Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

Business Continuity in a Box

Overview Document

Content Complexity
ADVANCED ●●●

cyber.gov.au

Table of contents

Disclaimer

The information herein is being provided “as is” for information purposes only. The authors do not endorse or favour any commercial entity, product, company, or service, including any entities, products, or services linked or otherwise referenced within this document.

Overview

Business Continuity in a Box – developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), with contributions from the United States Cybersecurity and Infrastructure Security Agency (CISA) – assists organisations to swiftly and securely stand up critical business functions during or following a cyber incident. By using Business Continuity in a Box, organisations can maintain or re-establish the basic functions needed to operate a business while responding to the issues affecting their existing systems.

Business Continuity in a Box is an interim solution to be deployed by either the organisation or its Managed Service Provider (MSP). These guidance materials provide step-by-step instructions on how to determine and then set up the required interim solution.

Business Continuity in a Box consists of two components:

- **Continuity of Communications** – focuses on keeping communications flowing during a cyber incident by assisting organisations to establish basic communications functionality.
- **Continuity of Applications** – focuses on establishing interim business-critical applications during a cyber incident by assisting organisations to deploy an interim cloud solution for hosting core applications.

Importantly, individual organisations will need to independently assess whether Business Continuity in a Box is the right tool for their unique circumstances, considering their needs and capacity to implement.

Why use Business Continuity in a Box?

Business Continuity in a Box is designed for situations where the availability or integrity of an organisation's data and/or systems has been compromised.

When organisations experience a cyber incident, they often do not have the capacity or resources to continue to undertake minimal business operations securely while incident investigation and remediation takes place.

Whilst a Business Continuity Plan (BCP) remains the most effective way for organisations to achieve business continuity, BCPs are not always developed, updated or regularly tested.

To assist organisations who do not have access to a relevant or recent BCP, Business Continuity in a Box provides an immediate, interim solution for establishing business-critical functions in a timely and secure manner. Business Continuity in a Box focuses on:

- Email Communications (Continuity of Communications)
- Business-Critical Applications (Continuity of Applications)

For organisations looking to better prepare for a potential cyber incident, Business Continuity in a Box can be integrated into an existing BCP. However, due to its targeted focus on email communications and critical applications, Business Continuity in a Box cannot replace a BCP in its entirety. We strongly encourage organisations to invest in a comprehensive BCP tailored to their unique business needs. For more guidance on how to prepare your organisation for a cyber incident, see the following resources:

- ASD's ACSC Preparing for and Responding to Cyber Security Incidents at cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/preparing-and-responding-cyber-security-incidents
- ASD's ACSC Cyber Incident Response Plan at cyber.gov.au/resources-business-and-government/essential-cyber-security/publications/cyber-incident-response-plan
- CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks - Although tailored to U.S. federal civilian branch agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident response activities and detail each step for incident response.

Is Business Continuity in a Box right for your organisation?

In the event of a cyber incident, Business Continuity in a Box assists small to medium-sized organisations (10-300 people) who require an interim Information and Communication Technology (ICT) solution to deliver minimal services. Larger enterprises and government departments can also use this guidance. However, they may need to apply additional configuration steps. It is recommended that larger organisations consult with an MSP and carry out appropriate independent risk and business impact assessments.

