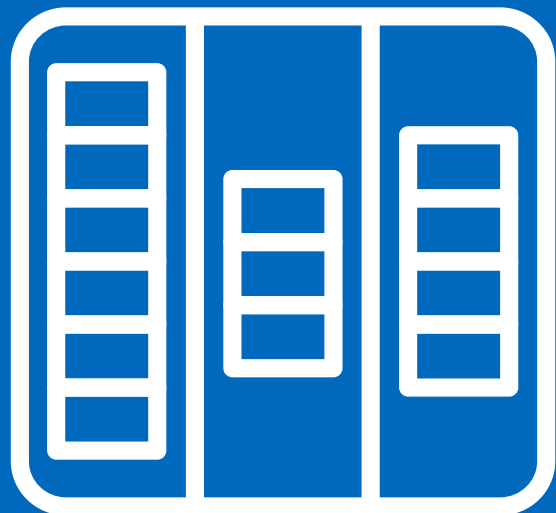
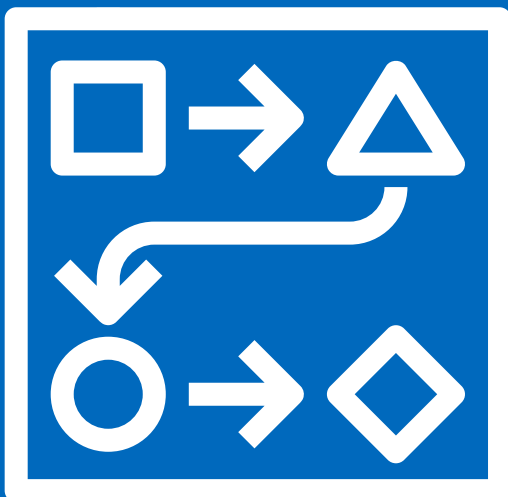
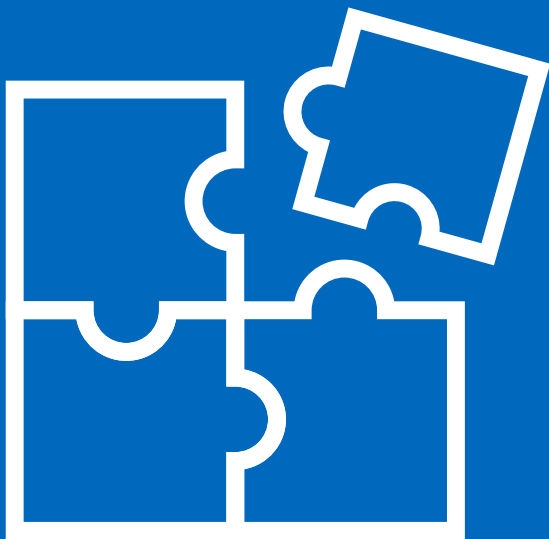


# Guide to Building a Business Case for Business Continuity Management



# The state of business continuity management in the age of Covid-19

In the midst of the Covid-19 crisis, it seems business continuity plans (BCPs), processes, and programs have never been in greater demand, as the C-suite wakes up to the need to adequately prepare for continuity events that could impact prioritized activities. But before business continuity managers get too confident in their ability to build sustainable programs going forward, they need to take a trip down memory lane, because we've been here before.

Both the 11 September 2001 terror attacks and late 2000's financial crisis spurred similar upticks in the popularity of business continuity management systems (BCMS). After both crises, federal, state, and local governments even went so far as to put new statutes on the books, mandating a base-level of business resilience among organisations operating in their jurisdictions – we can expect something similar coming out of this present public health crisis.

Despite those previous measures, the interest in business continuity management soon waned. Indeed, by the time Covid-19 came along, an alarming number of companies were unprepared, with some surveys pointing to majorities of up to 70 percent of companies lacking pre-existing disaster or crisis plans<sup>i</sup> - and that was even after close shaves with the SARS outbreak (2003), Swine Flu (2009), and Ebola (2014).

Other surveys put the percentage of companies with a business continuity plan (BCP) at the outset of the pandemic closer to 65 percent<sup>ii</sup>. But just below that top line, the numbers were troubling. Of the organizations that had BCPs, only 22 percent had plans that covered contingencies for more than two months, while the plurality, 48 percent, had BCPs that only covered two to three weeks-worth of emergency operations<sup>iii</sup>.

