Case Study: Developing a Tailored Business Continuity Management System

Office of the Commonwealth Ombudsman (the Office)

Audience

This case study is designed to assist Commonwealth officials at the Executive and Specialist levels.

It provides guidance on establishing a Business Continuity Management (BCM) system that supports coordinated responses by integrating business continuity with crisis management, cyber incident response and IT Disaster Recovery (ITDR).

At a glance

The Office commissioned a review of their BCM Framework and Business Continuity Plan (BCP). The Ombudsman and his executive were keen to understand the capability required to manage current and future threats, including operational disruption and cyber incidents.

The Office used the review outcomes to establish a tailored and effective BCM program including a fit-for-purpose crisis management approach to manage business disruptions and align operational and technology response planning.

This case study examines the Office's approach to designing a framework and response plan based on specific entity, operational and regulatory requirements.

It outlines how adopting a tailored approach supports the effective allocation of resources so that staff and managers can often resolve significant incidents under business-as-usual response arrangements without activating their business continuity plan.

Process

A three-stage project plan was developed.

Stage 1 – Current State Assessment

Approach:

A current state assessment of the Office's existing BCM system was developed based on reviewing documents and interviewing senior executives. The current state assessment identified opportunities to establish a refined BCM approach that was better tailored to the Office's operating and regulatory environment and recognised existing entity resilience and business-as-usual response capability.

Findings:

- BCM Framework: The Office's existing framework applied BCM principles but provided only high-level guidance on establishing a BCM program. It provided limited guidance on applying crisis management and business continuity disciplines. The framework lacked guidance on undertaking an organisational risk assessment that would be required to tailor the Framework to the Office's requirements.
- Business Continuity Plan (BCP): The existing BCP provided trigger points for activating and de-activating the BCP as a whole, but lacked guidance on specific crisis management and business continuity triggers and escalation points. The BCP did not support integration and coordination of aligned plans including ITDR. This meant BCM response activities were not easily identified and that some responses were duplicated, leading to ineffective use of resources.

Recommendations:

It was recommended that the Office establish a refined BCM Policy and Framework to provide clear governance including ownership, audit and review requirements to ensure response planning is tailored to entity requirements and integrates fit-for-purpose crisis management, business continuity and ITDR activities.

It was recommended that the BCM planning process be tailored to the Office's requirements using an annual top-down Strategic Business Impact Analysis (SBIA) to identify and prioritise entity level risks and critical activities. It was recommended that the existing BCP be reviewed to establish an Enterprise Response Plan (ERP) that incorporated a tailored crisis management process, recognised the Office's business-as-usual response capabilities and provided Playbooks for key identified threats. Establishment of a response plan hierarchy was recommended to clarify integrations between crisis management, business continuity and ITDR plans and Playbooks.

It was recommended that a refined annual review program be established to record the outcomes of testing, exercises and real incidents faced by the office. This process was recommended to help assess and improve business continuity planning.

Stage 2 – Conduct of a Strategic Business Impact Analysis workshop

Approach:

The SBIA workshop was undertaken with the Office's Senior Leadership Group (SLG) and senior management to provide top-down analysis of entity level risks and to identify critical activities.

The SBIA identified that further operational level BIA workshops were not required due to the Office's size and operational resilience (based on physical and technology-based capacity to transfer resources across geographies).

Outcomes:

The SBIA workshop identified:

- Strategic risks and threats faced by the Office
- A prioritised list of critical activities essential to the Office's business systems.
- Key enablers and dependencies for critical activities
- The maximum allowable outage (MAO) for each critical activity
- That the Office only required a BCP for critical activities with an MAO of seven days or less. The Office assessed it was capable of recovering critical functions with MAO's of greater than seven days using business-as-usual response capacity.

Stage 3 – Response Plan Workshops

Approach:

The Office undertook a series of response plan workshops with SLG and senior management, along with BCP and Playbook workshops with relevant business owners. The response plan workshops were used to design an updated ERP and validate the integration of crisis management and business continuity response processes.

