THE UTILISATION OF BUSINESS IMPACT ANALYSIS

By Jacob Taarup-Esbensen

Abstract

Business Impact Analysis (BIA) is the primary tool used in Business Continuity Management (BCM). The utilisation of the analytical approach supports decision-making and increases robustness and, thereby, the speed of recovery from adverse events in a social system. The paper argues that organisations can utilise findings in two distinct ways, in the form of risk reduction plans (RRP) and business continuity plans (BCP), both of which are used to create and improve preventive and protective barriers. Organisations can strategically increase their robustness by using the BIA's output to develop strategies to target vulnerabilities, thereby increasing the resilience of value-adding critical activities using fewer resources. Creating an effective response is improved by developing BCPs that target the recovery of specific critical activities. The paper uses examples from wildfire events in Greenland to illustrate how the analysis can play a role in increasing the resilience of a social system.

Key Words: Business Impact Analysis, Business Continuity, Resilience, Business continuity plan

The Utilisation of Business Impact Analysis

Organisations, companies and communities (social systems) increasingly focus on their ability to recover from adverse events. Spurred on by climate change and a global pandemic, the number and the scale of events impacting organisations and companies are on the rise. ClimateCost has estimated that, if there is no new policy action, on average, 345,000 people every year could be hit by coastal and river flooding in Europe by the 2050s, as rising water breaches riverbanks and sea defences during stormy weather (ClimateCost, 2021). Estimations are that, in the most severe case, the impact of climate change could wipe out 18.1% of world gross domestic product, while the reduction in the Organisation for Economic Co-operation and Development (OECD) will be above 10% (Swiss Re Institute, 2021; WEF, 2021). Such changes immediately affect human lives and destroy the physical, biological and social environment of those affected, thereby having a longer-term impact on their health, well-being and, ultimately, liveability. It is thus in the interests of organisations and governments to plan for effective recovery management, as economic, social and cultural sustainability depends on it (Elliot et al., 2010; Ning & Wong, 2009; Sawalha & Anchor, 2012). One of the regions experiencing the greatest impact from climate change is the Arctic. Climate research shows that warming prospects are close to or above the 1.5-degree target that the Paris Agreement proposed. For example, the estimate for Greenland is a current increase of between 1.1 and 4.2 degrees Celsius, while Svalbard will witness an average rise of above four degrees (Hanna et al., 2021; Norsk Klimaservicesenter, 2019). Hence, there is little reason to expect the situation to improve for social systems as we look south to the more significant population areas in North America, Russia and Europe.

Social systems risk suffering significant social, cultural and economic burdens when disaster strikes. The increases in severity from climate change highlight the need to prepare for the effects of climate-related hazards on the ability to protect critical activities and manage the potential impact if events prove too much for existing barriers. This is not to say that social systems will be on their own but that they will be increasingly more reliant on their resources and capability to organise than on society or insurance companies to take them through a crisis.

Within business continuity management (BCM) is the construction of preventative barriers, named risk reduction plans (RRPs), and protective barriers, which are called business continuity plans (BCPs). To understand their effectiveness and improve both RRPs and BCPs, we use Business Impact Analysis (BIA) (Barnes, 2011; Elliot et al., 2010; Hassel & Cedergren, 2019; Taarup-Esbensen, 2020). The analysis is a tool that a social system can use to investigate the consequences and impacts of a given disruption to its critical activities. For risk managers, BIA offers insights into the interdependencies that exist across organisational entities, providing hints as to the scale of the effect a given event might have on the organisation's ability to provide value to its stakeholders and, as mentioned, the effectiveness of preventive (initiatives before the event) and protective barriers (initiatives after the event).

This paper discusses the utilisation of BIA and how managers use the tool to make decisions that will reduce vulnerabilities and make the organisation resilient to significant disruptions. The paper explores the research question: What is business impact analysis, and how can social systems operationalise the findings? Two wildfire events in Greenland are used to argue how to utilise BIA and the steps taken to improve organisational resilience to future events. Here,

the utilisation of RRPs and BCPs is central to taking BIA from its analytical conclusions into practice and decision-making.

Business Impact Analysis

The following section describes the process of creating and using a BIA. The BIA forms the basis for preventive and protective barriers and, thereby, the development of RRPs and BCPs. The proposal is that a social system can use the BIA to retain and add value, by creating a virtuous circle of improvement. While the literature describes many ways of conducting the analysis, and variations exist depending on industry and context, the method described here applies to most private, public or civil society actors (Taarup-Esbensen, 2020). The model below illustrates the sequence of sub-themes to present a well-founded analysis of the business continuity challenges that a social system faces.