When it came to provisions for remote working, companies were even less prepared. Only 37 percent of companies had the right technology in place for employees to conduct critical operations from home in the event of an emergency. Meanwhile, almost 20 percent of companies said that none of their employees could do their jobs from home due to a lack of technology equipment owned and distributed by the company<sup>iv</sup>.

Clearly, an awareness of business continuity management hasn't yet produced well-resourced business continuity programs. How can continuity managers change the calculus in the era of Covid-19? Creating a business case for sustainable business continuity resources is a good place to start, especially if you need to demonstrate value, obtain approval, decide whether to outsource, prioritize projects, and secure funding. And this guide provides you the keys to how to populate one.


## A checklist of business case elements

What the business case explains	How the business case is structured
<ul style="list-style-type: none"> <li>Objectives</li> <li>Outlines the business need</li> <li>Provides relevant context and supporting information</li> <li>Describes how investment aligns with the organization's larger strategy</li> <li>Estimates whole-of-life costs and benefits (financial and non-financial)</li> <li>Provides timelines, resources, procurement strategy, and governance</li> <li>Quantifies risk and uncertainty</li> <li>Provides options</li> </ul>	<ul style="list-style-type: none"> <li>Executive summary</li> <li>Project definition</li> <li>Business requirements</li> <li>Evaluation of options</li> <li>Recommendation</li> <li>Project logic</li> <li>Benefits</li> <li>Risks</li> <li>Project stages and duration</li> <li>Financial analysis</li> <li>Estimate of project team resources</li> <li>Project authorization</li> </ul>

STEP 1

## Lay out the numbers.

How to build that case? Start with an executive summary that lays out the numbers. For one, the research clearly indicates that a failure to properly prepare for crises increases the risk of post-crisis business closure. Roughly 40 to 60 percent of small businesses close after a natural disaster, according to the U.S. Federal Emergency Management Agency (FEMA) – rates largely driven by the overwhelming 90 percent of businesses that fail because they can't resume operations within five days.



**Between 40 to 60%**  
of small businesses  
in the U.S.  
close following a  
natural disaster

Why can't they? Well, it could be because 20 percent don't spend any time maintaining their continuity plans, including provisions for IT redundancy, data management, and emergency supplies.

What's more, the pace of crisis is accelerating. Weather-related disasters are increasing apace, with The Economist tracking a 400x increase since the 1970s<sup>v</sup>. But natural disasters aren't the only threats organizations face. A 2018 Forrester study revealed that a full 100 percent of surveyed organizations confronted at least one critical event in a 24-month period – many responded to multiple crises, with the average being four.

From where do those threats issue? Well, according to the BCI Horizon Scan Report 2020 put out by the BSI Group, health and safety incidents, IT and telecom outages, cyber-attacks and data breaches, and lack of talent/key skills were 2019's leading disruptions<sup>vi</sup>. Forecasted top disruptions in 2020 included cyber-attacks and data breaches, IT and telecom outages, critical infrastructure failure, and lack of talent/key skills<sup>vii</sup>.

Add to that, organizations facing one critical event – say a global health crisis – aren't inoculated against a simultaneous hit from another critical event. Instead, without proper planning, they are more vulnerable. Largely unplanned for, the sudden rise of remote working arrangements, as a response to government-mandated lockdowns, was accompanied by a surge in cyber activity<sup>viii</sup>. Further, as many regions enter severe weather season, natural disasters – from earthquakes, hurricanes, tornadoes, floods, etc. – will continue to be a threat, while organizations in those regions still respond to the Covid-19 crisis.

As has become obvious, these disruptions all have material impacts on the organization's bottom line – the likeliest being:

-  Loss of productivity
-  Negative impact on staff morale/wellbeing
-  Customer complaints
-  Reputation damage
-  Revenue loss

The direct cost of unplanned downtime, in particular, can be significant. According to Gartner, the average cost of IT downtime is USD 5,600 per minute or USD 300,000 per hour, going up to as much as USD 540,000 per hour on the high end<sup>ix</sup>.

If you've suffered from disruptions before, highlight the relevant incident<sup>x</sup> in your business case, to make the procurement decision more relevant to senior leadership. Document the monetary cost of responding to the incident in question. Then, provide the subscription price of the vendors you have shortlisted – you might want to do this in a later section – that would have mitigated the above-mentioned threat. The delta between the cost of the incident and the subscription price represents the return on investment for your continuity solution.