Outcomes:

The Response Plan Workshops identified:

- Clear crisis and BCP criteria and definitions for the Office.
- The structure, membership and role requirements for the crisis response team and business continuity team.
- The importance of including top-down and bottom-up assessment, trigger and escalation processes for ERP crisis response and business continuity activities
- Clear integration points between the proposed ERP and aligned plans including the ITDR and emergency response plans

- The need for detailed business continuity response planning for in-scope critical processes
- The need for playbooks to support management of cyber incident, workplace violence and payroll disruption responses

Stage 4 – ERP design and validation exercise

Approach:

- Insights from the Response Plan workshops and SBIA were incorporated into the design of the ERP, which included an integrated hierarchy of plans and playbooks underpinned by the crisis assessment, trigger and escalation process (**refer, ERP design elements below**).
- The ERP and its constituent plans were socialised with the SLG along with ERP and aligned non-ERP response plan owners.
- An ERP desktop validation exercise was developed based on a scenario relevant to the Office and was delivered to the SLG and relevant plan owners. The exercise was used to:
  - Validate the application of ERP activities and plans;
  - Provide stakeholders experience in their individual roles in working as a team.

Outcomes:

The ERP design process and validation exercise:

- Clarified that the ERP was appropriately tailored to the Office's requirements including crisis escalation, stakeholder communications, BCP activation and Playbook application;
- Demonstrated that ERP role-holders were able to use the plan to identify their role requirements under exercise conditions
- Provided ERP role-holders experience in their individual roles in working as a team.

Practical tips and glossary

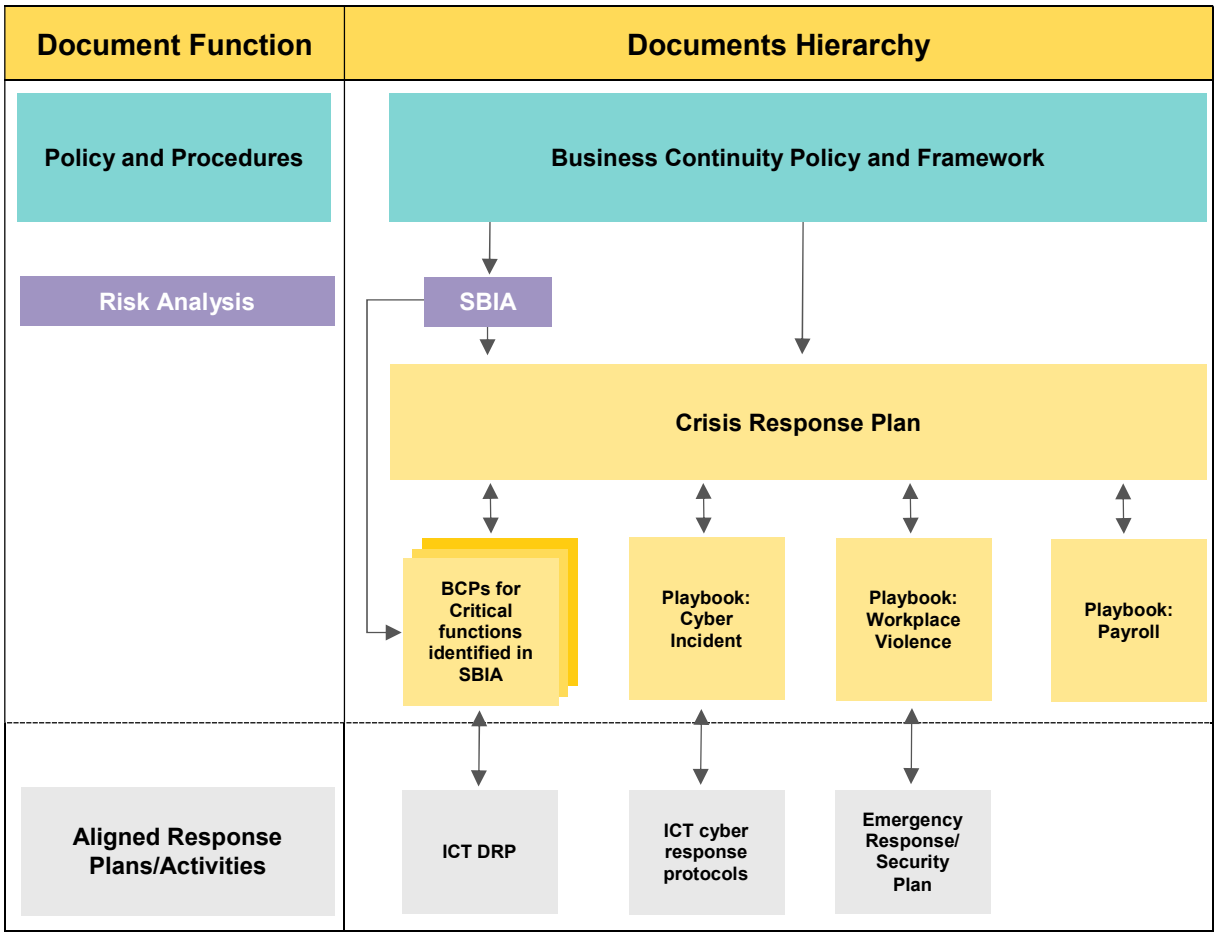
- Remember that every business continuity plan incurs a financial and administrative cost.
- Spend time identifying business-as-usual business continuity response capabilities so your entity can create as many plans as required, but not more than are necessary.
- Business continuity recovery strategies frequently rely on third party technology and an assumption that the ITDR plan will bring services back on-line in a timeframe that matches the BCP. These assumptions need to be tested beginning with ITDR timeframes and supplier service level agreements.
- Separate operational guidance in BCPs from governance in the framework documents.
- Help responders identify their requirements by establishing lean, checklist focused BCPs based on triggers, escalations and disruption responses.

