noggin | Business Continuity

Key Learnings from the Victoria Government's Business Continuity Audit

The Victoria State Government conducts a whole-of-government audit

Business continuity management consists of creating and executing frameworks, plans, and actions to ensure that entities can deliver prioritised services during a disruption. The practice takes on especial importance for government entities, tasked as they are with delivering services critical to residents' economic, financial, and social wellbeing.

That's the case with the Victoria State Government, responsible as it is for managing state finances, child protection, transport, criminal justice, and other vital services. And so, the state, having gone through one of the world's longest, continuous lockdowns, was particularly keen to understand how its business continuity capabilities fared during the COVID crisis.

As a result, an audit was commissioned. The Audit examined the business continuity capabilities of all eight Victoria State Government departments, as well as the ICT platform that provides service management to most departments.

What else was looked at? Considered in the Audit were each department's business continuity arrangements. The aim, here, was to ascertain whether departments had (1) successfully prepared for a major disruption prior to the outset of COVID and (2) effectively implemented contingency arrangements during the pandemic to maintain prioritised services.

Why does it matter?

Well, key conclusions stemming from the Audit, which the subsequent guide lays out, are of great relevance to most organisations – public entities or not. Indeed, many organisations will likely see their own experiences reflected in the Audit. And so, we advocate using the following findings, recommendations, and suggested solutions as templates for business recovery.

A failure to prepare for long-term disruption

The Audit starts with a frank admission that before the pandemic, most State Government departments' business continuity arrangements were inadequate. Responses to restoring and maintaining prioritised services were also reactive – less efficient and effective than they could have been.

The failure to plan and prepare suitably for a long-term disruption to services came even though a major event (specifically, a pandemic) was forecasted as a state-significant risk.

In fact, the State Significant Risk Interdepartmental Committee (Risk IDC) rated the pandemic risk as 'likely' to occur with 'severe' consequences the year before the outbreak of the crisis.

More problematic, pre-COVID tests of existing business continuity planning arrangements found glaring weaknesses. Many of those weaknesses, however, weren't addressed in time.

Specific findings: Lapses in planning and other business continuity processes

Where does the Audit suggest things went wrong? Did no department have mitigation strategies in place?

The Audit finds that many existing mitigation strategies were either inadequate or weren't put into place entirely. For instance, one department had a strategy for managing state-wide disruption.

That strategy, however, focused almost exclusively on emergency response (i.e., protecting life, assets, and the environment) at the price of the continuity of prioritised services.

Nor was there whole-of-government oversight of business continuity across the State Government, as was reflected in the lack of whole-of-government policies for staff deployments.

Further key findings include:

Major gaps in business continuity planning. As noted, departments didn't plan sufficiently for such a large-scale, complex disruption. Business continuity plans focused mostly on localised short-term disruptions of less than two weeks.

There were other reasons that the plans that existed were deemed inadequate. According to best practice, BCPs should be focused, concise, specific, and easy to use. However, the BCPs the Audit reviewed were found:

- Not to have been reviewed or updated on a regular basis
- Not to have activation criteria
- Not to have adequate recovery strategies
- Not to provide full detail about their scope, purpose, objectives, or dependencies.

What's more, BCPs were oftentimes duplicative, including unnecessary information, which reduced confidence from staffers.

Staffers themselves were competent. Their departmental plans, however, were considered difficult to understand and maintain.

Major gaps in business impact analysis. Did business continuity arrangements adhere to international standards in any respect? Indeed, they did. Oftentimes, they adhered to best-practice standard, ISO 22301.

But as the Audit notes, preparedness involves more than just adherence to policy – important as that is. Entities must also understand the services they provide, the impact a disruption would have on those services, and how they should respond.

This is the provenance of the business impact analysis. Here, however, the Audit found that many departmental BIAs did not fully assess the impact that a disruption might have on their services.

BIAs also did not fully consider minimum resource requirements and the internal and external suppliers that their services need to run, all gaps which can impact how effectively departments respond and maintain prioritised services during a disruption.

Why's that? The Audit found that departments hadn't undertaken sufficient work to collate services and assets relative to organisational priorities.

Gaps in the COVID response. What of the COVID response itself? Here, staffers garner plaudits. They responded quickly and flexibly. Incident response processes, structures, and strategies, in particular, helped departments quickly set up teams, make decisions, and communicate to staff.

But it needn't have come to that. Since departments weren't sufficiently prepared for such a complex disruption, they had to invest scarce time and resources on the fly into developing documents, streamlining processes, upgrading technology, and transitioning to remote working during the early stages of the pandemic.