Do not forget non-direct impacts from productivity loss, depressed morale, customer complaints, and reputation damage, which can be just as stark. In studies, those impacts actually proved of greater consequence to businesses than the direct monetary hit from loss of revenue.

**STEP**  
**2**

## Define the aims of the business continuity program.

Those numbers will open eyes. But you haven't made your case quite yet. Sure, the risk picture has darkened appreciably, and under-

prepared companies, specifically, stand to lose employee engagement and productivity, customers, and, of course, revenue. You will still have to prove that the ROI of value-creating business continuity resources, i.e. risk mitigation. For, the question always is: how will allocating the requested resources minimize brand damage and the risk of interruption to prioritized activities? Focus on the concrete ROI in the strategic logic for your project:



Reduces likelihood of losses by identifying ways to prevent or mitigate threats.



Ensures compliance by dedicating resources to minimize the risk of compliance violations.



Helps retain existing and secure new business by showing customers that their assets will be protected.

Time to define terms – starting with what business continuity management is. Business leaders might be surprised. As practiced today, business continuity management is a holistic management process for identifying potential threats to an organization and the operational impacts those threats would pose. It's the role of business continuity professionals to build a durable framework for organizational resilience, in compliance with regulations and prevailing business standards like ISO 22301.

The BCP is a mainstay of the practice (more on that later). Designed to prepare organizations to maintain essential functions in the event of a disaster or other major disruption, the BCP is a collection of resources, actions, procedures, and information<sup>xi</sup>. And it's this planning effort that enables the continuous delivery of critical services and products to customers. Indeed, the BCP has two important objectives:



Ensuring critical operations continue to be available



Minimizing impacts to the business, irrespective of the type of incident or disruption

The aims of business continuity resources shouldn't be expansive – at least not in the initial business case. Instead, the resources should solely address the organization's most critical functions. Here, the business case can turn into a conversation with stakeholders; what qualifies as business-critical and therefore in scope for the project. Part of building the business case is understanding who those primary stakeholders are and finding out what their requirements are.

Also, steer clear of some of the landmines in your business case. For one, business continuity often gets dismissed as a mere auditory function, rather than a value- and revenue-creating function that aligns with the business's larger objectives. You will need to make the case that business continuity will make a proactive intervention in the lifecycle of critical products and services, by being the only function with a clear map of all of the business units, activities, and resources (more broadly) that support the delivery of critical products and services.

That map will help senior management quantify its appetite for risk (including precise enumerations of acceptable downtimes), should there be disruptions to critical products and services. Any downtimes exceeding the prescribed become in-scope for the function. This glossary of key continuity concepts might help:

<b>Prioritized Activity</b>	Those activities essential to deliver outputs and achievement of business objectives.
<b>Maximum acceptable outage (MAO)</b>	The time an activity can be disrupted before its loss becomes unacceptable and significantly impacts the organization.
<b>Recovery Time Objective (RTO)</b>	The time from which you declare a crisis/disaster to the time that prioritized activities must be fully operational in order to avoid serious financial loss.

## STEP 3

# Include relevant assets that reflect the context of your organization.

Concepts are one thing. Creating relevant assets that garner C-suite buy-in is quite another. The first asset consists of the business impact analysis (BIA), diagnostic of a business's internal dependencies and vulnerabilities, which provides the analytical baseline for developing (later) BCP materials.

Too often, continuity managers get waylaid at this juncture. The BIA process gets overly complicated, divorced from immediate business realities. Not the whole kitchen sink, the BIA should offer senior management a bird's eye view of the prioritized activities that generate the most money or benefits to the organization, how badly those activities would be impacted by a disruption, as well as insight into the pathways by which impact would possibly take place.

It is these interdependencies that the business impact analysis is particularly focused on identifying and quantifying, with the analysis itself serving as a necessary prerequisite for an informed prioritization of assets to protect and the relevant recovery actions to initiate in the case of an emergency.

That kind of impact analysis is oriented towards critical indicators that sum up the "breaking point" for business operations. That's the maximum amount of damage an operation can sustain before the business is functionally dead in the water (maximum acceptable outage), and, of course, the resources required to return operations back to functional (strategies for recovery).

