TC NOTES

PRACTICAL **LEADERSHIP**
AND **GUIDANCE** FROM
TORONTO CENTRE

BUSINESS CONTINUITY PLANNING FOR A SUPERVISORY AUTHORITY

APRIL 2020

TORONTOCENTRE
Global Leadership in Financial Supervision

BUSINESS CONTINUITY PLANNING FOR A SUPERVISORY AUTHORITY

TABLE OF CONTENTS

BUSINESS CONTINUITY PLANNING FOR A SUPERVISORY AUTHORITY

I. Introduction[1]

Organizations need to anticipate unexpected incidents and plan how they are going to respond to them. This is not forecasting what will happen, nor calculating the probabilities of events occurring. It is assuming that incidents will occur and planning to enable the organization to continue to operate in that event.

All organizations therefore need a well-constructed business continuity plan (BCP). Supervisory authorities are no exception. Indeed, the COVID-19 outbreak demonstrates yet again the importance of business continuity planning.

This Toronto Centre Note outlines the key elements of a BCP and relates these to the specific circumstances of a supervisory authority. It provides a starting point for a supervisory authority wanting to construct a BCP, or to review and revisit its existing BCP.

If a supervisor already has rules or guidance on business continuity planning for the firms it supervises, then that might also provide a starting point for a supervisor to self-assess its own BCP.[2]

II. What is a BCP?

In essence, a BCP sets out the ways in which an organization will respond to a serious incident in order to maintain or resume its critical activities.

A BCP is broader than (but should include) a disaster recovery plan, which typically focuses on responding to disruptions to specific areas such as IT infrastructure, buildings, and a limited number of other operations.

Meanwhile, a BCP is narrower than operational resilience, which covers not only how the organization would respond to and recover from operational disruptions (in essence the BCP) but also the measures the organization puts in place to prevent such disruptions from occurring.

Similarly, a BCP is only one part of crisis preparedness and crisis management, which typically refers to disruptions that extend beyond the supervisory authority itself and that have a significant adverse impact on the wider financial system. A supervisory authority might have to activate its BCP during some types of crisis, but its BCP will not cover all aspects of crisis management.[3] Crisis management is a key activity of a supervisory authority, so one purpose of a BCP is to enable the supervisory authority to maintain or to recover rapidly its ability to undertake crisis management.

---

[1] This Note was prepared by Clive Briault.
[2] See for example Joint Forum (2006).
[3] Toronto Centre (2019b) describes the contents of a crisis binder and the activation of crisis management.

III. What is an incident?

A BCP should not focus on a specific type of incident, but should be designed to enable a supervisory authority to respond effectively to a wide range of potential incidents:

- Natural disasters – fire, flood, earthquake, volcanic eruption, snow, hurricane, tsunami, pandemics.
- Wilful damage by internal or external parties – sabotage by employees or contractors of premises, data or IT, cyber attacks, terrorist attacks, civil disorder.
- Third party failures – interruption in supply of utilities (energy, water, telecommunications), loss of third party (outsourced) supply of products and services.
- Project failures – unanticipated disruptions arising from problems with large-scale IT, building, or other change in projects.

Some incidents may affect only the supervisory authority itself (for example, a fire destroying its head office), but others may also have a disruptive impact on at least some supervised firms (for example flooding or a terrorist attack on the financial centre) or on the financial sector and the economy more generally (pandemics, loss of utilities).

IV. Constructing a BCP

We set out here six steps in the construction of a BCP, beginning with the identification of key supervisory activities.

These steps should be undertaken by a BCP team that includes staff from both the main supervision areas of the supervisory authority (authorization, supervision, enforcement, financial stability, and any key areas that may be in separate departments such as anti-money laundering) and its operational areas (IT, premises, HR, finance, outsourcing). Only the supervision areas can determine which supervisory activities are critical and what resources they need to deliver these activities.

This team should be chaired by, or at least report to, a senior individual in the supervisory authority (such as the chief executive or chief operating officer) who is responsible and accountable for business continuity planning and, along with the governing board, has the ultimate responsibility for decisions regarding priorities and activities in the event that the BCP is activated.[4]

The BCP team should discuss and develop ‘playbooks’ that cover different potential incidents, their potential impacts on key supervisory activities, and the responses that might have to be taken under the BCP as a result.

