A Framework for Post-Crisis Business Continuity Plans

Sharvari Kulkarni  Gezinus J. Hidding  Serhat Cicekoglu

skulkarni4@luc.edu  ghiddin@luc.edu  scicekoglu@luc.edu

Quinlan School of Business, Loyola University Chicago

Abstract

The traditional risk management literature is oriented towards preventing and decreasing the impact of a crisis on an organization’s Business Continuity (BC). This is generally done by identifying, analyzing and assessing the impact that certain anticipated risks would have on the organization. In contrast, there is a relative dearth of literature on what organizations should do once a crisis has occurred. This paper proposes a general framework for post-crisis Business Continuity Planning (BCP). The BCP framework consists of multiple planning aspects, multiple phases and many detailed elements for BC plans. Based on the framework, organizations can design, tailor and/or assess their post-crisis BC plans. Future work will involve industry-specific extensions of the BCP framework.

1. Introduction

The Actuaries Institute defines Enterprise Risk Management (ERM) as ‘the process by which organizations assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organization’s short and long-term value to its stakeholders [1]. Definitions from other articles such as [27], [10], [25] and [26] respectively focus on management, identification, interdependencies and impact of risks and identification of potential events (i.e., known knowns) to reflect the risk appetite of the organization’s management level. Professional organizations, such as the Project Management Institute, have also incorporated techniques based on such views into their professional approaches, such as PMBOK [20], and related certification programs. We note that the focus of ERM is on “preparedness” for crises. Regardless, crises happen [29]. For a recent Delphi study of 86 threats in 11 categories that are “not now receiving adequate planning or adequate development of mitigation options”, see http://www.iscramlive.org/portal/node/2763.

In the cases of crises, the fundamental objective of ‘staying in business’ is not emphasized in the ERM literature, according to [5]. According to an anonymous reviewer of this paper, many companies consider business continuity (BC) a low-rated activity and do not pay much attention to BC planning (BCP); even the area of information system attacks may not have received sufficient attention in many companies. In, or after, crisis situations, organizations respond by blaming top executives, firing them and bringing in new leadership, or by blaming new competitors’ cheaper and better product(s). One industry consultant studied 280 organizations with a risk management plan that went out of business after a crisis [28]. Most, if not all, of them were driven out of business by their competitors.

Ideally, organizations should be able to manage, absorb and adapt to a crisis, i.e. stay in business during and after crisis. However, as the same anonymous reviewer remarked, serious BCP may fall to the wayside, as well-paid executives (particularly in the US) are implicitly expected to have an immediate decision for everything, and cannot admit not to have an immediate answer. Also, organizations may rely on insurance and government agencies to take care of crisis management, e.g., the BP oil spill, or the subprime lending crisis.

We adopt the Business Continuity Institute’s definition (which reflects definitions in various international standards) of a BC Plan as a “documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level” (http://www.thebci.org/glossary.pdf). We propose a BCP framework that focuses on BC activities that a medium-size organization may adopt in and after a crisis situation.

We avoid terms such as “disaster”, “calamity”, “catastrophe”, and “emergency” since they are often associated with natural disasters (e.g. earthquakes, floods, etc.) or terrorism, which, while within the scope of our research, is not the focus of this paper. Since our
view of BCP is broad, we use the terms “crisis” that is sparked by an “event”. We define crisis as an expected or unexpected situation that forces changes to the organization’s normal day-to-day operations to ensure that it remains in business and operable. This definition implies that the nature of the crisis will vary from one organization to another, and may vary from one industry to another. However, so far, our research has focused on similarities of BC plans across industries.

2. Literature Review

Much research on crisis management has been done in the public sector on topics such as Continuation of Operations (COOP) [8], Hazard Vulnerability Analysis (HVA) [13], Threat and Hazard Identification and Risk Assessment (THIRA) [31] and by organizations such as, Centers for Disease Control (CDC) [6] and The Federal Financial Institution Examination Council (FFIEC) [9]. Such research is meant for public organizations such as emergency responders. We acknowledge the need to address preparedness and the need for identifying risks and ensuring that risk management frameworks exist in each organization. However, since much research has already focused on crisis management, particularly from an emergency management point of view, we focus less on it.

