategic** – Re-organisation, change of leadership, diversification.
- **Operational** – Loss of a critical system, business interruption, service delivery failure.
- **People** – Personal injury, employee relations, pandemic.
- **Regulatory** – GDPR breach, non-compliance, governance.
- **Financial** – income, fraud, fundraising.
- **Hazard** – Fire, flood, environment.

These should be low frequency/high impact events, all of which have potential to cause lasting reputational and financial damage.

When considering risks that have a crisis potential, a traditional risk assessment approach, considering both risk likelihood and consequences, existing risk control measures and the residual risk may have limitations. Risk control measures may fail, particularly if there is a human element involved and unlikely events can still occur. Therefore when assessing the crisis risks, organisations should still consider those events/situations that could have the most serious consequences, even where the likelihood of occurrence is deemed to be low.

It is beneficial to have input from a cross section of internal stakeholders, as well as external expertise when undertaking the assessment part of the process. External expertise could include risk consultants or insurance brokers, who can provide a critical and unbiased assessment of the organisation and identify specific vulnerabilities.

Planning

A key part of the planning process is to use standard risk assessment and mitigation processes to avoid being caught up in a crisis in the first instance. For example, in the case of fire risk, ensure that there is a Fire Risk Assessment carried out annually and that all action points arising are addressed in a timely manner. In the case of personal injury to staff or public, ensure there is suitable health & safety policy, appropriate task based risk assessments, staff training and premises/ equipment maintenance regimes.

Essentially, you should do all that is reasonably practicable to reduce known risks to your business/ organisation. This includes testing the resilience of your IT systems.

Nevertheless, despite taking all reasonable precautions, the risk of a "sudden emergency situation" may still remain. Having assessed the residual risk, your organisation may decide that it does not have the expertise to manage a crisis and in those circumstances, you may decide to outsource the function. There are many companies that can provide a suite of crisis management solutions and you will be able to choose those that are right for your organisation. It is recommended that you look to use companies that specialise in your particular sector.

If you consider that you would prefer and are able to handle a crisis internally, then the following should apply.

Crisis Management Planning Team

Firstly, a crisis management team should be formed, with appropriate levels of authority, experience and expertise. The team should include representatives from Senior Management, Human Resources, Legal, IT Services, Finance, General Operations, Site Facilities, and Communication/PR.

The function of the team is to:-

- Act as the decision making authority
- Develop the procedures on how to handle the Crisis
- Establish and maintain a crisis management suite that will have the necessary equipment available for rapid activation during an emergency. The equipment includes communications equipment, emergency plans and procedures, a log to record all actions taken during the crisis, necessary office equipment/supplies.
- Distribute the CMP to all employees so that everyone is aware of their roles and responsibilities.
- Test, review and update the CMP, to ensure that names and contact details are accurate and that the document still reflects the likely crisis scenarios.

We are aware of one organisation whose CMP failed upon testing, as it was discovered that the IT system was not backed up. Unbeknown to management an IT service contract had lapsed and cloud storage was not in place. Were it not for testing the CMP, this may not have been discovered.

The Crisis Management Plan

With so many potential crises, it is unlikely that a single CMP will be suitable for all circumstances. There should be at least one formal documented procedure for each of the categories. There will however be a number of actions that are common to all CMPs. The following points should be considered when completing a CMP.

- Activation guidelines – not every serious incident requires full crisis management.
- Tasks and roles should be appropriately designated to named staff.
- Outline a chain of command and allocate decision-making authority.
- There should be an agreed high level strategy to deal with each crisis situation.
- There should be pre-determined actions for individuals to undertake to support each strategy.
- There should be a person identified within the organisation to act as media spokesperson.
- Create a Response Log and designate an individual to manage this. Consider how the log can be managed without access to premises and IT systems.
- Identify internal & external stakeholders and establish your notification/communication system – For example in the case of education establishments - how, when and who will communicate with media, police, local authority, parents, pupils, lawyers, insurers, governors, trustees etc. Again, consider how this could be done without access to Premises and IT systems. Do you have contact details backed up elsewhere?
- Development holding statements, whilst remembering to be "quick, honest, open and compassionate."
- Manage the social media impact. A full review of social media impact is beyond the scope of this document, suffice to say it is crucial to take control of the narrative and do not leave an information vacuum. Ensure that you can get your messages out on all appropriate sources, e.g. Twitter, Instagram, Facebook, LinkedIn etc. Be clear who and how this will be done in the event of no access to premises.
- Identify back- up resources, in particular in IT services.

The CMP should integrate with Business Continuity Planning, Emergency Services Management and Disaster Recovery plans.

Business Continuity - Business Continuity Planning is concerned with keeping business operations running - perhaps in another location or by using different tools and processes - after a disaster has struck.