It is important that the creation, communication, testing, and updating of the BCP is owned by the board and senior management of the supervisory authority, so that the BCP is supported and promoted from the top down. The BCP should be approved by the board of the authority, and the board should ensure that accountability and responsibility for managing the BCP is clearly identified and applied. Senior ownership of the BCP is also likely to be critical to promoting staff awareness of the significance of the BCP, and buy-in to the importance of training on how the BCP would operate.

[4] Toronto Centre (2020) discusses how supervisory activities should be prioritized in the event of a major incident.

It is also important to recognize that the approach to constructing a BCP is to begin by focusing on the key supervisory activities that need to be maintained or rapidly restored. This will then inform the determination of the critical functions, people, systems, and processes that are needed to deliver these key supervisory activities. It may also be possible to deliver some of these key supervisory activities using alternative systems and processes (for example by reverting to manual processes or taking the opportunity of a major incident to upgrade the resources of the supervisory authority). A BCP is therefore not simply about restoring existing functions, systems, and processes.

In some cases – for example where a supervisory authority is situated within a central bank – the scope and coverage of a BCP may be wider than supervisory activities. In such cases, it is important that the supervisory activities are given proper weight in being correctly identified, prioritized, and covered in the BCP.

As part of the creation (or review) of a BCP, the BCP team should talk to staff of the supervisory authority (or indeed staff of other organizations) that have experienced major incidents to hear their "war stories" and what worked well or less well. This could provide valuable insights.

For example, when the staff have walked for miles to reach a back-up site, or the IT department has been working all evening to load up laptops for staff to use at home, it would be great for someone to provide food and drink to the weary. But who knows where the nearest food outlet is, and whether it is open in the evenings and weekends?

V. Step 1: Identify critical supervisory activities

In constructing a BCP, a supervisory authority should begin by identifying the most important supervisory activities it performs.

For a private corporation this might be driven by considerations of profitability and of the costs of stopping a business activity. For a public body such as a supervisory authority, the starting point here should be its mandate and objectives.

Whilst these form an essential starting point, the formal mandate and objectives of a supervisory authority will typically be rather high level and of limited help in identifying critical supervisory activities in detail. It is also necessary therefore to consider supervisory activities at a more granular level. For example, a supervisory authority will perform a wide range of activities in order to pursue mandates such as those relating to the safety and soundness of the firms it supervises, retail and wholesale market conduct, and anti-money laundering. Some of its activities may also be based more on historic custom and practices and related only indirectly to its formal objectives and hence its critical activities.

A supervisory authority should decide which of these activities need to be maintained (or resumed) as a matter of priority.

Since material incidents are by definition disruptive, some prioritization of supervisory activities needs to be contemplated when constructing a BCP. Supervisors following a risk-based supervision approach should be familiar with the thought process here – if resources are (even more) limited following an incident, then the available resources will need to be

prioritized even more towards identifying and addressing the largest risks to the supervisory authority's objectives.[5]

The criticality and prioritization of supervisory activities may also depend on the nature of the incident and whether it also has an adverse impact on supervised firms and on the financial sector or the wider economy. The need to prioritize will be reinforced if the incident is also affecting the financial sector, in which case some risks may have increased.[6]

The incident may even threaten a financial crisis of some sort, in which case management of the wider crisis may become an overriding priority for the supervisory authority, at the same time as it is having to deal with the impact of the incident on its own operations.

Example of a supervisory authority addressing the prioritization of supervisory activities

The supervisory authority decides that its key priorities are:

- requiring supervised firms to maintain prudential soundness;
- requiring supervised firms to correct serious breaches of prudential or conduct of business requirements;
- market monitoring for market abuse and manipulation;
- anti-money laundering monitoring; and
- crisis preparedness and crisis management.

The supervisory authority decides that other supervisory activities could if necessary (depending on the severity and nature of an incident) be:

- stopped for a temporary period (for example authorizing new entrants, and developing and implementing some new policies);
- undertaken less frequently (for example risk assessments, thematic reviews, and communications with trade associations);
- phased over longer periods (for example some parts of supervisory action plans following a risk assessment, and enforcement actions against more minor rule breaches); or
- re-purposed to focus on the impact of an incident on supervised firms (for example adjusting thematic visits to focus on the impact on firms of incident-related risks).

VI. Step 2: Identify critical resources and dependencies

The second step is to identify the critical resources – the people, systems, processes, and other resources – necessary to deliver the key supervisory activities identified at step 1. For each key supervisory activity these critical resources are likely to include:

- The number and types of people required (depending on the type of incident, the organization may be facing a shortage of staff, so it may be necessary to re-assign staff to new roles);

[5] See Toronto Centre (2018) and Toronto Centre (2019a).
[6] Toronto Centre (2020) discusses such prioritisation issues in the context of the Covid-19 outbreak.