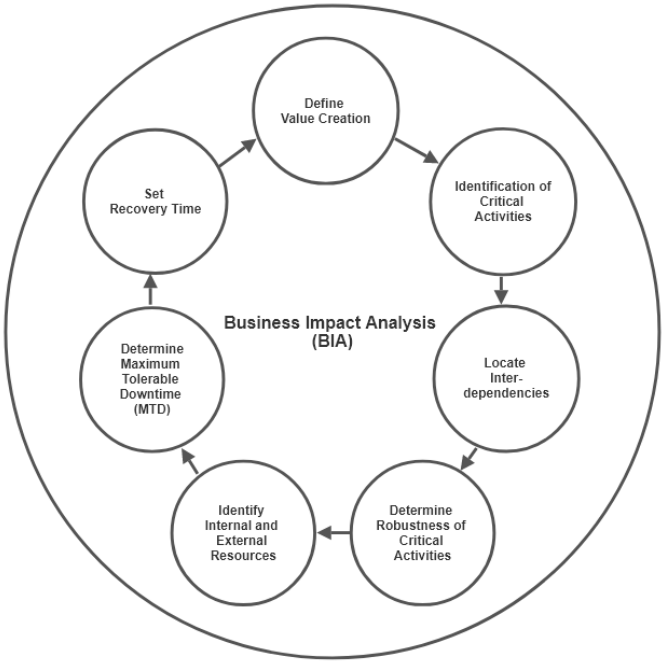

Figure 1 BIA model

Value creation

The BIA process defines how the organisation creates value, which is central to the analysis for all the following steps. Understanding the value-creating process is central to creating preventive and protective barriers that will mitigate threats to the social system (E. Aven & Aven, 2015; Hibberd, 2011). Value creation can be monetary but can also include other outputs deemed to be essential, such as cultural, human or social. Hence, the idea of value is taken beyond merely financial terms and becomes a broader definition, describing what is deemed crucial and considered worth protecting. The literature describes different ways of defining how organisations create value, for example, through their business model (Osterwalder & Pigneur, 2009) or value chain (Porter, 1985). A business model is an analytical tool that combines products or outputs, the organisation and its stakeholders, to provide a comprehensive understanding of how its activities produce customer value. Other tools include SWOT (Strengths, Weaknesses, Opportunities and Threats), supply chain and stakeholder analysis that can be helpful when dealing with specific industries, contexts or simply political priorities that

rank community activities as essential (Anbumozhi et al., 2020; Anthony & Cox, 2012; T. Aven & Flage, 2020; Freeman & Reed, 1983; Zsidisin & Henke, 2019). Value creation is, in this way, regarded as the foundation for the social system's reason to exist.

Identification of critical activities

Insights into the value creation process of a social system are used to identify, understand and protect its critical activities. The BIA uses input from the value creation analysis to identify critical activities, which, should they be disrupted, would seriously affect the organisation's ability to perform (Barnes, 2011; Hassel & Cedergren, 2019; Tammineedi, 2010). Critical infrastructure is, in most cases, automatically included, such as the ability to provide electricity, transportation infrastructure, freshwater, process sewerage and communication (Alderson et al., 2015; Curt & Tacnet, 2018; Pursiainen, 2018). Each element includes activities essential to the quality of the organisation's output and hence of value to its key stakeholders. For example, an organisation has to communicate with customers and create information that will serve the customers' needs, making market communication a critical activity. It can include access to electricity to ensure essential services are functioning in a community. There will be hundreds of processes within each of the activities that go into the analysis, ensuring that the social system creates value for its stakeholders. A hierarchy exists between processes and critical activities. An activity can comprise several processes, each playing a role in providing a value-adding service that the social system relies on for its value creation.

Interdependencies

The third part of the BIA process focuses on how critical activities are connected and dependent on each other. In this context, interdependencies can be identified by mapping how the social systems' in- and outputs of critical activities are connected and contingent on each other (Delmestri, 2009; Miller, 2009; Perri, 2005). For example, while freshwater is unaffected, an event can impact the electricity grid, resulting in pumps not working and therefore unable to provide water to the customers. One way of analysing interdependencies is to take on a value-chain analysis approach, which consists of two parts, support and primary activities (Porter, 1985). Primary activities describe the flow of material and information within the organisation and how they add to value creation. Support activities span the primary activities and provide input by making IT, infrastructure, personnel and other resources available. Interdependencies are points where the output from one activity crosses from one to another within the value chain. For example, from inbound logistics to production, there will be a series of processes that need to take place to produce output or where they rely on support activities to function, for example, the availability of IT systems or qualified personnel. We can use a value chain approach to reduce the number of critical activities needing protection or, if an event occurs, needing to be recovered by concentrating on these independencies.