Poor inter-agency communication during the pandemic was also called out. Written guidance was lacking on how departments should:

- Communicate or escalate whole-of-government issues
- Access or share resources to deal with surge resourcing issues
- Prioritise services at a whole-of-government level.

Further issues included:

- Lack of a clear understanding of which services needed to be prioritised and how to do it
- Risk of service delivery being affected due to insufficient staff or ICT access
- Lack of clear processes to implement social distancing measures
- Increased risk of poor communication across and within departments
- Need to invest time and resources into developing communication plans as well as towards their response

Gaps in workforce capacity and remote working arrangements. Another repercussion of inadequate pandemic planning was the lack of strategy to prepare departments for remote working and surge capacity.

For one, there was no whole-of-government policy for staff redeployment for continuity of government services. This meant that departments responded reactively to COVID, devoting scant resources to developing new remote working processes and addressing surge capacity issues.

In consequence, state entities saw sharp increases in privacy concerns, cybersecurity as well as occupational health and safety risk.

And though departments have advised staff about the importance of privacy and occupational health and safety, the Audit notes that more still needs to be done to better manage risk as new challenges arise, e.g., work-life balance and/or security.

Gaps in reporting. The Audit also found a generalised data problem, stemming from gaps in reporting. The genesis of this reporting problem was that departmental processes favoured qualitative reporting and specific services.

Nor did departments systematically report against their business continuity RTOs or MTPDs. As a result, departments are now unable to determine how effective their arrangements were in maintaining prioritised services.

Recommendations going forward: Business continuity planning and more

What then does the Audit recommend for the recovery period, to ensure enhanced contingency processes for the next long-term disruption? For starters, departments ought to better prepare for foreseeable major disruptions of longer durations, i.e., longer than a couple of weeks.

To do so, they will have to make the following changes to their business continuity arrangements.

Organisations will firstly have to address the pandemic scenario as a standalone threat, with a dedicated pandemic scenario plan. Some departments did but many did not.

In addition, organisations will have to treat their business continuity plans as living documents, testing them more regularly (at least every two years) to ensure they will be effective in a disruption and that staff knows how to respond. The plans themselves should more clearly highlight organisation-wide priorities and strategies, as well.

Further Audit recommendations for business continuity planning include:

- Align plans with international standard, ISO 22301
- Identify clear plan activation criteria
- Make plans better reflect the current operating environment
- Better cover prioritised services
- Address the need for additional or surge resources where relevant
- Include strategies for addressing long-term disruptions (either within the specific plan or in another linked document)

Similarly, BIAs ought to be undertaken at least every two years – more often when there are significant changes to the organisation.

New BIAs should be reviewed along with the business continuity management exercising program. This program will serve to validate business continuity strategies across the whole organisation, ensuring strategies are in alignment with the risk profile.

Mandatory training for staff who have dedicated business continuity responsibilities should also be provided, both when they start in the role and at least every two years. Such training should include (1) roles and responsibilities, (2) required response actions, and (3) reporting obligations.

The importance of digital transformation in upleveling business continuity arrangements

Although there's much to do, the Audit notes that the pandemic itself has created opportunities for departments to make positive change. One such change is the much-needed acceleration of digital transformation to adopt more efficient processes.

After all, the pandemic has already made entities rethink how they work, leading oftentimes to the quick roll out of new technology-related processes and projects.

Here, the Auditors make especial note of the value of streamlining processes and adopting new (digital) technology, to ensure efficiency in performing business continuity tasks.

Though not singled out directly, pragmatic business continuity software can help organisations of all stripes make the most of the COVID recovery and get better prepared for next time. How exactly can digital technology provide solutions to audit findings and recommendations?

Uses include:

- **Audit finding.** BIAs did not fully assess the impact that a disruption might have on departmental services; and plans were largely focused on localised short-term disruptions of less than two weeks.
- **Digital solution.** With pragmatic business continuity software, organisations can easily create an impact assessment for multiple types of impacts for each prioritised activity within a BIA, including the impact of disruptions over multiple time periods, not just shorter-term disruptions.
- **Audit finding.** Departments failed to consider all minimum resources requirements and the internal and external suppliers that their services need to run.
- **Digital solution.** With pragmatic business continuity software, organisations can highlight if a prioritised activity has key staff dependencies, as well as the BAU head count required, the number of staff required for the minimum business continuity objective, whether the staff dependency is a single point of failure, in addition to recording staff members who are essential to complete the activity.