- Access to data and information (including physical and electronic files, reports, regulatory reporting, etc);
- Decision-making processes (it may not be possible to maintain pre-incident decision-making procedures, so decision-making processes and authorizations may need to be adjusted. To allow necessary decisions to be taken expeditiously, greater involvement of alternates and more junior staff may be appropriate for specified decisions);
- IT hardware and operating systems;
- Premises (including back-up locations and the ability for staff to work from home);
- Communications equipment;
- Other support operations – HR, finance, legal, etc; and
- Third-party (outsourced) suppliers of services, equipment, raw materials (these suppliers may, or may not, be operating normally during the incident – indeed their failure may be the cause of the incident).

A supervisory authority should develop a comprehensive understanding and mapping of the resources that support its key supervisory activities. By looking at all the resources required to provide these activities, an authority will be able to develop a clearer picture of how best to support its business continuity. This includes resources over which the authority may not have direct control, namely outsourcing and third-party service providers.

Example of a supervisory authority identifying critical resources

- All senior staff (department head and above) are required for the BCP team and oversight of usual responsibilities (refocused in some cases).
- All IT staff to maintain electronic communication channels and automated data capture and records management, and to implement additional communication channels as necessary (for example to facilitate video conferencing).
- All supervisory teams responsible for high- or medium-high impact supervised firms and financial market infrastructure to continue close monitoring, with daily updates and daily returns if necessary.
- Conduct of business/AML teams to focus on what are perceived to be the highest risk firms/sectors.
- Authorizations, enforcement and policy staff available to support supervisory teams if necessary.
- Development work on automated data capture system (with outside supplier).

Having considered the critical resources required for each key supervisory activity, it is then necessary to consider the dependencies across the key supervisory activities. For example, are multiple key supervisory activities dependent on the same critical resources? If a critical resource cannot be maintained or restored, or is in short supply, what impact would this have on key supervisory activities?

VII. Step 3: Establish tolerances

The third step is to determine the critical downtime for each key supervisory activity, and the consequential critical downtime for each critical resource. For example, the impact tolerance for some key supervisory activities may be that they should be restored within 24 hours, while for others it may be acceptable to restore them within a few days or a week. Activities may have different levels of priority in terms of the speed of restoration, which is not necessarily the same as their intrinsic importance to the supervisory authority (a supervisory

activity could be very important to the supervisory authority, but it may not need to be restored in hours rather than days).

It is important that these impact tolerances should be agreed at board level and that they are clearly documented, because (a) they will determine the strategy for incident management, including the roles and responsibilities of individuals within the supervisory authority, and (b) they will widen the mindset of the board and senior management beyond traditional risk management towards accepting that disruptions to business activities are inevitable, and need to be managed accordingly.

It is also necessary for a supervisory authority to determine other tolerances, including its tolerance for the risks that might arise from the activation of a BCP. For example, moving to a back-up site, using back-up IT services, and increased working from home may all create higher risks relating to data confidentiality, cyber security, less well-structured decision-making procedures, and lapses in record keeping. These may be inevitable consequences of implementing the BCP that need to be accepted, albeit reluctantly. The supervisory body should however recognize that these risks exist and have some explicit tolerance for them.

Example of a supervisory authority setting impact tolerances

Low tolerance for:

- IT and other communication failures that compromise the ability to communicate with firms and other stakeholders.
- Failure to monitor medium-high and high-impact firms on both prudential and conduct of business/AML basis.
- Failure to follow up serious rule breaches.
- Business misconduct – especially where linked to the impact of the incident (for example where firms give inappropriate advice to clients).

Higher tolerance (but only during the incident) for:

- Failing to meet service standards for the time taken to process an authorization application, to respond to questions from supervised firms, and (where applicable) to deal with complaints from consumers.
- Delays in processing returns from lower-impact firms.
- Minor breaches of rules.
- Delays to supervised firms submitting regulatory returns.
- Temporary suspension of projects, for example the development of an IT system for processing regulatory returns.
- Delays in supervised firms taking action to meet training and competence and governance requirements.

VIII. Step 4: Create the BCP

The fourth step is to create a documented BCP to maintain or recover key supervisory activities (as identified in the first three steps) in response to any disruptive incident.

