BlackBerry
Intelligent Security. Everywhere.

White Paper

Best Practices in Crisis Management

Communications Planning

BlackBerry AtHoc

At the time of this publication, the world was in the midst of an unprecedented global pandemic event: COVID-19[1] . While governments and organizations across the world were expected to have a pandemic response plan in place, having learned from past experiences with SARS, H1N1 and the MERS-COV, this particular pandemic stretched limits and challenged any previous planning assumptions regarding business and supply chain disruptions.

It also introduced challenges around equipping staff and critical vendors with personal protective equipment (PPE) and adhering to workplace safety and health guidelines. Planning parameters that were based on anticipated resurgence waves, a limited and contained timeframe, and cross-border transmissions all strayed off-course as the situation evolved. It is a crisis affecting every country, organization, as well as individuals, that escalated exponentially within a short period of time.

Despite navigating the challenging circumstances and variables, whether it's in a global pandemic or other critical incident where a crisis management is required, organizations and communities can have better control during the initial phase of an event and thus minimize preventable confusion amongst stakeholders with good planning.

The purpose of this paper is to assist organizations in reviewing their current resilience and crisis management plans through better awareness of established frameworks and practices, offer recommendations in crisis management plan development, recognize the challenges in communicating and executing established plans, and consider available options for enhancing crisis communications.

1 World Health Organization (WHO) Director-General's opening remarks at the media briefing on COVID-19 (11 March 2020)

Role Of Communications In Crisis Management

Crisis management is a holistic process that identifies potential impacts that threaten organizations and communities. It provides a framework for creating resilience with the capability for an effective response that safeguards the interests of the organization's key stakeholders, reputation, brand and value-creating activities, as well as effectively restoring operational capabilities[2]. The scope of crisis management can vary between organizations depending on their industry, business structure, and size. While it may be viewed as a strategic/management level response in larger organizations for major incidents, such as after the activation of operational and tactical level response teams, it may also serve as the one and only management response in smaller or leaner organizations by encompassing everything from emergency response for possible scenarios through business continuity recovery.

An essential component in any crisis management plan is a well thought-out communications process that addresses stakeholder concerns, the mobilization of scarce resources, and demonstrates management command and leadership during the course of the crisis. Depending on where and who a crisis may impact, the details of the plan may be designed according to the relevant crisis management frameworks adopted.

Key components to the communication process in crisis management

Address
stakeholder concerns

Mobilize
scarce resources

Demonstrate
management command and leadership

2 ISO 22300:2018 (Security and Resilience - Vocabulary) (February 2018)

Crisis Management Frameworks

Crisis management can be undertaken in three phases: the preparedness phase, the response phase, and the recovery phase.

For each phase, the communication process and delivery may vary depending on the demographics as well as the desired outcome expected of the stakeholders. Globally, governments, organizations, businesses in regulated sectors and specific communities may adopt or be subjected to sector-specific or "best practice" frameworks in designing their crisis management plans.

These frameworks and plans may be built upon established resilience guides or standards. For reference, the following common standards and guides are summarized: *Federal Emergency Management Agency (FEMA), Business Continuity Institute (BCI), and ISO 22301:2019 (Security and Resilience – Business Continuity Management Systems - Requirements):*

FEMA's Comprehensive Preparedness Guide 101[3] (CPG 101) is the foundation document for planners at all levels of the government in developing their emergency operations plan (EOP). Planners in other sectors and domains may also adopt the guidelines of CPG 101 in developing their EOPs. It promotes a common understanding of the fundamentals of risk-informed planning and decision making to help planners examine a hazard or threat and produce integrated, coordinated, and synchronized plans. CPG 101 provides methods for planners to: conduct community-based planning according to the actual population in the community and seeks the involvement of community leaders, ensure plans are developed through an analysis of risk, identify operational assumptions and resource requirements, prioritize the planning efforts to support the seamless transition from development to execution for any threat or hazard, and, integrate and synchronize efforts across all levels of government.