Even after organizations prepare for a crisis, unexpected events will occur and impact the organization. For example, the Tylenol case, where bottles of medicine on drug store shelves had been laced by an outsider with cyanide.

Various BCP frameworks and standards have been promulgated, such as the international ISO 22301, the British BS 25999, and Australian HB 293-2006. Such BCP standards as well as crisis management frameworks such as COOP emphasizes preparedness. Labaka et al. have identified policies for organizations to improve the resilience of their Critical Infrastructures (CIs), such as during industrial accidents [15]. They describe various policies to prevent, and/or to prepare for handling, failures of CIs. Several of Labaka’s policies focus on activities that should be performed pre-crisis, such as design and construction of CI’s or preparation and training of various actors (e.g., management or first responders). Some of Labaka’s policies touch on activities to be performed once the crisis event has occurred, e.g., use of crisis response equipment.

3. Post-crisis Business Continuity Plans

We take the idea of preparedness one step further with Taleb’s Black Swan argument that unexpected events occur anyway and they may impact an organization both positively and/or negatively [29]. In essence we extend the definition of resilience as defined by Labaka et al. as the ability of an organization to manage an unexpected crisis.

If the organization wishes to remain in business, it should have a BCP that is to be executed after the event that precipitated the crisis (“post-crisis”). We use the short-hand “post-crisis” even though the crisis itself may play out over a long(er) period of time. For example, in the event of a competitor introducing a much better product causing serious damage to an organization’s competitiveness, we view “post-crisis” as starting immediately after the precipitating event. In the remainder of this paper, we concern ourselves mainly with the BC activities to be performed post-crisis (as opposed to preparation activities to be performed pre-crisis) particularly for medium-sized businesses in competitive industries. We introduce a BCP framework below.

This framework is the result of inductive reasoning based on literature references to one or more BC activities to be performed post-crisis. In other words, we created a conceptual framework inspired by specific pieces, a process of induction that has been called “conceptualization” in [19]. Conceptualization is only the first step in the scientific research process. It defines the nature and the general variables of the problem. Subsequent steps, to be taken in future research, involve building a “scientific model”, with specific variables for which data will be gathered to test the framework, and applying the validated model to real-world situations.

We modeled our BCP framework after [15], who proposed an implementation methodology of a resilience framework with phases and different variables. The detailed activities in our framework also draw from Botha et al. [4]. We have attempted to make our framework modular, while addressing the post-crisis business continuity activities via three aspects of BCP, namely, Severity, Recovery and Maturity. Each aspect is further broken down into more granular and succinct details. The three aspects are depicted in figure 1. We elaborate on each of these aspects in this section.

3.1. Severity

Much the same way as successful operation of critical infrastructures is important for the proper functioning of society [15], identification of assets and capabilities which are critical to the organization’s business continuity becomes a key activity.

Severity deals with identifying such assets/capabilities, e.g., the organization’s Facilities,
Human Capital, Inputs (Suppliers/Raw Materials), and Customers. For humans, air, water and food are critical for our survival. Similarly, we argue that organizations need to identify which assets/capabilities are critical for their survival. Consequently, BCP’s should consider the Severity of loss of assets and capabilities and identify what assets and/or capabilities are crucial to the organization, and how to manage the organization in the face of a loss of such assets and/or capabilities post-crisis. The respective Severity factors that each organization identifies may vary by organization and by industry. The scope of this paper is restricted to only highlighting the importance of identification of Severity factors, and, so far, is industry independent.

![Diagram of Post-crisis BCP life-cycle](image)

**Figure 1: Post-crisis BCP life-cycle**

### 3.2. Recovery: Three phases

Recovery deals with how to use the organization’s (remaining) assets/capabilities during and after the immediate crisis [15]. The response to any crisis consists of not only of managing the immediate aftermath, but also of Business Continuity [5]. Our post-crisis BCP framework draws on Boeing’s BC model in [5], but with a key difference. In Boeing’s BC model, the phases are sequential, i.e., one after the other. In our framework, phases can overlap. For example, an organization may consider Business Recovery activities almost immediately after the initial crisis event while continuing to manage the immediate response to the crisis.