A BCP should be clear, concise, and easy to use. It needs to be the “go-to” document, not a massively lengthy tome that gathers dust on a shelf (or hard drive) somewhere. It should

specify – using a consistent and standardized format – the possible responses to disruptions, but should not aim to cover all the detail about how these should be carried out. This is because the detail should be covered elsewhere (for example, the IT department should know how to switch to a back-up server or to alternative software, and the premises department should know how to activate back-up premises). A BCP has to have a broad scope to cover all types of incident and response, and a BCP has to allow flexibility in determining the response to a specific incident.

In practice, for any incident it is unlikely that all the possible responses will need to be activated, only those that are necessary to maintain or recover the key supervisory activities affected by the incident.

Key elements of a BCP include:

Governance and ownership – as discussed above under "Constructing a BCP".

Version control – when was the BCP last updated, and when was it last approved by the BCP committee and by the board.

Key supervisory activities and critical resources – the BCP should describe, at a high level, the identified key supervisory activities (see step 1 above) and the critical resources needed to deliver them (step 2).

The identified critical resources should include:

- People.
- IT hardware and software (the full details of how these can be provided should be covered in an IT-specific disaster recovery plan).
- Communications equipment.
- Files and other sources of information.
- Back-up site(s), their capacity, the logistics of relocating staff and equipment, and the equipment and other supplies needed to operate effectively (desks, IT, laptops or PCs, access to stored data and regulatory reports, telecommunications and access to internet, office supplies, catering).
- Decision-making procedures.
- Documentation and record keeping.
- Capacity for working from home, including the availability and usability of equipment (bandwidth, laptops, ability to conference call), issues of data management and security, issues of health and safety, and time period issues (for some staff/functions, home working may be tenable for 1 month but not 3 months).
- Outsourced services. Supervisory authorities are increasing their dependency on outsourced and third-party service providers. The BCP should therefore cover the provision of outsourced critical functions, including how these critical functions can be maintained, restored, or replaced in a major incident. There are a lot of regulatory standards and guidance on outsourcing that could usefully be applied to supervisory authorities as well.

Plan activation procedures – the response to an incident should be managed and driven by appropriate individuals. A BCP senior-level committee should be established (in advance) with powers and procedures to activate the BCP and to take decisions under the BCP in order to initiate the necessary responses to an incident. This committee should include the chief executive, chief operating officer, heads of IT, premises and HR, and a senior supervisor.

The BCP may need to be invoked in a range of unusual and pressing circumstances. It may not be possible for the BCP committee to meet in full (be it in person, by telephone or by email) to activate the BCP and to initiate responses. Procedures should therefore allow for deputies/alternates for members of the committee, and for a sub-group of the committee or even some individual members of the committee to activate the BCP if the full committee cannot meet at short notice.

Communications – clear and effective communication channels are necessary to both the staff of the supervisory authority and external stakeholders. Planning, testing, and exercising communication procedures is essential to ensure the continuity of key supervisory activities.

Five elements of BCP communication

Effective communication (both when the BCP is activated and at various times during the incident) depends on the following five elements that should be covered in the BCP.

First, all the staff of the supervisory authority need to be aware of the existence of the BCP and aware of what they might be asked to do under the various response options. For some staff this may involve specified roles and responsibilities within elements of the BCP, while for other staff the starting point may be to carry on as before until instructed to do otherwise. For example, if the BCP committee decides that the supervisory authority should move to a back-up site, some staff will have very specific roles and responsibilities to ensure that the site is properly set up. But it would not be effective (and may not be physically possible) for all staff to turn up at the back-up site on day one. So for many staff, the first message to them is likely to be that they should stay at home until instructed otherwise.

Second, because all staff may need to be contacted at short notice, the BCP needs to include clear procedures and mechanisms for communicating to the staff of the supervisory authority. Most organizations rely on a call cascade for this, where the BCP committee communicates to the head of each department, and the message is then passed down to the staff of each department through previously established procedures (for example the department head contacts the managers, who in turn contact their teams).

This requires each messenger in the chain to have access to the work, mobile, and home telephone numbers (use might also be made of emails and other forms of communication) of each person they are responsible for contacting. This will also require a system for keeping all these contacts up to date as both staff and their contact details change. And it requires anyone responsible for contacting others to have at least one nominated deputy or alternate to lessen the risk of one part of the communication chain failing.[7]

Third, the BCP itself does need to include contact details for key staff, such as the members of the BCP committee and their deputies/alternates, and staff with responsibilities for the provision of critical resources such as IT, premises, and outsourced services. And for at least some of these staff, consideration should be given to alternative forms of communication (for example satellite phones) in case mobile phone networks and the internet are compromised by the incident.