3 FEMA – "Developing and Maintaining Emergency Operations Plan", Comprehensive Preparedness Guide 101 – Ver 2.0 (November 2010)

BCI's Good Practice Guidelines[4] (GPG) advocates the adoption of a business continuity management lifecycle as a framework in designing and implementing a business continuity program within the organization through six "professional practices" (PP), namely: policy and program management, embedding, analysis, design, implementation, and validation. Each PP provides specific guidance for organizations to develop a resilient framework (example, conduct of risk assessment and business impact analysis, concepts in designing recovery strategies, consideration factors in developing tests and exercises, etc.).

ISO 22301:2019 – Business Continuity Management Systems Requirements[5] is a document specifying requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of, the occurrence of, prepare for, respond to, and recover from disruptions when they arise. The requirements specified in this document are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.

These three referenced standards and guides adopt the common framework approach of preparedness, response and recovery. Key activities such as risk and threat assessment, impact assessment, resource allocation planning (including supporting resources), incorporating planning assumptions, identifying stakeholder roles and responsibilities, establishing an escalation process, prioritizing response actions, determining an incident "stand down", and conducting after-action reviews, are evident in these documents.

The difference in these standards and guides would probably be in the prescribed format and structure in crafting a crisis management plan as well as the focused intent. While FEMA's CPG 101 advocates three different (and detailed) formats for consideration in designing a single EOP with greater emphasis on adopting a "all hazards" threat assessment and response approach in responding to emergencies, BCI's GPG as well as the ISO 22301 focusses more on managing the consequences and continuity of operations following a business disruption (regardless of incident severity). FEMA's CPG 101 may also be deemed as the "industry standard" in crafting crisis management plans primarily involving federal, state or local governments and associated stakeholders within America, while the other two standards and guides can be considered as "widely adopted" outside the country.

For organizations seeking to acquire certification for their business continuity management system, the ISO 22301 will be the required standard for all to adopt.

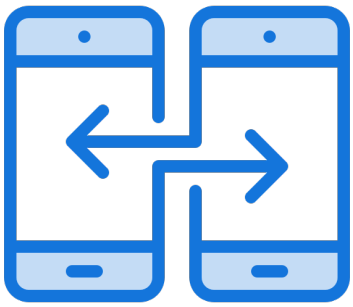
---

4 BCI "Good Practice Guidelines (2018 Edition)" (2017)
5 ISO 22301:2019 (Security and Resilience – Business Continuity Management Systems - Requirements) (October 2019)

In summary, regardless of the standards or guides adopted, an effective crisis management framework will involve the presence of strategic, operational and tactical level plans; is able to integrate with other relevant plans and policies; focuses on the impact (rather than every available scenario for resource efficiency); facilitates on-going situational and risk assessment; incorporates an escalation mechanism in the swiftest form; provides for collaboration; and, includes a reliable communications process including dedicated platform(s) for critical messaging and information delivery.

Further details on these standards and guides as well as its impact on communications can be found in ANNEX A.

Crisis Communications In Practice



Communications is crucial at the onset of any incident. Critical information shared in the initial phases with the relevant stakeholders will aid in subsequent incident (or crisis) management initiatives.

Within the aviation industry, for example, when air traffic controllers receive an emergency request by the pilot of an incoming (or diverted) aircraft, a series of well-coordinated activities will be executed in accordance to the Airport Emergency Plan. Besides alerting the airport fire and rescue service to take up standby positions, other designated stakeholders within the airport community will be pre-mobilized (example, medical center facility, ground operations teams, passenger terminal teams, etc.) for possible deployment.

As more details are gathered from the pilot and depending on the severity of the incident, the Operations Commander will have to conduct a priority assessment and make his recommendations. Should the incident be classified as a "full emergency" (i.e., the equivalent of a "priority 1" incident), stakeholders who received the initial alerts will proceed to take up their respective positions and open up/ cordon off any required facility within the airport compound to receive passengers from the distressed aircraft, or provide initial pre-healthcare triage on-site (prior to conveyance to the nearest hospital).