Robustness of critical activities

The fourth element is to establish the robustness of each of the critical activities. Robustness is the ability of a social system to absorb disruptive events and, at the same time, retain operational integrity (Hassel & Cedergren, 2021; Woods, 2019). Estimating the robustness level is conditional on the occurrence of a risk event, which means that it is impossible to know the full extent of the system's ability to absorb a hazard without the event occurring. Activities will produce output, not at the same level but as a percentage of the optimal operation during an

event. For example, a company with only one central production facility will have lower robustness than one which applied a system with multiple production facilities that could take over some of the processes in the case of an event. A hospital will switch to generators in case of a power outage and provide a minimum power level to essential services. A university can revert to online teaching if the classrooms are unavailable, thus continuing to educate, albeit at a lower activity level.

While the robustness part of the BIA intends to provide evidence as to the minimum functional level of a process, it also provides input to the analysis that follows, by providing decision makers with insights into the vulnerability the organisation currently possesses. The robustness analysis is critical for two reasons. First, it is needed to determine the organisation's vulnerability and hence the minimum operating level for each critical activity, as described above. But it is also required to identify activities considered fragile and in need of resources to increase their robustness. Expanding the organisation's ability to cope with adverse events means that it will make investments that will strengthen the preventive and protective barriers.

Figure (2) below illustrates how adjustments to the level of robustness will improve recovery time. The process consists of three phases: before, during and after an event. The figure on the left shows how a process will be affected and recovered if the organisation takes no action (also called natural recovery time). Before the event, the critical activity will be at its optimal efficiency, e.g. 100%. When the social system manages the event, the activity will be at its lowest possible level, which means that it has triggered its vulnerability. As seen on the left side of figure 2, the social system can reduce recovery time by manipulating the robustness level through preventive barriers. For example, a fire might take the same time to manage before recovery can commence, but, with a higher level of robustness, the recovery time will be shorter. In the example on the left, the robustness is at 20% efficiency. The critical activity recovers as the organisation strives to recuperate from the impact. The right side of the figure shows the time it takes if robustness increases to 50%, which will significantly reduce the recovery period for the critical activity. As depicted, an increase in robustness level will also directly translate into an improvement in recovery time, thereby creating value.

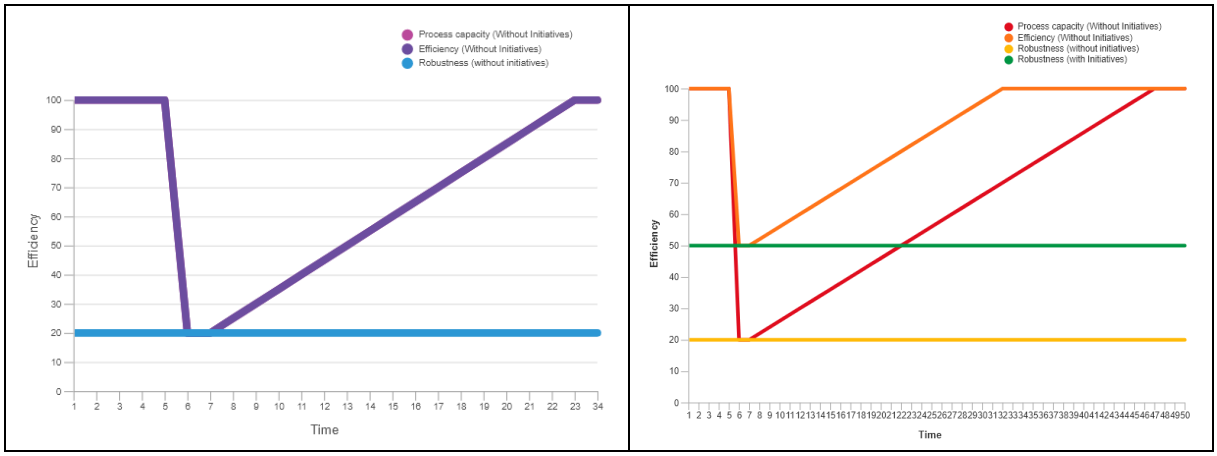

Figure 2 Robustness and recovery

There are three levels of response to an event that a critical activity can have. "No response" is when the barriers do not reach the resistance threshold. In the second level, the resistance increases until one of two outputs occurs, recovery or failure. At the third level, we find the consequence of an event that surpasses the recovery threshold. Recovery is still possible as long

as the barrier response is below the maximum robustness threshold. Failure means exceeding the barrier's robustness level, triggering its vulnerability. For a system to be characterised as robust, it needs to respond to disturbances in a way that means it continues to produce the same output despite changes in context. For example, a social system can construct a preventive barrier to stop a wildfire and invest in the maintenance of firebreaks, thereby preventing a fire hazard from having consequences. The firebreak will have no effect under normal conditions, e.g. no response. When there is a wildfire, the robustness of the barrier responds to the disturbance, and, as the fire spreads, the system response becomes more prominent. As long as the fire stays within the robustness threshold of the firebreak, the community will be safe. If the event surpasses the recovery threshold, the firebreak will fail, triggering its vulnerability and further escalation of the wildfire. The social system then deploys its protective barriers, e.g. us of water hoses or construction of new firebreaks.