Business Continuity Management (BCM)	The development, implementation and maintenance of policies, plans and other supporting initiatives to assist the entity in managing a business disruption event, as well as build whole-of- entity resilience.
Business Continuity Plan (BCP)	Identifies the responses the entity will use to restore and deliver a critical business function following a disruptive event, as soon as practicable.
Crisis Management	Crisis management is the process by which an entity deals with a disruptive and unexpected event that threatens to harm the entity.
IT Disaster Recovery (ITDR)	The collection of resources and activities to re-establish IT services (including components such as infrastructure, telecommunications, systems, applications and data) following a disruption of IT services. Disaster recovery includes subsequent resumption and restoration of those operations.
Business Impact Assessment (BIA)	The process the entity uses to identify which functions are critical business functions and to determine the maximum acceptable outage period (MAO) for each identified function.
Maximum Acceptable Outage (MAO)	Maximum period of time a critical function can be disrupted before the impact reaches a major or severe consequence on the entity's business outputs.
Critical Activity	A vital activity the entity cannot operate without to meet its key business outcomes. If a critical business function is interrupted the entity may not achieve its objectives or deliver its services, may suffer a financial loss or reputational damage, breach a legal or regulatory requirement or fail to meet stakeholder expectations.

Disruptive Event	An incident or crisis that exceeds the entity's business-as-usual incident response arrangements impacting, or likely to impact the entity's critical functions. Any event which causes a significant disruption in the delivery of one or more of the Office's critical functions; e.g. no building/infrastructure, no ICT, significant staff unavailability or any combination thereof.
Business-as-usual	The normal conduct of business regardless of current circumstances, especially difficult events which pose a potential negative consequence. The phrase can also mean maintaining the status quo.
All Hazards approach	A recognition that most emergencies and crises cause similar problems and that many of the measures required to deal with post-emergencies are generic.