Fourth, there is likely to be a need to communicate with external stakeholders, either because they are critical to the operation of the BCP (key external suppliers of critical resources) or to inform external stakeholders of how the activation of the BCP might affect

[7] It is not necessary for the BCP itself to list every contact number. But they should be available to HR and to management chains. In some organizations in some countries, this has been a problem because some staff have objected to their home and personal mobile numbers being held by their employer.

them (including government departments, the central bank, other national supervisory authorities, relevant authorities in other countries, supervised firms, the media, and the general public). The BCP should make clear who has responsibility for contacting each external stakeholder, and this responsibility should include knowing the contact details for external stakeholders if they have also had to activate their own BCPs and have moved to their own back-up sites.

The BCP should contain the contact details of key external suppliers (and who should be in contact with them once the BCP is activated) and some other external stakeholders (in particular public authorities). But in some cases the BCP should assign responsibility for maintaining contacts to specific members of staff or their departments (so, for example, supervisors should be expected to hold contact details for all supervised firms; and the press office should be expected to know how to issue press releases and social media statements and to contact the media). Again, this should include the possibility that external stakeholders are themselves affected by the incident and may not be operating normally.

Fifth, the BCP should include sample pre-drafted and pre-approved communications to cover a range of eventualities, including how to inform staff that the BCP has been activated and what they need to do as a result; messages to other public bodies; messages to supervised firms; and press statements. It is quicker to adjust an existing draft to the specific circumstances of the incident than to start from scratch.

Path of return to normality – the BCP should include procedures under which the BCP committee can determine that the incident that triggered activation of the BCP is over, and that the supervisory authority can return to normal.

IX. Step 5: Test the BCP

The next step is to test the BCP. Testing a plan is the only way to know it will work.

This can take various forms, including desk-top (paper-based) exercises to consider how the BCP might operate in various scenarios; walk-through exercises in which departments and individuals walk-through their roles in one or more scenarios; call cascade exercises to check whether messages can be communicated quickly and effectively to large numbers of staff; and full activation of at least some elements of the BCP, such as moving operations to a back-up location, holding a “working from home” day, or activating back-up IT infrastructure and systems.

Each of these types of testing should be undertaken regularly and should be based on a range of incidents that vary in nature, severity, and duration, including some that are deliberately at the severe and challenging end of the spectrum.

Some tests might be pre-announced, but others should be unexpected to most staff – for example, a pre-announced move to a back-up location might be the best way to test how well a supervisory authority can work from its back-up site, while a surprise move would be the best way to test initial communication and the ability of relevant staff to find their way to the back-up location.

There will also inevitably be real tests of a BCP when serious incidents occur.

X. Step 6: Learn lessons and amend the BCP

A supervisory authority should strive to learn lessons from real-life incidents (in particular when its BCP was triggered), from testing, and from periodic reviews of its BCP; and should then amend and redistribute the BCP accordingly.

There is a risk that even if a BCP is written, and even if it is tested occasionally, the plan will become outdated as key supervisory activities and critical processes change and evolve. People, systems and processes come and go, so the BCP needs to be updated. It should therefore be reviewed annually. Any weaknesses should be corrected, and an updated plan distributed to all pertinent staff.

Regular testing, learning lessons and amending the BCP accordingly should also keep the plan fresh and provide a cultural context in which the importance of the BCP is emphasized. This can be reinforced by actively soliciting input and feedback from staff, and from asking departments to review aspects of the plan that are relevant to them.

.

XI. References

Joint Forum. *High-level principles for business continuity*. August 2006. https://www.bis.org/publ/joint17.pdf

Toronto Centre. *Risk-Based Supervision*. March 2018. https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision%20FINAL.pdf

Toronto Centre. *The Development and Use of Risk Based Assessment Frameworks*. January 2019. https://res.torontocentre.org/guidedocs/Development%20and%20Use%20of%20RBS%20Assessment%20Framework%20FINAL.pdf

Toronto Centre*. Crisis Binder: An Essential Tool for Crisis Preparedness.* October 2019. https://res.torontocentre.org/guidedocs/Crisis%20Binder.pdf

Toronto Centre. *Ten Issues for Supervisors During Crises*. April 2020. https://www.torontocentre.org/Files/NewsResources/4-8-2020/Ten%20Issues%20FINAL.pdf