External stakeholders such as the AAIB[6], nearest designated hospital(s), municipal fire departments or state police will also be alerted for assistance on the airport compound. At the strategic level, the crisis management team will be activated and regular updates on the incident will have to be monitored, from initial response right through to aircraft or scene recovery. Throughout these activities, media communications will need to be addressed and managed as well.

The above illustration demonstrates that the moment an incident is escalated to a crisis state, the focus on crisis communications will not only widen, but starts to shift in attention from internal, to external stakeholders. Operational and tactical communications and messages at the incident site would normally not be "shared" with the public. Instead, the crisis management team should release approved messages and information to the media (in this instance, via the media liaison team). Where a positive coordinated effort needs to be projected, pre-approved messages would have to be ready in hand, validated based on the nature of the incident, before internal dissemination or official media release.

The general process in crisis management and communications can be similar in other potential scenarios as well. Some probable differences would be the level of stakeholder's coordination required (example: a national civil emergency incident, compared to a localized contained fire incident in a shophouse), the pace of incident escalation (example: a recurring seasonal pandemic, compared to a targeted cybersecurity incident at a financial institution), as well as, the effort required in maintaining consistent communications (example: a temporary business disruption, compared to a sustained crisis).

6 Aircraft Accident Investigation Bureau (or equivalent, depending on location of aviation incident)

Common Challenges In Crisis Communications

While frameworks exist to guide the development of crisis management plans and communications processes, challenges will exist as every scenario is unique:

- **Initial alerts and warnings** received often need to be re-broadcasted through various communication platforms, thus causing delays in critical information dissemination
- **Acknowledgement of received information** is recorded in various formats - following post-recovery, where an after-action review (AAR) needs to be performed, it will take some time to collate and validate
- **Accuracy of information** communicated, particularly where it may be relayed through multiple parties
- **Adherence to timely situation updates**, regardless at the frontlines, or to official media outlets
- **Currency of information** by the time it reaches the crisis management team or media spokesperson
- **Absence of a common operating communications platform** (or its reliability), leading to different response stakeholders within the affected community not being able to seamlessly collaborate with one another
- **Potential for misinformation** in today's environment, where information can be relayed from multiple sources (worst, distorted), and the general public may not know which official source to refer to
- **Cybersecurity risks**, particularly where the adopted communications platform is insecure, non-compliant or unstable

The above is not exhaustive and is dependent for every incident that occurs. As the environment becomes more complex, previous planning assumptions may no longer be valid and organizations must be prepared for multiple incidents occurring simultaneously or concurrently.

Addressing Crisis Communication Gaps

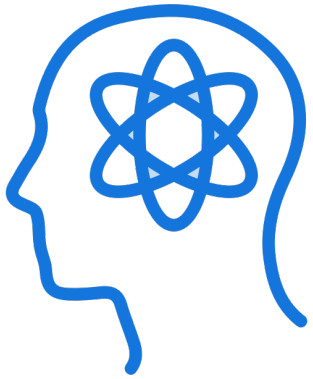
For communications to be effective in crisis management, the following should be considered, whether it is applied at the strategic, operational, or tactical levels:

- **Uphold** principle of "true source and one voice" for information (or instructions)
- **Conduct** a final review of "what needs to be said" from pre-prepared messages before broadcasting
- **Exercise** discipline in timely dissemination of critical information
- **Be ready** to push out information once validated and relevant
- **Implement** a system or process that minimizes dissemination error
- **Ensure** all intended recipients receive them at the same time
- **Be certain** that information reaches out to intended stakeholders and is acknowledged
- **To mitigate potential security risks, ensure** your means of communications abides to the relevant security requirements defined in your respective industry/sector

Any investment made in a reliable communications platform should in summary, be able to: send out critical alerts in the most expeditious manner; enable accountability of actions taken; facilitate the collection of critical information of operational or tactical responders and crisis management units; and, support collaboration of multiple stakeholders in a harmonized and secured environment.