Internal and external resources

It is necessary to be aware of the internal and external resources to support preventive and protective barriers. The robustness of critical activities relies on the resources that the social system can mobilise in an event. At this level, the analysis describes and quantifies the physical and intellectual resources that the system relies on to produce its desired output, such as access to personnel, equipment, tools, buildings, road infrastructure, water, electricity, gas, communication and waste management systems. Decision makers can utilise physical and intellectual resources to protect and restore critical activities. Physical resources could be the ingredients for specific processes that the social system cannot produce, such as fuel for vehicles, lubricants, supplied semi-manufactured goods, etc., and structures such as dikes or roads. Understanding the consumption of different resources will help determine minimum storage requirements and how long the social system can function given their availability. Access to intellectual resources is the competency needed to manage an event if it should occur and assist the recovery of the critical activity. Having plenty of people available does little good if they do not have the necessary qualifications to operate the equipment. Some personnel will be essential, and it would be difficult for the social system to produce value if their skills were not present. These could include IT support, finance, process specialists, middle managers, etc.

Maximum tolerable downtime

The maximum tolerable downtime (MTD) describes the point in the future at which the social system will no longer be able to provide value (Elliot et al., 2010; Hiles, 2014). The MTD is the point in time when recovery of a critical activity becomes unsustainable for economic, cultural or social reasons. The point at which something is deemed unacceptable is when the cost of recovery is higher than the value creation. Decision makers need to know when it is no longer in the interests of the social system to recover a specific activity and when to change their priorities. For example, a company experiencing a flooding event at some of its production facilities can divert resources to other less compromised sites and improve the recovery of less affected critical activities. When assessing the MTD for each critical activity, it is central that the social system considers and justifies the response. A prevailing assumption is that the faster you recover, the more significant the value you preserve. However, this might not necessarily be the case, as the cost of recovery, such as moving staff from one location to another, changing suppliers, or setting up alternate production sites, might take longer and will incur a higher cost than the MTD justifies. Defining MTDs is thus a tool that can aid decision-making on how to

prioritise when handling an evolving event that leaves little time to debate where the organisation's spare resources should go.

Some organisations require data as part of value creation, so not having access to data might mean significant losses. The equivalent of the MTD for access to data is the Maximum Tolerable Data Loss (MTDL), which refers to how much information the critical activity can lose before it is impossible to recover (Hiles, 2014). The MTDL specifies how old the data may be, if recovery is possible, without severely reducing the ability to produce value. There are several cases where companies have had to pay ransoms, as they were denied access to their data due to hacking or malware. For example, the shipping and logistics company Maersk was denied access to their shipping system in 2017, which caused a loss of millions of USD; a similar event impacted the facility service company ISS in 2020 (Goud, 2020; Greenberg, 2018). Hence, defining the MTDL also has a series of consequences attached to it, as the social system needs to ensure that there is no external force and to intervene with its stored information.

Recovery time

The final part of the analysis involves defining the recovery time for each critical activity. The recovery time objective (RTO) expresses the aspiration to fully recover a given activity (Hassel & Cedergren, 2019; ISO, 2012). The RTO is a managerial desire to restore processes faster than the MTD, given that interdependencies exist between different critical activities within the organisation, their robustness and resource availability. For example, access to power might have an MTD of several days, while activities such as production, logistics or communications are reliant (interdependent) on much faster access to such services. A shorter RTO can also stem from an ambition to meet customer demands for specific products, thereby increasing market share during an event or other considerations related to the business model. For some social systems, the pressure to recover can be political, as the recovery of specific activities is deemed essential.

The recovery point objective (RPO) refers to the age of the data or information that the organisation works with (Gibb & Buchanan, 2006; Tammineedi, 2010). It aims to restore access to data so that it does not affect the ability of the organisation to produce value. In some cases, this means restoring data to the status immediately prior to an event or to an earlier position hours, days or weeks before. Many processes within the organisation and directly related to the business model require processing data. In some cases, it is possible to conduct operations with ease using several months or years-old information. However, for many social systems, value creation is based on having access to up-to-date and readily available information about customers, suppliers and other stakeholders. The specific RPOs for critical activities requiring information as input depend on the MTDL, given how the organisation produces customer value. Figure 3 below depicts the RPO and RTO for a given critical activity.