Furthermore, the organization’s post-crisis competitive situation may well be different as pre-crisis, because of changes in, e.g., competitor actions, customer preferences, laws or regulations, technologies, etc. So the focus shifts from response to recovery and finally to “resilience” [15], [30]. Our framework proposes three phases for the Recovery aspect: Crisis Management, Business Recovery, and Business Renewal, see figure 2. We use the terms Business Recovery and Business Renewal after Taleb’s Anti-fragility concepts [30]: Business Recovery is the ability of an organization to withstand a crisis, i.e., not to succumb to it, and Business Renewal is the ability to bounce back after a crisis, to become possibly even stronger than before, i.e. the pre-crisis period [30]. The possibility of an organization benefiting from a crisis is in contrast with some views, e.g., [12], that risk management should be focused on downside/negative impacts only.

Crisis Management is well-researched, as argued in our earlier literature review, so we focus less on it. Business Renewal is largely about strategic planning, a field with its own existing extensive literature, so we also focus less on it. However, the Business Recovery phase has not seen extensive research, so we focus more on it.

![Diagram of Phases of a Business Continuity Plan](image)

**Figure 2: Phases of a Business Continuity Plan**

#### 3.2.1. Crisis Management

This phase comprises of first-response type of activities that an organization, in the event of a crisis, must perform and with immediate effect. For example, if an IT organization is in a crisis, it would probably want to know if its data centers and
servers are down, unavailable or inaccessible. And if they are, the IT organization should probably have backup plans, as a part of BCP, that call for fail-over (i.e. switch to a redundant or backup system ensuring uninterrupted access to business operations) of data centers or backup servers to ensure business continuity. Similarly, if the warehouse of retail chain is hit for any reason, the BCP should suggest alternative supply sources to ensure that the retail chain’s most critical process in the value-chain, i.e. sales, should be least affected.

3.2.2. Business Recovery. Activities performed under this phase may begin in parallel with the activities in the Crisis Management’ phase. The assumption here is that the organization has survived the initial crisis event and now is gradually moving back to business as usual. Activities performed in this phase are oriented towards gathering information on what went wrong, performing an analysis on the impact of the crisis and deciding on next steps.

3.2.3. Business Renewal. This phase comprises of activities that are performed assuming that the organization is no longer managing the (immediate aftermath of the) crisis. For example, as a result of the crisis, competitors may have gained or lost market share, customer needs or preferences may have changed, suppliers may have gained or lost market share etc. That is, the competitive situation after the crisis may be quite different from that before the crisis. Consequently, the organization should update, or redo, its strategic plans. As a result, there may need to be a change in the way the organization needs to be structured post-crisis and it may need new/different operating procedures, resources etc. to continue operating.

3.3. Recovery: 10 General Elements

Our BCP framework identifies 10 elements that need to be addressed while managing a post-crisis situation. Given that our research so far is only in the conceptualization stage, we do not claim that this list of elements is exhaustive. The 10 elements are: Team, Operations Centre, Situation Awareness, Finance, Communications, Business Processes, Customer Relationship Management, Supplier Relationship Management, Information (Technology) Management and Miscellaneous. They are common across the three phases, although specific activities within them may vary across phases. Figure 3 shows examples of BC activities by element and by phase.

For the following subsections we relied on several references that relate to multiple elements of our framework: [11], [15], [16], [23], [6], [8], [9], [13], [31] and [27]. Additional references that relate only to a specific element are cited in the particular subsection below, often next to the subsection heading, that describes that element.

3.3.1. Team. [14], [17] To manage Business Continuity, a team of people with clearly defined roles and responsibilities is essential. We propose that the team include stakeholders from different segments of the organization. Ideally, such stakeholders collaborated effectively with each other in preparing the BC plan. The pre-crisis planning team as well as the post-crisis BC team are likely subject to matrix management. The better the planning collaboration pre-crisis, the better the BC team can act post-crisis. The team could also involve local people as volunteers (especially in cases of first response). The team would interact with outsiders, e.g., government and NGOs.

Our BCP framework proposes that team roles be clearly delineated, along with escalation procedures, succession and authority details of each team member. For example, a team member should know when and how to alert higher ups so that they may get involved. Teams should manage vital records and must have the ability to make decisions while under considerable stress [22]. We endorse the five principles of mindfulness as proposed in [32], including the principle of ‘deference to expertise’. We propose that to identify correct people for such roles, the organization run personality tests and profile people who would be suitable for such situations [3] (Based on personal communication with Prof. Arup Varma, April 7th, 2014). Such profiling may identify team leaders as well as other people suitable for various other roles.