To be practical, the process must surface recovery requirements that will later be used to develop discrete strategies, solutions, and plans for overcoming operational vulnerabilities, i.e. the BCP, which will also cover the other resources, services, and activities necessary to ensure the continuity of prioritized activities, including:



Organizing objectives and driving principles. The primary objective of your plan is to ensure maximum possible services levels are maintained. Meanwhile, assessing business risk for probability and impact might also be an important principle to document.



The objectives and principles sections might be part of a longer executive summary, a comprehensive overview of the BCP<sup>xii</sup>.



References. Helpful information might include links to the appropriate state and federal regulator, e.g. Emergency Management Australia.



Relevant standards with which the plan complies, e.g. ISO 22301.



The contents of the BIA, including a list of likely threats, i.e. building loss, document(s) loss, systems going offline, loss of key staff, etc.



A list of relevant company, insurance, and supplier contacts.



Provide scenario planning for the risks you've identified. Once the risk is listed, the BCP outlines probability and impact of occurrence, likeliest scenario(s) to unfold, business functions affected, actions to take and preventative mitigation strategies, staff responsibilities, as well as operational constraints.

## STEP 4

# Ask for the right resources to maintain acceptable risk levels.

Producing assets that are relevant to the context of your organization will help strengthen a business case for contingency planning resources that are proportionate to the task of maintaining acceptable risk – once measured.

What would those resources look like? Well, business continuity technology should be part of the project scope. And there's research to back that up. In crisis, every minute matters. But only one third of organizations can activate emergency communications plans in five minutes, according to BCI. Ten percent take more than an hour.

Manual processes, practices, and systems just won't cut it. Indeed, failure of manual processes gets cited as the reason for the failure to achieve accepted response levels over 25 percent of the time<sup>xiii</sup>. Further, gathering, validating, and sharing accurate information, communicating with staff, customers, and other stakeholders, as well as getting staff to follow planned procedures remain key business continuity challenges, all of which are either caused or exacerbated by manual processes<sup>xiv</sup>.

The investment in technology and increased dedication to training and exercising also has a positive ROI. Seventy-three percent of organizations who've made that investment achieve their expected response levels<sup>xv</sup>.

Of course, not all business continuity management software is created equal. Indeed, stark limitations exist on both ends of the market, as you should address when evaluating options. So-called point solutions, while affordable, offer limited functionality and thus a poor return on investment (ROI), based on the sheer number and variety of potential threats and continuity events that can disrupt the average firm every day. Conversely, too complex can be an issue, too. At that end of the market, costs tend to be prohibitive – definitely not in scale with quantified risk. Further, those solutions often require lengthy configurations before getting up and running which will balloon your estimates for project team resources.

Instead, you should make the procurement case for practical business continuity technology with all the tools needed to effectively assess business risks and impacts, coordinate responses to disruptions, and manage incidents. The features and functionality to look out for include:



### Exercise management.

It's a no-brainer, but business continuity software actually needs to respond to business interruptions efficiently. To do so, teams need to first activate tested, best-practice plans and strategies. And following the response, teams need to document and internalize lessons learned during the recovery stage. Unfortunately, that's where most BCM software falls down: too little planning and review-related functionality. The best ROI will come from a solution that provides a comprehensive library of crisis and incident response plans and teams structures, covering anything from common disruptions to hazards scenarios. The platform will also be able to digitize those continuity, crisis, and incident response plans, including strategies and considerations, roles and responsibilities, as well as pre-assigned checklists that are ready to deploy when incidents do occur.

Still, teams shouldn't just wait for a critical event. Failure to test is a persistent challenge to effective response. By enabling teams to conduct routine exercises, software with robust exercise management functionality, or test capability, can help, however. The key is: when events do occur, plans should come to life seamlessly and teams know what they need to do, and progress gets tracked in real time.



### Automated workflows save time and effort

The system should also be able to assign and track business impact assessment and risk management activities for your organisational unit owners. It should also be able to ensure timely notifications about critical events to staff and stakeholders via email, SMS, or in-app.



### Designed with users in mind

When surveyed, organizations admit that user and usability issues are often to blame when teams fail to achieve accepted response levels. That's because the systems used aren't designed with C-level executives, continuity professionals, and business unit managers in mind. They don't include features relevant to different industries and user persona types either. Getting that level of flexibility with your solution will allow all kinds of users to report and manage business continuity incidents and issues within a single platform.

Unit specific dashboards and resources should also include well-formatted forms, lists, and processes with text guidance for proper use across different units to produce consistent and unbiased responses. These responses will then be automatically harmonized into a global dashboard, giving executives the data-driven insights they need to set actionable priorities with confidence.