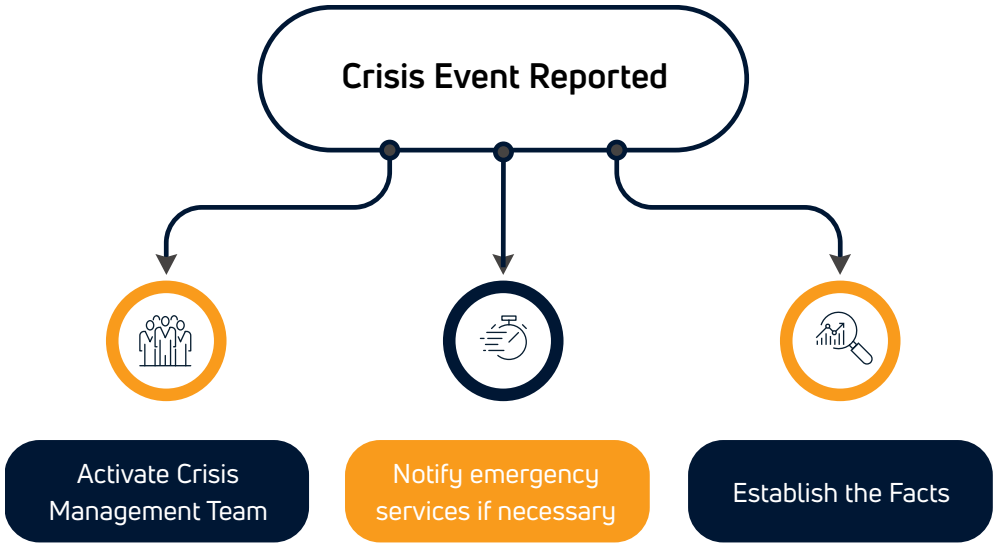
Emergency Services Management – This outlines how your organisation will liaise and manage the emergency services team should they be required in the event of a crisis. Site plans should be made available.

Disaster Recovery – The primary objective is to restore normal business operations after a disaster has struck, whether that be Premises related, IT or Personnel.

Execute Plan

Once a crisis has been reported/identified, it is crucial that the CMP is implemented without delay. The CMP team should convene, whether physically or remotely and address the following:-

- Strategy – How could this crisis damage the organisation? What is the best and worst case scenarios and how can loss and damage be mitigated.
- Priorities – What are the immediate priorities – is everyone safe?
- Evidence gathering should commence
- Implement the appropriate CMP



Who	Immediate action - first hour	Short term action - first 24 hours	Medium term action - following few days
Senior Management	Ensure safety of employees & public.	Set up formal investigation. Cooperate fully with emergency services.	Complete investigation and share the findings and action plans.
Designated coordinator	Commence Incident Response log.	Maintain the log and update the team.	Retain the log for evaluation of CMP.
Senior Management	Agree a factual statement and notify all stakeholders, including Insurers.	Issue an update and commit to a timeline for further updates.	Consider the need for external assistance e.g. psychological support.
Media spokesperson	Take control of narrative.	Remain in touch with media.	Update on investigations and action plan. Accentuate the positives.
Designated personnel	Monitor Social Media and feedback to senior management.	Monitor Social Media and feedback to senior management.	Monitor Social Media and feedback to senior management.

Recovery

There are essentially four elements to recovery following a crisis:

- Physical – e.g. building reinstatement. This will be arranged in conjunction with Insurers, Loss Adjusters, Builders, Architects and other appropriate professions.
- Financial – Was it an insurable loss? Many insurance policies do not cover terrorism or cyber-attack as standard. Is there adequate Business Interruption cover in place? In the event of a fire, your Maximum Period of Indemnity should be long enough to allow for the building reinstatement and the time it would take the organisation to be back trading at the same financial level as they were before the fire. It may take two years to reinstate a building but much longer to recover your customer base.
- Reputational – The goal here is to minimise the long term reputational impact to the organisation or even enhance your reputation by demonstrating that the incident was well managed during and after the event. The length of time it takes an organisation to recover to a pre-crisis financial level, will, in part, be determined by its success or otherwise in minimising reputational damage. In the aftermath of a crisis, organisations will have opportunities to accentuate the positives, apologise for failures and commit to remedial actions. Again, pro-active managing of media/social media is essential. Use all appropriate means to get your positive message out there.
- Review – lessons to be learned. This is an opportunity to assess the damage. What worked well and what did not. In hindsight, what would you do differently? In terms of personnel, did some emerge as natural leaders, with others, were there training opportunities identified?

Conclusion

The reality is that there are many serious threats that can adversely affect organisations of any size, including terrorism, cyber-attacks, sexual abuse, in addition to the more traditional fire, flood etc. Doing nothing is rarely a good strategy in mitigating the impact. Time spent planning and testing for a crisis is never wasted. It lets your employees and external stakeholders know that you have a robust risk management attitude, teamed with a culture of resilience. Remember you only have one chance to manage that initial response. Crisis management planning will help you make to most of that opportunity.

Need to contact us?

For further advice Ecclesiastical customers can call our Risk Management Advice Line on **0345 600 7531** (Monday to Friday 09:00 to 17:00, excluding Bank Holidays) or email us at **risk.advice@ecclesiastical.com** and one of our experts will call you back within 24 hours.

ecclesiastical

Proudly part of the BENEFACT GROUP

Ecclesiastical Insurance Office plc (EIO) Reg. No. 24869. Registered in England at Benefact House, 2000 Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom. EIO is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 113848.