Furthermore, our framework proposes that there be three different teams, one for each phase. In order to facilitate effective collaboration, particularly across teams, we propose that clear information management procedures and guidelines be incorporated. This would serve as a one-stop-shop for all the teams, within and across the three phases of our framework, to acquire and update information related to the crisis, which may be helpful during the crisis, but also afterwards in evaluating and updating the BC plan(s).

3.3.2. Operations Centre. [17], [27] We propose that the organization have a “war room” for the team – possibly a sort of a bunker – that it can use in the event of a crisis. This (possibly make-shift) workplace should be fully equipped to manage the key operations
of the organization and be able to manage vital records. For example, United Airlines has, adjacent to its operations center, a designated room that is fully equipped with pre-assigned workstations for various actors ready to be used at any time in case of a crisis. This element of the BCP framework should also address the issue of identifying alternative physical locations that the organization may use if their “war room” or current office/workplace is unavailable. The purpose of the “war room” is a ‘stop-gap’ arrangement until regular work locations are restored or rebuilt. A “war room” finds its place particularly in the first two phases. Overlapping with the Team element as well as Situation Awareness, the war room can help to manage the documentation of the way in which the crisis is handled and how the business is brought back to life. This intellectual property would preserve knowledge from the crisis by making the organization better prepared a next time around and/or during the Business Renewal phase. In that phase, the framework assumes that the organization is (back) in a stable and long-term workplace, leaving a “war room” less relevant.

3.3.3. Situation Awareness. [11], [14], [17], [27] This element of our BCP framework acknowledges the importance of proactive monitoring of the post-crisis situation [5]. The specific activities may differ by phase. For the Crisis Management phase, our BCP framework proposes that the organization assess the condition and accessibility of its assets (assets are information, people, facilities etc.). It is important for the organization to understand what is working and what isn’t, so as to take necessary steps accordingly. Situation Awareness also involves the analysis/assessment of the impact of any inability to meet prior commitments (e.g., production or shipping). It also should involve an awareness of (short-term) cascading effects, as well as prediction and mitigation of the impact of such cascading effects. For example, if there is a power failure, computers and communications systems may be down, which raises the needs for other ways to communicate with employees, first responders, customers, etc. For the Business Recovery phase, our BCP framework proposes that the focus be on competitive intelligence, and on restoring or maintaining pre-crisis situation awareness capabilities. It becomes important for the organization to assess the timeframe and cost to recover and/or restore any assets that the crisis may have rendered inoperable. We propose that the organization analyze scenarios and determine responses to them, e.g. operating at reduced capacity and/or under contingency arrangements. We advise the organization to perform an analysis/assessment of (root-) causes of any failure of existing business processes and how to manage such processes differently going forward. This process is two-fold: 1) to generate a "plan"/"approach" for the management to take decide upon and 2) to devise steps/milestones to be achieved and estimate the impact of the inability to meet prior commitments. It is imperative that the organization adapt to the impact of cascading effects (both short and long term).

For the Business Renewal phase, our BCP framework proposes that the organization assess its business model with respect to the new competitive situation. That is, that the organization re-think its growth trajectory, by thinking about the sustainable (and possibly new) core of the business and explore other growth possibilities. In other words, that the organization engage in strategic (re-)planning. The organization may also have to perform strategic analysis/assessment of (root-) causes of any failure of existing business process and how to manage such processes differently going forward. Lastly, we suggest that the organization understand the power and impact of cascading effects (both short and long term) of the strategic decisions that are being made in this phase.

3.3.4. Finance. [17] In any situation, including post-crisis management, managing finances is critical. Again, specifics may differ by phase. While in the immediate post crisis, our BCP framework proposes that finances be managed as permitted/constrained by organization’s profitability and level of debt. In the initial two phases, the focus should be on cash on hand, with questions to be addressed such as ‘Can the organization process receivables?’, ‘How does the organization plan to handle payables?’, ‘What are the different ways by which the organization can process new orders?’ and ‘Has / Does the organization need to register (liability) claims with its insurance companies?’. (Based on personal communication with Prof. Steve Todd, October 2013) The organization could also maintain offsite copies of the insurance documents and proof of purchase of any equipment that is going to be claimed as lost.