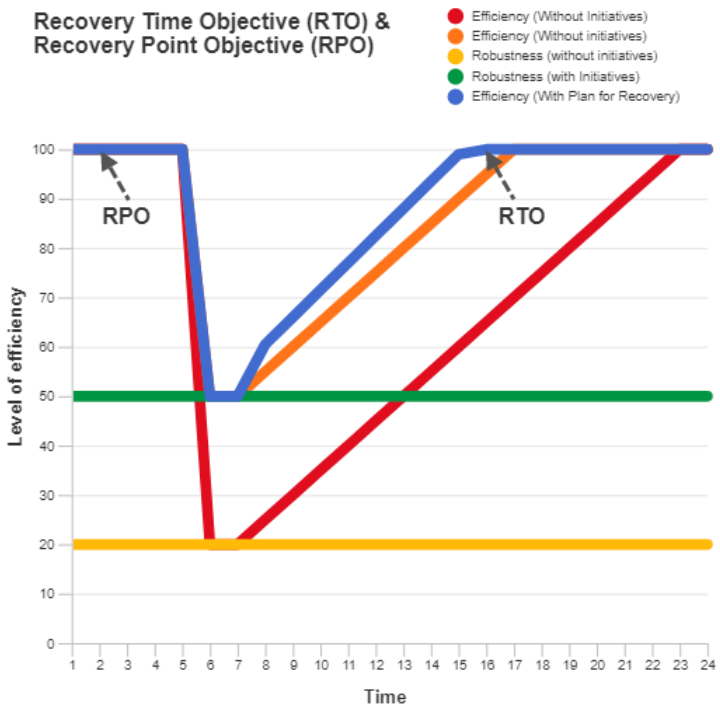

Figure 3 RPO and RTO for a critical activity

The risk reduction plan (RRP) and the business continuity plan (BCP)

BIA helps decision makers reduce vulnerability and increase recovery times, by developing risk reduction plans (RRPs) and business continuity plans (BCPs) for each critical activity (see figure 4). The bow-tie model is widely used in risk management and serves as an analytical tool in many organisations (Jacinto & Silva, 2010; Markowski & Kotynia, 2011). The analysis includes the complete event scenario, compounded by a fault tree (the left side), which identifies causes, and an event tree (the right side), which deals with the consequences of an incident once it is realised. A series of preventive and protective barriers exist that will either prevent the event from materialising or protect the organisation if it does (Delvosalle et al., 2006; Kurowicka et al., 2008). These barriers are physical or organisational structures that, in different ways, prevent a hazard from becoming an event and further develop into tangible consequences that result in a loss.

The lines in the model depict how hazards can be stopped by the different barriers or materialise as a consequence that the organisation will need to manage. To be considered relevant, barriers must have a realistic chance of preventing a hazard from becoming an event or an event from having consequences. A barrier can produce three types of outcomes: prevention, mitigation or failure. The outcome depends on its robustness and the degree to which it targets a particular hazard. In this way, the barrier is acting like a reducer of impact and a delayer of frequency, diminishing the overall effect that the hazard might have later.

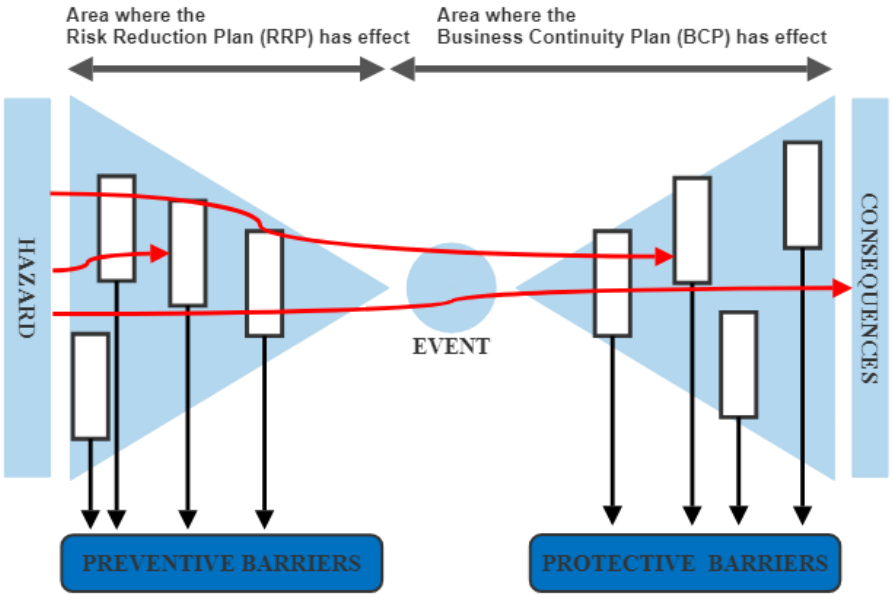

Figure 4 Bow-tie and BCM

BCM works to improve both preventive and protective barriers. The RRP's function influences robustness and thereby the minimum level at which a critical activity will operate. The strategic nature of these plans focuses on the increase in robustness towards identified vulnerabilities. Such efforts can include investments in infrastructure and suggestions to relocate a critical activity to an alternate site, thereby providing better opportunities to build preventive barriers. In this sense, the RRP is a strategic tool that organisations use to increase the robustness of critical activities.