## Streamlined compliance with international standards like ISO 22301

Mitigating compliance risk gives business continuity management some of its strongest ROI. Audit logging of changes and approvals of plan template and recovery strategies matter, as well. So, finding a system that gives teams notifications when exercises are due, as well as the ability to visualize all upcoming and recently completed exercises with action dashboards, as well as gaps in the process or areas for improvement to identify high-risk activities with no recovery plans and strategies is key.

Finally, the present crisis moment clarifies the need for effective business continuity resources. But somehow past crisis moments haven't quite produced the level of widespread acceptance of the value-saving business continuity resources required to mitigate risk and ensure compliance. Make this moment different by clearly laying out the business case for practical business continuity software, like Noggin for Continuity, that gives you all the tools needed to effectively assess business risks and impacts, coordinate responses to disruptions, and manage incidents.

Like what you read?  
Follow Noggin on social media



@teamnoggin



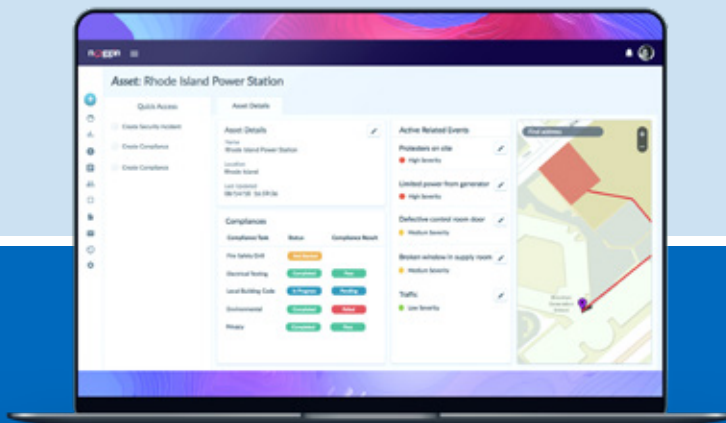
facebook.com/teamnoggin



linkedin.com/company/noggin-it

## Citations

- i *Blank Rome: Covid-19 Employer Trends Survey. Available at <https://www.blankrome.com/sites/default/files/2020-03/blank-rome-coronavirus-employer-trends-survey-results.pdf>.*
- ii *Todd R. Weiss, TechRepublic: Business continuity plans and tech are lacking during the coronavirus pandemic. Available at <https://www.techrepublic.com/article/business-continuity-plans-and-tech-are-lacking-during-the-coronavirus-pandemic/>.*
- iii *Ibid.*
- iv *Ibid.*
- v *The Economist: Weather-related disasters are increasing. Available at <https://www.economist.com/graphic-detail/2017/08/29/weather-related-disasters-are-increasing>.*
- vi *Rachael Elliot et al., BCI Group: BCI Horizon Scan Report 2020. Available at <https://www.bsigroup.com/localfiles/en-gb/iso-22301/resources/bci-horizon-scan-report-2020.pdf>.*
- vii *Ibid.*
- viii *Ray Espinoza, Tech Crunch: What you need to know about COVID-19-related cyberattacks. Available at <https://techcrunch.com/2020/04/14/what-you-need-to-know-about-covid-19-related-cyberattacks/>.*
- ix *Andrew Lerner, Gartner: The Cost of Downtime. Available at <https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/>.*
- x *Oftentimes, you will be citing multiple incidents of the same kind, e.g. IT outage.*
- xi *Stephen Woods, Yale University Emergency Management: Business Continuity Planning. Available at <https://emergency.yale.edu/planning/business-continuity-planning>.*
- xii *Queensland Government, Business Queensland: What's in a business continuity plan? Available at <https://www.business.qld.gov.au/running-business/protecting-business/risk-management/continuity-planning/plan>.*
- xiii *Rachael Elliot et al., BCI Group: BCI Horizon Scan Report 2020. Available at <https://www.bsigroup.com/localfiles/en-gb/iso-22301/resources/bci-horizon-scan-report-2020.pdf>.*
- xiv *Ibid.*
- xv *Ibid.*



# noggin

## for Business Continuity

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Business Continuity gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Business Continuity solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,  
visit: [www.noggin.io](http://www.noggin.io)  
or contact: [sales@noggin.io](mailto:sales@noggin.io)