  Further, with pragmatic business continuity software, organisations can create and manage lists of dependencies, including internal and external suppliers. It's also easy to add these to prioritised activities, as well as recording if there are any dependencies on other prioritised activities.
- **Audit finding.** Not all BCPs aligned with the ISO standard. Nor did all include prioritised activities.
- **Digital solution.** Pragmatic business continuity software applies industry standards drawn from the latest versions of ISO 22301, ISO 2231, and ISO 22317.
- **Audit finding.** Departments were found to have inadequate recovery strategies.
- **Digital solution.** With pragmatic business continuity software, each recovery strategy gets an efficacy rating and testing status. Recovery strategies also follow an automated approval process, so organisations can ensure that their recovery strategies are reviewed, approved, and always tested.

  In addition, by collecting and aggregating data, pragmatic business continuity software highlights any critical activities, processes, assets, and resources lacking recovery strategies, or untested recovery strategies that put your business at risk.
- **Audit finding.** Departments failed to exercise their BCPs to ensure they would be effective in a disruption. When they did, departments often limited exercises to small-scale or desktop exercises, i.e., testing SMS functionality or testing the impact of a disruption on one or two business units.
- **Digital solution.** With pragmatic business continuity software, organisations can conduct simultaneous exercises across multiple business units to practice and battle-test teams, response plans, and communications. The software also makes it easier to record after-action reviews, lessons learned, and improvement activities for evaluation.
- **Audit finding.** Departments failed to undertake BIAs every two years or more often.
- **Digital solution.** Pragmatic business continuity software automatically reschedules BIAs; organisations, therefore, don't run the risk of forgetting to review.
- **Audit finding.** Organisations ought to review their business continuity management processes to (1) validate business continuity strategies across the whole department and make sure they align with the risk profile (2) test a scenario that affects and involves multiple business units or departments simultaneously.

  Departments also need reporting functionality to ensure executives understand (1) what services have been impacted, (2) If any recovery time objectives have not been met, and (3) whether other services are at risk.
- **Digital solution.** With pragmatic business continuity software, organisations can create a post-incident report for executives in just a few clicks - as well as providing them access to their very own dashboard highlighting key information in an easy to digest format.

  Organisations can also review their post-incident report templates to include a section outlining prioritised services, recovery time objectives, and if services are disrupted, how long.

Finally, the COVID crisis pointed up the inadequacy of business continuity arrangements. Audits, like that undertaken by the Victorian State Government, are crucial for pinpointing which particular arrangements were lacking.

But as important as post-mortems are to business recovery, they aren't the end of the story. Audits provide organisations a list of recommendations. Implementing those recommendations are just as crucial to business recovery.

Here, accelerating digital transformation is considered key to upleveling business preparedness and maintaining business resilience. Within the mix, pragmatic business continuity management software, we note, stands out.

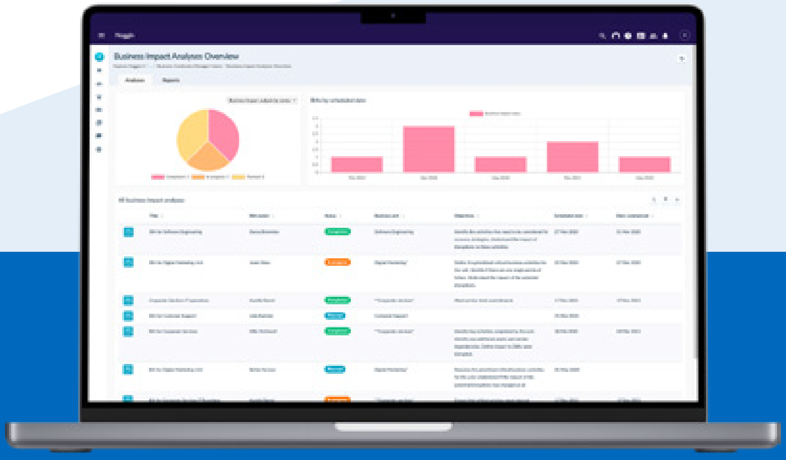
These digital solutions don't just follow best practice, they bring it to life to drive continuous improvement. As a result, organisations who procure them can scale up business continuity arrangements to any incident – no matter how complex or disruptive – and back down to business as usual as quickly as possible.

Like what you read? Follow Noggin on social media

@teamnoggin

facebook.com/teamnoggin

linkedin.com/company/noggin-it



Business Impact Analyses Overview

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**
or contact: **sales@noggin.io**