The BCP describes the organisation's actions if an event should occur (see figure 5). The plan includes the organisation's activities during and in the recovery phase. The input to the plan comes from the BIA as the events that potentially could impact the organisation's critical activities.

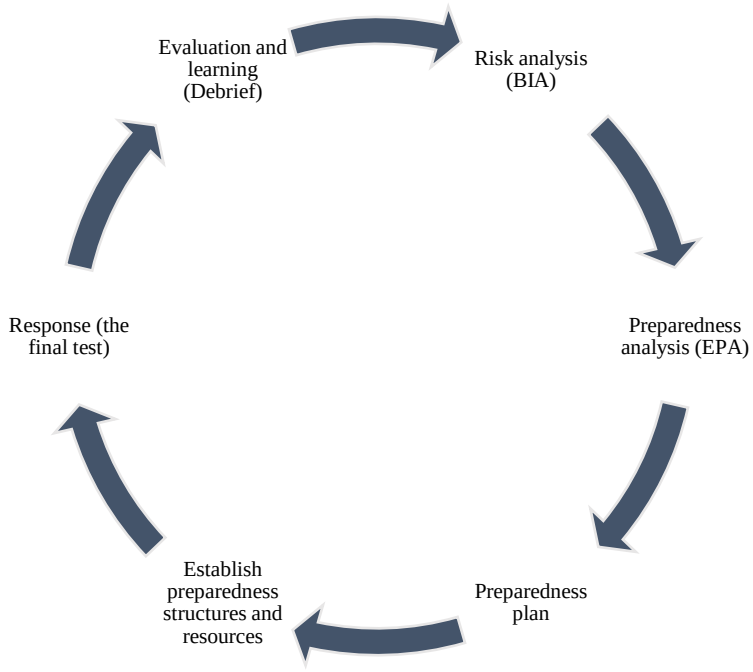

Figure 5 The BCP process

The BIA establishes the fundamental premise for what type of hazard events could potentially impact the organisation's critical activities. Based on the input from the BIA, it is possible to create an emergency preparedness analysis (EPA). The purpose is threefold. First, it establishes the organisation's emergency preparedness level, by defining situations of hazards and accidents that fall under the jurisdiction of emergency preparedness. Second, the analysis supports setting a standard for emergency preparedness that defines emergency response strategies and performance requirements. The final purpose is to identify the technical, operational and organisational emergency response measures needed to cover whatever is necessary to meet performance requirements to establish an effective protective barrier.

A preparedness plan can be created, based on the BIA and EPA, establishing the realised response to each prioritised risk scenario. The document is a guide for crisis management and includes all aspects of a possible risk event. As a minimum, the plan consists of the objective that it aims to achieve (scope), contexts, roles and responsibilities, coordination and management, standard operating procedures, required resources (human and technical), escalation plan (in case an event is out of scope for the response), stakeholder communication and revision number/date.

The "preparedness structures and resources" theme identifies, in practical terms, the resources needed for a successful protective barrier, given the scope of the emergency plan. Preparedness includes incident management, competencies and technical resources, communication and coordination with key stakeholders. The focus here is on the realised capacity of the emergency response rather than that described in the preparedness plan. The organisation uses the theme to identify potential gaps between what is envisioned during the analytical phase and the actual capacity of the emergency response to enact.

It is possible to train specific parts of the BCP, ranging from simple to complex events, including walkthroughs, workshops or orientation seminars, tabletop, functional and full-scale exercises. Depending on input from the "preparedness structures and resources" theme,

different emphasis can be placed on gaps identified, new staff or changes made to standard operating procedures deployed by the organisation. The response can be an exercise where preparedness plans are rehearsed or in the form of an actual event where enactment comes from a realised risk event. A risk event is the best way to test the alignment between plans, resources and competencies with organisational goals to meet its RTO or RPO.

Evaluation and learning is a structured and systematic approach to improve the process of a risk-based approach to dimensioning. An effective emergency response centre is based on the idea that the right resources are available and utilised effectively when a hazard is realised. In practice, this means that the knowledge and capacities developed by governments, professional response and recovery organisations, communities and individuals can be used to anticipate effectively, respond to, and recover from, the impacts of likely, imminent or current hazard events or conditions (UNISDR, 2012). After a response, the organisation debriefs its members, to identify key learning points and gaps in the emergency plan, preparedness structure, and the applied resources. These key learning points are subsequently used in the following risk analysis, whereby the emergency response organisation can enter into a virtuous circle of continuous improvement.