Overall, an effective communications platform should be able to provide clear visibility and situational awareness of the current crisis, without having to rely on multiple disjointed sources or causing additional stress loads to your communications process.

Future Challenges (Being Prepared)



Through past scenario planning exercises, both public and private sector organizations may have developed crisis management plans based on potentially outdated planning assumptions.

The recent global pandemic has taught us (and the world) that our perceptions of a crisis would have to be adjusted and calibrated. In addition, other identified risks will continue to threaten organizations and society. While it may be simple to say, "just be prepared," leaders, managers and resilience planners need to ask themselves: "what are we preparing for?" Along with such questions, consider what common critical assets your organization should review that can effectively mitigate common impacts to your initial response, as well as business continuity recovery objectives.

In addition to prominent risk management reports, along with sector-specific information enabling organizations to perform their business impact analysis and hazards assessment, the other approach to adopt, would be incorporating "agility" in your emergency response, crisis management and business continuity plans, and partnering with reliable and resilient stakeholders or solution providers to facilitate this capability. The same applies to investing in a critical communications platform solution for your organization or community, where it is essential to ensure consistency and reliability of information flow to intended stakeholders during critical moments.

Next Steps

While crisis management frameworks provide useful guidance and a benchmark to adopt in enhancing an organization's resilience, there will be challenges in implementing and operationalizing them, due to the following:

- Incidents can occur anytime and anywhere (and may not occur in silo). Staff who are assigned to oversee and manage (in particular) the initial response will need to be vigilant and experienced to communicate critical details of the incident.
- Besides the commitment of time and (most likely) dedicated resources to look into enhancing resilience and critical communications during a crisis, post-incident evaluations on incident handling is an increasingly mandatory requirement, particularly in regulated sectors (and thus requires prompt provision of data or incident logs when requested).
- Even where there is an existing communications platform, along with a dedicated team of resilience professionals in the organization, some may still find managing communications in an efficient and secured manner a challenge. For some organizations, this may even be viewed as an impossible task.

Recognizing and understanding the above considerations is just one aspect in enhancing an organization's resilience. Implementing a secured and trusted communications platform in consultation with our specialists can help the organization focus on its core business, while ensuring life safety and continuity of operations is looked after.

When Preparedness, Response and Recovery is Crucial

The ability to reach out to your staff and essential stakeholders during an impending incident or crisis can help to minimize further business impacts and disruptions. Whether it's at the preparedness, response or recovery phase of your crisis management framework, communicating critical information can inform and involve your staff and the community on the required actions to adopt, create trust, and mitigate potential loss.

BlackBerry AtHoc

Organizations need to focus on their business. Let BlackBerry® AtHoc® help keep your people safe and operations running.

To learn more about how BlackBerry AtHoc software helps organizations communicate and collaborate in times of crisis, please visit: blackberry.com/athoc and follow @AtHoc.

Trusted by organizations globally to unify their crisis communications, BlackBerry AtHoc meets various stringent standards including FedRAMP, ISO 22301/ 27001:2013, FEMA and many others.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

BB20-JM02 | 200612

Annex A

FEMA – *Emergency Operations Plan (EOP) Formulation*

FEMA's mission is to lead America to prepare for, prevent, respond to, and recover from disasters. FEMA embraces a comprehensive planning approach on emergency and crisis management, by adopting the National Incident Management System along with the Incident Command System as a critical component in managing domestic incidents, as well as the National Response Framework, the guide for how the nation conducts all-hazards incident response.