We suggest that, in the Crisis Management phase, the organization should expect to establish a crisis management budget for expenses for rentals, purchases and service providers related to, e.g., clearing debris, temporary facilities, alternative staffing, back-up equipment, etc. In the next phase, Business Recovery, finances related to receivables, purchases, payroll and insurance claims come back into focus. Also, the organization may need to purchase/rent new facilities, equipment, etc. When the organization successfully moves on to the final phase, Business Renewal, receivables and payables should obviously continue to be managed as usual. The BCP framework also
proposes that the organization review its financial model and strategically analyze and assess loss and recovery of revenue and estimate the cost of restoring or establishing the desired operational structures.

3.3.5. Communications. [27] In this element of our BCP framework, communicating with relevant stakeholders and, in particular, the public at large is of utmost importance and must be done in all three phases. Since this element too is a part of the BCP framework, it essentially comes into play after the crisis has taken place. Our framework does not assess the role or importance of communication before the crisis. We propose that the organization decide upon factors such as media (print, email, TV broadcast, Twitter etc.) to use, and when to communicate, to which target audience(s) and by which member(s) of the BC team. The organization may also think of engaging goodwill ambassadors and external reputable people to convey the organization’s message. Honesty, being forthright and open about the situation in its communication will help the organization (in the long run).

There are action items more specific to each phase. For example, in the Crisis Management phase, it is important for the organization to communicate with first responders and emergency management authorities (principally the government) and also with the public at large via trusted third parties. In the subsequent two phases, the communication may be more with business and strategic partners, but possibly still with the government (e.g., regarding laws or regulations that were changed as a result of the crisis).

3.3.6. Business Processes. [11], [14], [17], [27] The purpose of this element in our BCP framework is to ensure that the organization can (continue to) run its most critical business processes as best as possible post-crisis. For example, continued (partial) delivery of product and services to customers could be one such process. In one company we know, the CIO has contingency plans to bring her data center back up, but the business executives have not determined the priority of which business processes should be recovered first, next, etc.

For the Crisis Management phase, we propose that the organization executes pre-defined contingency arrangements or alternative processes which should be geared towards ensuring continuation of activities with minimal hassles and/or resumption of activities at the earliest possible time. (Analysis done as a part of Situation Awareness may be useful in this element).

Contingency arrangements could be for facilities and/or equipment, i.e., the organization may operate from alternate rented or leased locations until operations are restored at the affected facility. In case a few personnel are unable to reach the location or, in the worst case, are dead, the organization should ensure to have back-up resources in place. This is especially critical at management levels, where the (alternate) chain of command should also be laid out. In the Business Recovery phase, we propose that the organization think of restoring critical processes or think of alternate processes or improvise the existing ones to suit the post-crisis situation. In the Business Renewal phase, we propose that the organization assess and analyze its business processes, especially the ones that were affected by the crisis, leading (possibly) to a redefinition of its existing business model and value chain.

3.3.7. Customer Relationship Management. [21] This element of our BCP framework focuses on deciding which customers are most valuable to the organization and, following the 80-20 rule, advises the organization to focus more on them. Organizations might adopt the Customer Value Matrix (CVM) framework in deciding their most valuable customers and then servicing them first [21]. Regardless of whom the organization chooses to serve first, we propose that the organization must communicate and coordinate with all of its customers and to do so through all the three phases of post-crisis management.

We advise organizations to strategically serve its customers in a way that will ensure that the organizations are able to remain afloat. During the last phase, Business Renewal, the organization may rethink on its CRM strategy and choose to restructure it based on the changes that the crisis has brought with it.

3.3.8. Supplier Relationship Management. [2] In our BCP framework, this element is similar to CRM, except that it is targeted towards suppliers. We propose that the organization decide which suppliers/materials are the most critical and also think of pre-defining alternative suppliers in the event of a crisis. This is especially important in the Crisis Management phase. All through the three phases, the organization should think of managing and focusing on its most critical suppliers and coordinating with them.