ERP design elements

Hierarchy of plans example



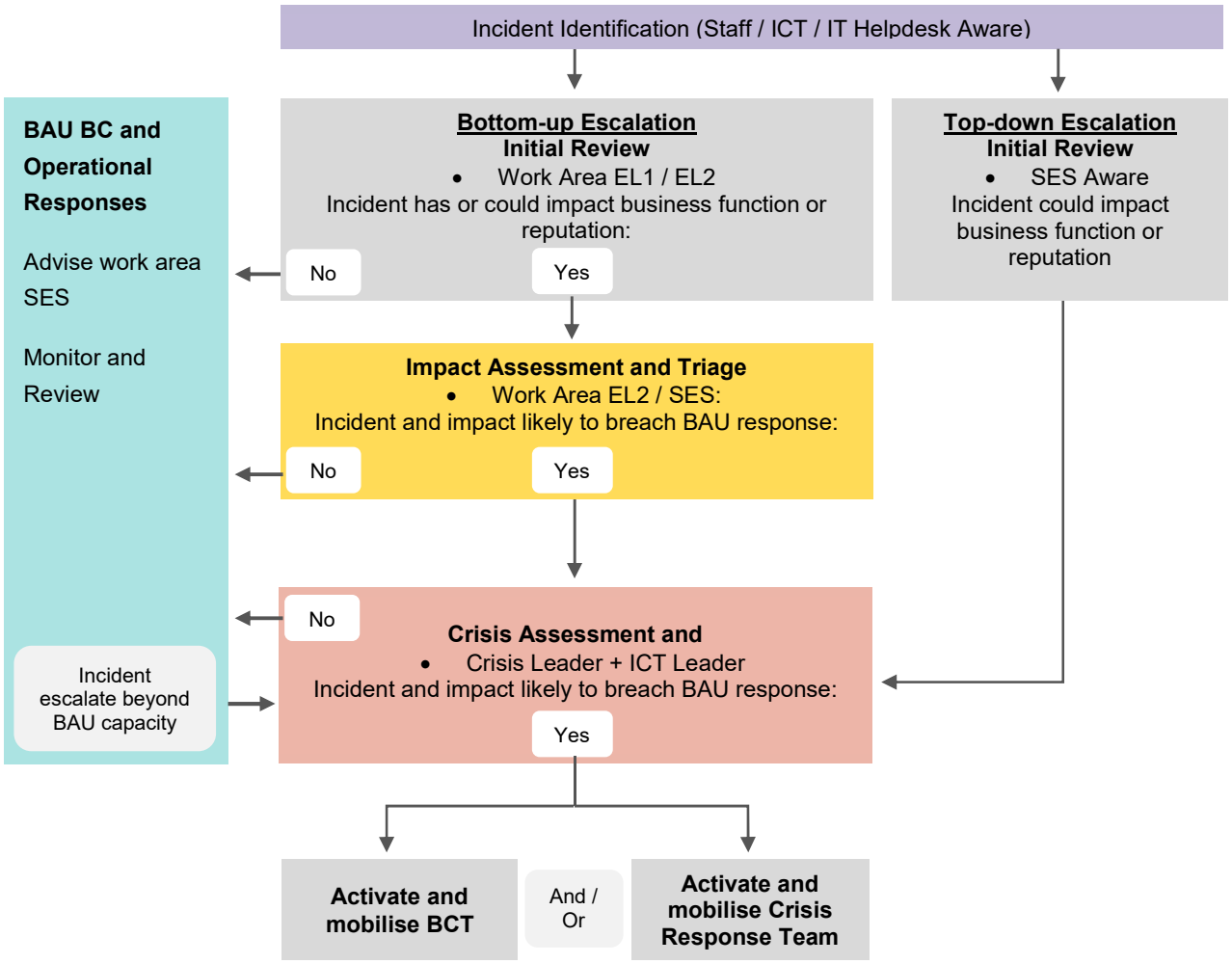
Crisis assessment example

Triggers: Has the situation caused, or does it have the potential
Disruption of a defined critical function (BCP activation)
Significant technology disruption / cyberattack / sensitive data breach
Local or national denial of access to facilities
An imminent threat of serious litigation, negligence or criminal charges
Allegations of potential or actual unethical conduct
Threats related to potential or actual regulatory breach
Adverse media, political or public interest that may damage organisational reputation, and / or result in significant loss of confidence by the public / agencies / Parliament
An imminent threat to, or actual, loss of life, serious injuries or emotional harm to staff

Crisis vs business-as-usual event management considerations example

Business as usual	Crisis Management
The incident can be managed and resolved at the Business Unit level using existing delegations and authorities	Assessment by the crisis management leader/ Executive that a crisis trigger has been breached
The incident can be managed alongside other existing priorities	Resolution of the incident requires entity resources across multiple Business Units and/or offices that must be prioritised over business-as-usual activity
The incident is assessed as unlikely to escalate in severity	Incident resolution requires RT leadership, Response Plan activation and/or management of uncontained risks

Escalation process example



Related resources

Names and links to related BCM information resources

- Commonwealth Risk Management Maturity Model
- Department of Parliamentary Services: BCM Case Study

Contact

If you have any questions or feedback in relation to this information sheet, please contact Comcover Member Services at comcover@comcover.com.au.

Use of this information sheet

Comcover's series of Risk Management Case Studies are learning resources and are not mandatory.

It is important that entities develop risk management frameworks and systems that are tailored to the needs of their entity. Entities may choose to adopt some or all of the concepts contained in this information sheet to suit their specific needs or use alternative methodologies.