FEMA prescribes three available formats in designing the Emergency Operations Plan (EOP): (i) Traditional Functional EOP format, (ii) Emergency Support Function format, and the (iii) Agency/Department Focused EOP format. The traditional functional structure is most commonly used, and many jurisdictions have been developing their EOPs since the 1990s. It consists of three major sections: the basic plan, functional annexes, and hazard-specific annexes (see Figure 1):

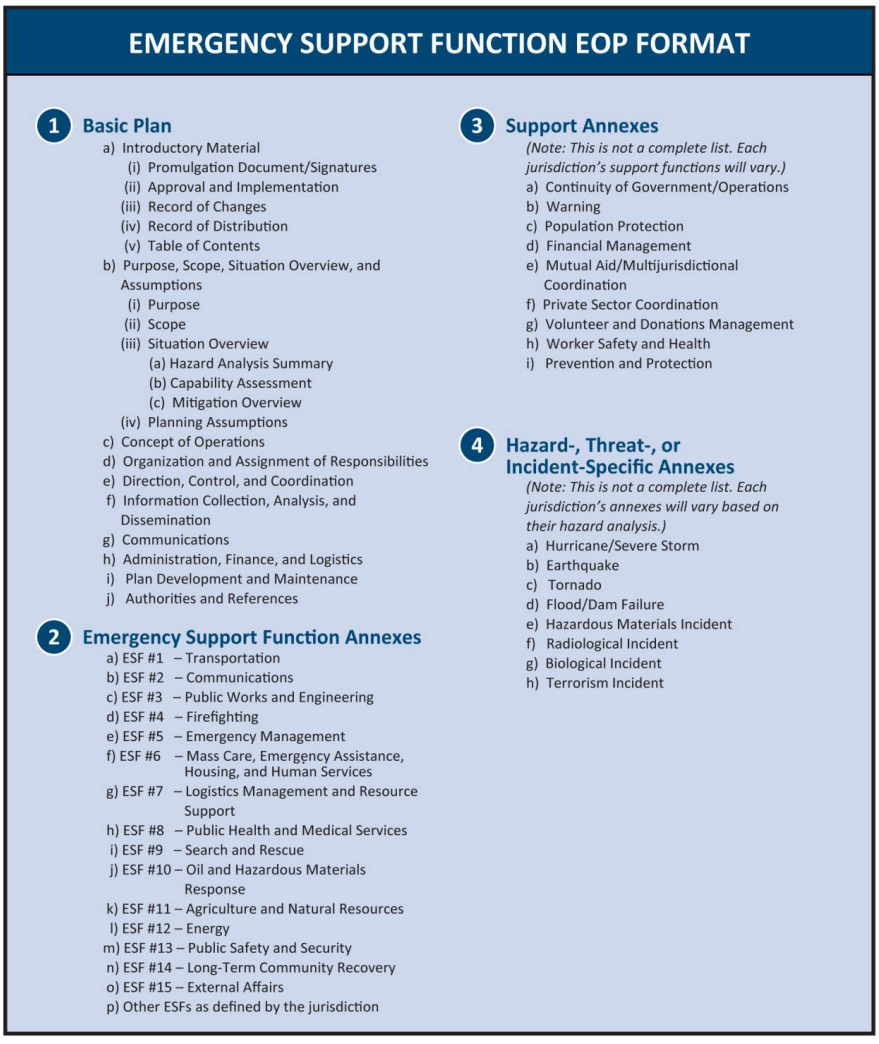


Figure 1:
Traditional Functional EOP Format

An important point to note is that an EOP should be flexible enough for use in all emergencies. The document describes the purpose of the plan, the situation, assumptions, concept of operations (CONOPS), organization and assignment of responsibilities, administration and logistics, plan development and maintenance, as well as authorities and references. The emphasis in interoperability (vertically within government, or laterally involving community and private organizations), providing sufficient alert and warning, accomplishing effective command and control, as well as integration of communication networks and accessibility, demonstrates the need for resilience planners to ensure effective processes and assets are committed to support effective emergency management.