3.3.9. Information (Technology) Management. [4], [14] Our BCP framework acknowledges the critical importance of Information Technology (I.T.) while managing a business in today’s world. Disaster Recovery is a well-established practice in I.T. We suggest that in the first two phases, it becomes imperative for the organization to assess whether or not
the (access to) its data center(s) and/or data has been affected. If so, attempts must be made to recover access or have a backup of the essential systems in a separate location as a viable alternative. This backup can be used into the Business Recovery and Business Renewal phases, if necessary, until the data center and the data have been restored. In the Crisis Management phase, the organization must, importantly, also check access, availability, accuracy and security of information, since important decisions must be made, possibly under extreme time pressure, based on this information.

<table>
<thead>
<tr>
<th>Phases</th>
<th>Elements</th>
<th>Crisis Management</th>
<th>Business Recovery</th>
<th>Business Renewal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Team</td>
<td>-Include all the primary and secondary stakeholders -Ensure clearly defined roles and responsibilities -Identify the right people to do the job using personality profiling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) Operations Center</td>
<td>-Ensure presence of alternate facility that is equipped to manage vital records and key operations</td>
<td></td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>3) Situation Awareness</td>
<td>Assess accessibility to assets and their condition</td>
<td>Focus on competitive intelligence and devise milestones for BC</td>
<td>Assess the operating business model with respect to the new situation</td>
<td></td>
</tr>
<tr>
<td>4) Finance</td>
<td>Focus on 'cash on hand', rentals, insurance claims, receivables and payables</td>
<td>Review financial model and analyze loss and recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5) Communications</td>
<td>-Communicate with honesty with the public at large -Decide on mode of communication and type of message to respective stakeholders and the person who'll deliver it</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6) Business Process</td>
<td>-Ensure that the organization is efficiently and correctly able to identify its most critical business processes -Analyze and review the business model and value-chain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7) Customer Relationship Management</td>
<td>-Identify most valuable customers -Ensure communication and coordination with customers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8) Supplier Relationship Management</td>
<td>Manage and focus on most critical suppliers and ensure communication and coordination with them</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9) Information Technology Management</td>
<td>Ensure access, availability, accuracy and security of information</td>
<td>Maintain access, availability, accuracy and security of information</td>
<td>Exploit access, availability, accuracy and security of information</td>
<td></td>
</tr>
<tr>
<td>10) General / Miscellaneous</td>
<td>Ensure the presence of an 'emergency response kit'</td>
<td>Focus on recovery of business and post-mortem analysis of crisis</td>
<td>Re-think and re-draft business model and value chain</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: Example BC activities by phase and element
Of course, organizations should always ensure access, availability, accuracy and security of information, but the immediate post-crisis situation may be so confusing that organizations might not realize that certain information is unavailable, inaccurate or insecure. Even worse, astute competitors or adversaries might try to exploit an organization’s information issues, or, worst of all, sabotage an organization’s information (technologies). Managing Information (Technology) continues to be critical in the Business Recovery phase. The organization may look into possibly exploiting (new) information (technology) in the Business Renewal phase.

3.3.10. General/Miscellaneous. While formulating the BCP framework, we found certain activities that were important but did not fit neatly under any of the nine aforementioned elements. Nevertheless, we found these activities to be important for the completeness of our framework, and therefore list them here. The common attribute is the ability of the organization to manage known unknowns. Examples of the activities are discussed below phase-by-phase. For the Crisis Management phase, the organization must (continue to) maintain security of its assets: cyber- and physical assets. Depending on the nature of the crisis, the organization may have to handle emergency evacuation procedures and perform search and rescue, and recovery operations. The organization may need an emergency response ‘kit’ (of, say, supplies or particular equipment) as well as checklists [16]. It should also think of alternative equipment and contingency arrangements.

In the Business Recovery phase, the assumption is that the organization has successfully come out of first phase and is now working on recovery of the business. Therefore during this phase an analysis of the organization’s ability to absorb and digest a subsequent crisis can be performed. Comparison with previous similar crises may also be done [18].