Concluding remarks

This paper has discussed the application of the BIA and BCP, illustrating how managers use the tool to make decisions that will reduce vulnerabilities and make social systems resilient to significant changes in their environment. A good and thorough BIA can act both to analyse business continuity challenges and vulnerabilities and as a tool for effective crisis management. There is no uniform set approach to conducting a BIA but plenty of advice concerning which standard structure to follow, based on the sector- industry- and organisation-specific needs. This paper has sought to explore what an analytical approach could look like, given that the overall aim is to restore critical activities and thereby protect or restore something of value for the organisation and its stakeholders. While the example used focuses on a context and event situated in a setting considered abnormal by most, it does provide some valuable insights. The structure offers a simple approach for determining when something an organisation does is critical to its value creation. Using the BIA simplifies and reduces the number of key focus points included in the RRP and BCP, but it is also a strategic tool that the organisations can utilise to prioritise their resources, as seen in the wildfire example. The outcome is a set of suggestions for how a given social system can invest strategically in creating more robust preventive barriers. The BCP is concerned with what the social system plans to do if an event should emerge, should these barriers not hold.

Literature

Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015). Operational Models of Infrastructure Resilience. *Risk Analysis*, *35*(4), 562–586. https://doi.org/10.1111/risa.12333

Anbumozhi, V., Fukunari, K., & Thangavelu, S. M. (2020). Supply chain resilience. In V. Anbumozhi, K. Fukunari, & S. M. Thangavelu (Eds.), *Handbook of Research on Global Supply Chain Management*. Springer International Publishing. https://doi.org/10.1007/978-981-15-2870-5

Anthony, L., & Cox, T. (2012). Community Resilience and Decision Theory Challenges for Catastrophic Events. *Risk Analysis*, *32*(11). https://doi.org/10.1111/j.1539-6924.2012.01881.x

Aven, E., & Aven, T. (2015). On the Need for Rethinking Current Practice that Highlights Goal Achievement Risk in an Enterprise Context. *Risk Analysis*, *35*(9), 1706–1716. https://doi.org/10.1111/risa.12375

Aven, T., & Flage, R. (2020). Foundational challenges for advancing the field and discipline of risk analysis. *Risk Analysis*, *40*(S1), 2128–2136. https://doi.org/10.1111/risa.13496

Barnes, P. (2011). Business Impact Analysis. In Andrew. Hiles (Ed.), *Definitive Handbook of Business Continuity Management* (pp. 166–182). John Wiley & Sons inc.

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, *49*(18), 5375–5393. https://doi.org/10.1080/00207543.2011.563826

ClimateCost. (2021, December 19). *Economics of climate change*. ClimateCost. http://www.climatecost.cc/reportsandpublications.html

Curt, C., & Tacnet, J. (2018). Resilience of Critical Infrastructures : Review and Analysis of Current Approaches. *Risk Analysis*, *38*(11). https://doi.org/10.1111/risa.13166

Delmestri, G. (2009). Institutional streams, logics, and fields. In *Research in the Sociology of Organisations* (Vol. 27). Elsevier. https://doi.org/10.1108/S0733-558X(2009)0000027006

Delvosalle, C., Fievez, C., Pipart, A., & Debray, B. (2006). ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. *Journal of Hazardous Materials*, *130*(3 SPEC. ISS.), 200–219. https://doi.org/10.1016/j.jhazmat.2005.07.005

Elliot, D., Swartz, E., & Herbane, B. (2010). *Business Continuity Management*. Routledge.

Franzosi, R. (1987). The press as a source of socio-historical data: Issues in the methodology of data collection from newspapers. *Historical Methods: A Journal of Quantitative and Interdisciplinary History*, *20*(1), 5–16. https://doi.org/10.1080/01615440.1987.10594173

Freeman, R. E., & Reed, D. L. (1983). Stockholders and Stakeholders: A New Perspective on Corporate Governance. *California Management Review*, *25*(3), 88–106. https://doi.org/10.2307/41165018

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, *26*, 128–141. https://doi.org/10.1016/j.ijinfomgt.2005.11.008

Goud, N. (2020). Ransomware attack on ISS World. *Cybersecurities Insiders*.

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information and Libraries Journal*, *26*(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Greenberg, M. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*.