Ensuring relevant stakeholders are familiar with the organization's EOP through (at minimum) table-top exercises and drills can enhance the organization's preparedness. In the event of an emergency or crisis, the ability to inform relevant stakeholders of the incident, the pre-planned measures they are required to take (example, building security team to verify a reported suspicious parcel, or the local Police to request for public safety assistance and management), and keeping all parties updated is important. Where these critical processes can be clearly communicated through a common platform accessible by all, it can significantly help organizations in its response and recovery phases.

Business Continuity Institute (BCI) – *Preparedness in ensuring continuity of operations*

The BCI's Good Practice Guidelines (GPG) advocates the adoption of a business continuity management lifecycle as a framework in designing and implementing a business continuity program within the organization through six "professional practices" (PP), namely: policy and program management, embedding, analysis, design, implementation, and validation.

Specific details on crisis management are addressed under "PP5 – implementation," where a clear distinction is made between an "incident," as well as a "crisis.". To ensure organizations develop an effective response structure, the following factors should be considered:

- The ability to recognize and assess threats when they occur
- Clear escalation procedures
- Individuals and teams with sufficient authority and capability to develop and select an appropriate response to an incident
- Clear procedures for the activation and control of responses to an incident or the crisis
- Responsible personnel with the authority and capability to implement the agreed business continuity solutions as defined in the organization's plans

- Ability to communicate effectively with internal and external stakeholders
- Access to sufficient resources to support the implementation of the continuity solution
- Ability to recognize when key external suppliers should be notified and included in the implementation of the continuity solution
- An agreed budget to support the response structure

This would mean that an organization's business continuity and crisis management plan should categorize the various potential threat scenarios and should include "alerting thresholds" (ie, at what point should other parties need to be notified and take action), who would have the authority to decide, and who should be notified (ideally those in responsible positions who can decide on the mobilization of response, support or recovery assets).

PP5 further recommends that an organization's communications plan should: be catered for internal and external interested parties; define relevant channels of communication (example, social media, print, etc.); consider multiple communication methods and channels to ensure availability; assign relevant authority and maintain consistency in delivery; and appointing a spokesperson to engage the media.

Given today's highly connected environment where misinformation can be easily disseminated, the availability of pre-formatted messages dedicated to relevant stakeholders should be prepared, reviewed regularly, and ready for publication when a crisis or incident arises. Where misinformation may unfortunately reach stakeholders earlier than official information, the true source must not lag too far behind.

ISO 22301:2019 – *Standardizing business continuity*

The ISO 22301:2019 is a document specifying requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of, the occurrence of, prepare for, respond to, and recover from disruptions when they arise. The requirements specified in this document are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity. The document guides organizations in the establishment of a Business Continuity Management System (BCMS).

In designing and sustaining the BCMS, the following components should be addressed in business continuity plans:

- Purpose, scope and objectives (ie, what is the purpose of this BCP and which Divisions/ Departments does it cater to)
- Roles and responsibilities of the team that will implement the plan (ie, In these identified Divisions/ Departments, who are the people required to perform relevant tasks? Also, who else has a part in this BCP?)
- Actions to implement the solutions (ie, To execute these recovery strategies, what are the key steps to be fulfilled?)
- Supporting information needed to activate (including activation criteria), operate, coordinate and communicate the team's actions
- Internal and external interdependencies (ie, who are the internal and external stakeholders involved in executing this BCP? What are their roles and responsibilities?)
- Resource requirements (ie, what assets are required to see through the execution of your BCP from activation right through to recovery?)
- Reporting requirements (ie, what specific information is expected to be provided during a business disruption? What is the frequency of reporting? In what format are they required to report?)
- Process for standing down (ie, what critical factors must be observed or achieved, before the crisis management team can "stand down", leaving to the "recovery team" to continue with its tasks?)

From a communications perspective, it should cover:

- Communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate
- Receiving, documenting and responding to communications from interested parties, including any national or regional risk advisory system or equivalent
- Ensuring the availability of the means of communication during a disruption
- Facilitating structured communication with emergency responders
- Providing details of the organization's media response following an incident, including a communication strategy
- Recording the details of the disruption, the actions taken and the decisions made