A crisis may result in many internal and external changes to the environment that the organization operates in. Therefore, during the Business Renewal phase, the organization may have to rethink its business model and value chain. It may want to reposition its brand/image in the market based on the impact that the crisis has had. For example, after a continuing slide in its market share, Yahoo decided to hire Mayers after her success at Google. It is imperative that the organization consider timely strategic decisions pertaining to procurement, M&A, divestments, partnerships, service providers etc. and also restructure its logistics and distribution model. Lastly, a retrospective study of the crisis handling may be done and lessons learned should be incorporated in the subsequent BCP.

4. How the BCP Framework can be used

The BCP framework can potentially be used in various ways. First, organizations might use it as a checklist or rubric in formulating their post-crisis Business Continuity Plan towards the goal of remaining in business if an unexpected crisis occurs. Aided by the respective aspects, phases and elements in the BCP framework, the organization may be able to formulate an effective plan for itself. The Severity aspect of the framework should help to identify the areas that are critical to the organization’s survival. The Recovery aspect should help the organization to identify relevant activities from the 10 elements across the Crisis Management, Business Recovery and Business Renewal phases. We note that the current version of our framework is generic with respect to various industries. That is, we expect the elements, phases and suggested activities to be relevant in most, if not all, industries. For the time being, it does not yet contain extensions with specific elements or activities that will be relevant in particular industries, such as healthcare, transportation, etc.

Second, if the organization already has a Business Continuity plan, it can evaluate its plan against our framework. The organization can check whether or not its existing plan is missing any relevant activities from any of the 10 elements across the three phases.

Third, using our framework, perhaps existing plans can not only be evaluated, but even assigned a maturity score, which is the third aspect of our framework that is explored further in the next section.

4.1. Maturity

Maturity deals with how well, or sophisticated, the organization is expected to perform, post-crisis, the various BC activities under the 10 general elements and three phases. Inspired by the Capability Maturity Model (CMM) [7], “Enhanced Building Block Approach” [24] and [16], we have defined maturity levels in the form of a ladder model. The progression of sophistication is shown in figure 4. Each rung on the ladder, i.e., each maturity level, can be assigned a numeric score, from 1 to 6. Such maturity scores can be collected for all activities, e.g., by assessors collecting data in an organization, or perhaps by a streamlined online self-assessment questionnaire.
Maturity scores for all activities can potentially be aggregated, e.g., by averaging, into an overall BCP maturity score for a business unit or the entire organization. (As our research is only in the conceptualization stage, we have not yet gathered any maturity data from real organizations. Also, the development of any numerical or statistical algorithms for computing maturity scores is still to be developed.)

Just like with CMM, suggestions for organizations how to reach the next higher level(s) of maturity, and estimates of cost and duration of doing so, will have to be developed in future research. Like other assessment instruments, our BCP framework is not prescriptive. Once an organization learns its maturity score(s), a cost-benefit analysis will need to be done towards a decision to (not) increase its BCP maturity.

5. Conclusion, Limitations and Future Research

Our motivation behind the BCP framework has been to contribute to research into Business Continuity Planning based on the reasoning that 'unexpected things do happen'. After all, organizations would ideally be able to remain in business after unexpected ‘Black Swan’ crises. The objective of current research is to provide a conceptual framework for organizations to assess their business continuity plans to be used post-crisis. Our framework is by no means prescriptive or a potential industry-wide BCP standard. For example, an organization may be assessed with a low score and choose to not improve that score.

So far, our research has limited itself to the development of the conceptual framework based on literature review. A potential next step is to validate the BCP framework by conducting retrospective studies based on the way organizations handled past crisis situations (Based on personal communication with Prof. Joan Phillips, April 1st, 2014). Or, to conduct interviews and initial reviews of our framework in mid-sized organizations with top executives.

Another next step is to build industry-specific extensions of the various aspects, phases and elements. As suggested by an anonymous reviewer, we may find that organizations in, e.g., high technology or drugs, have done better in business continuity. This may well lead to adding, or subtracting some, elements for specific industry verticals (finance, consumer packaged goods etc.) or even to industry-specific BCP frameworks.

As to our framework is aimed at eventually assessing maturity, it would require some kind of algorithm to calculate a maturity score for each (part of an) organization [7]. Assuming maturity scores were available for multiple organizations, our framework may enable benchmarking of BC plans across organizations, by industry segment, geography, size of organization, etc.

6. References