Hanna, E., Cappelen, J., Fettweis, X., Mernild, S. H., Mote, T. L., Mottram, R., Steffen, K., Ballinger, T. J., & Hall, R. J. (2021). Greenland surface air temperature changes from 1981 to 2019 and implications for ice-sheet melt and mass-balance change. *International Journal of Climatology*, *41*(S1), E1336–E1352. https://doi.org/10.1002/joc.6771

Harvey, E. J., Waterson, P., & Dainty, A. R. J. (2019). Applying HRO and resilience engineering to construction: Barriers and opportunities. *Safety Science*, *117*, 523–533. https://doi.org/10.1016/j.ssci.2016.08.019

Hassel, H., & Cedergren, A. (2019). Exploring the Conceptual Foundation of Continuity Management in the Context of Societal Safety. *Risk Analysis*, *39*(7). https://doi.org/10.1111/risa.13263

Hassel, H., & Cedergren, A. (2021). Integrating risk assessment and business impact assessment in the public crisis management sector. *International Journal of Disaster Risk Reduction*, *56*(January), 102136. https://doi.org/10.1016/j.ijdrr.2021.102136

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, *52*(6), 978–1002. https://doi.org/10.1080/00076791.2010.511185

Hibberd, G. (2011). Developing a BCM strategy in line with Business strategy. In Andrew. Hiles (Ed.), *The Definitive Handbook of Business Continuity Management* (pp. 23–30). John Wiley & Sons inc.

Hiles, Andrew. (2014). *Business continuity management : global best practices, fourth edition* (Kristen. Noakes-Fry, Ed.; 4th ed.). Rothstein Associates.

ISO. (2012). Societal security – Business continuity management systems Requirements. *BSI Standards Publication*, 36.

Jacinto, C., & Silva, C. (2010). A semi-quantitative assessment of occupational risks using bow-tie representation. *Safety Science*, *48*(8), 973–979. https://doi.org/10.1016/j.ssci.2009.08.008

Kurowicka, D., Cooke, R., Goossens, L., & Ale, B. (2008). Expert judgment study for placement ladder bowtie. *Safety Science*, *46*(6), 921–934. https://doi.org/10.1016/j.ssci.2007.11.013

Markowski, A. S., & Kotynia, A. (2011). “Bow-tie” model in layer of protection analysis. *Process Safety and Environmental Protection*, *89*(4), 205–213. https://doi.org/10.1016/j.psep.2011.04.005

Miller, K. D. (2009). Organisational risk after modernism. *Organisation Studies*, *30*(2–3), 157–180. https://doi.org/10.1177/0170840608101475

Ning, W., & Wong, Z. (2009). The strategic skills of business continuity managers : Putting business continuity management into corporate long-term planning. *Journal of Business Continuity & Emergency Planning*, *4*(1), 62–69.

Norsk Klimaservicesenter. (2019). Climate in Svalbard 2100 – a knowledge base for climate adaptation. In *NCCS report no.1/2019* (Issue 1).

Osterwalder, A., & Pigneur, Y. (2009). *Business Model Generator* (T. Clark, Ed.). Self-published.

Perri. (2005). What’s in a frame? Social organisation, risk perception and the sociology of knowledge. *Journal of Risk Research*, *8*(2), 91–118. https://doi.org/10.1080/1366987032000081213

Porter, M. E. (1985). *On Competition* (1st ed.). Harvard Business School Publishing.

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*, *27*(653390), 632–641. https://doi.org/10.1016/j.ijdrr.2017.08.006

Sawalha, I. H., & Anchor, J. R. (2012). Business continuity management in emerging markets : The case of Jordan. *Journal of Business Continuity & Emergency Planning*, *5*(4), 327–337.

Swiss Re Institute. (2021). *The Economics of climate change: no action not an option*. https://www.swissre.com/dam/jcr:e73ee7c3-7f83-4c17-a2b8-8ef23a8d3312/swiss-re-institute-expertise-publication-economics-of-climate-change.pdf

Taarup-Esbensen, J. (2020). The Business Impact Analysis. *Working Paper*, *1*(1), Article 1.

Tammineedi, R. L. (2010). Business Continuity Management : A Standards-Based Approach. *Information Security Journal: A Global Perspective*, *19*, 36–50. https://doi.org/10.1080/19393550903551843

Turnowsky, W. (2017, August 7). Den største brand, jeg kan erindre. *Sermitsiaq*. https://sermitsiaq.ag/node/197790

UNISDR. (2012). Disaster risk and resilience. In *Disaster Risk and Resilience* (Issue May). http://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/3_disaster_risk_resilience.pdf

WEF, W. E. forum. (2021, June 28). *This is How Climate Change Could Impact The Global Economy | World Economic Forum*. Uplink. https://www.weforum.org/agenda/2021/06/impact-climate-change-global-gdp/

Woods, D. D. (2019). Essentials of resilience, revisited. In M. Ruth & S. Goessling-Reisemann (Eds.), *Handbook on Resilience of Socio-Technical Systems* (pp. 52–65). Edward Elgar Publising ltd. https://doi.org/10.4337/9781786439376.00009

Yin, R. K. (1994). *Introduction and designing case study - Case study research Design and methods* (2nd ed.). SAGE Publications. https://doi.org/10.1017/CBO9780511803123.001

Zsidisin, G. A., & Henke, M. (2019). *Revisiting Supply Chain Risk* (G. A. Zsidisin & M. Henke, Eds.). Springer International Publishing.