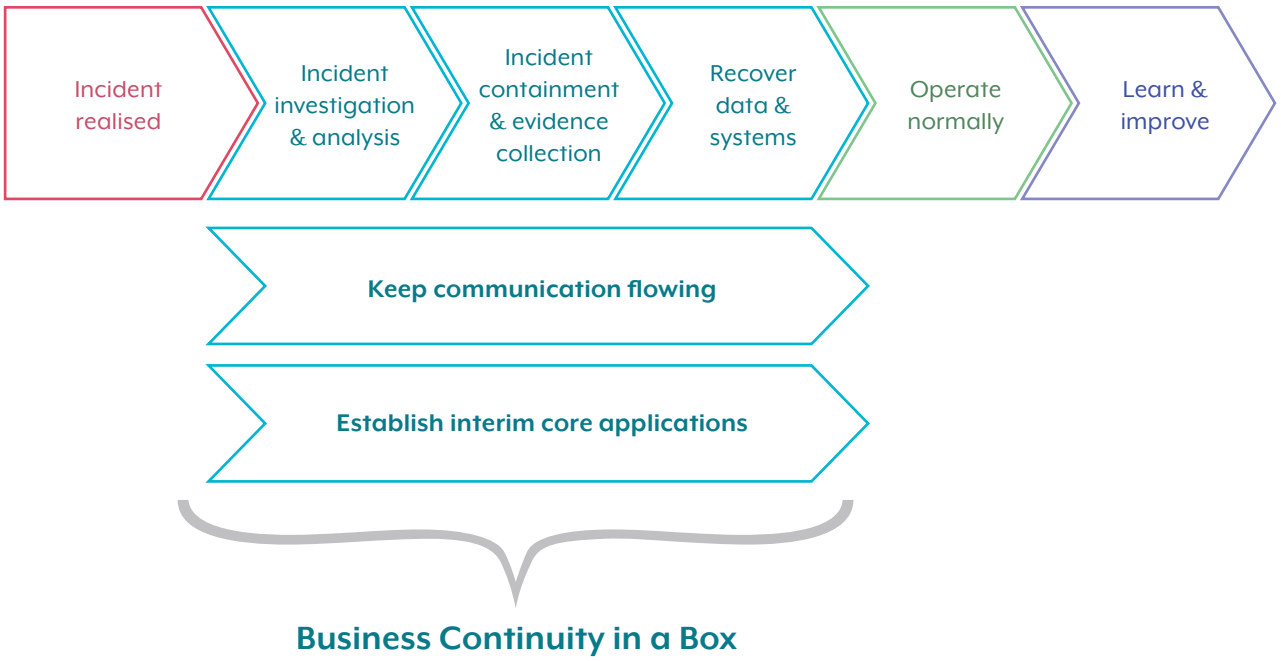
Whilst Business Continuity in a Box has been designed to maximise ease of use, implementation of:

- the Continuity of Communications package requires a basic level of computing knowledge; and
- the Continuity of Applications package requires an intermediate level of knowledge of cloud services.

Business Continuity in a Box includes some technical implementation details (where appropriate). However, due to the unique needs of individual organisations, it is not possible to provide specific technical details for all types of technologies and software that consumers of this guidance may require.

How does Business Continuity in a Box fit into a cyber incident response?

Business Continuity in a Box is designed to complement a broader cyber incident response timeline:



Continuity of Communications

It is critical that organisations have effective means of internal and external communication, especially when responding to a cyber incident. As an interim solution, Business Continuity in a Box provides organisations with the ability to re-establish basic communications functionality quickly and securely. This includes guidance on how to set up a catch-all mailbox so that critical communications sent to the organisation are not lost during the period when usual email systems are unavailable.

The Continuity of Communications package includes the following:

- Written guidance on provisioning a Microsoft 365 Business Standard tenant.
- A tool for automated configuration of a 'catch-all' mailbox in the Microsoft 365 Business Standard tenant .
- Written guidance on configuring security settings for the Microsoft 365 tenant, to ensure a minimum secure baseline.

This package has been developed using Microsoft 365 as the core technology stack due to its prevalent usage across business and government organisations. The package has been designed to accommodate interoperability, functionality, compatibility, and security.

The Continuity of Communications package has been designed based on the Microsoft 365 Business Standard subscription, which offers comprehensive security and management features within the Microsoft 365 ecosystem. The configuration is based on better practice security configuration advice from ASD's ACSC, as well as recent guidance from CISA and the Center for Internet Security (CIS).

> ⓘ **NOTE:** We do not recommend the Continuity of Communications package for existing Microsoft 365 of Google Workspace customers. In the event existing customers are impacted by a cyber incident, we recommend contacting the relevant Microsoft or Google incident response service available to them as part of their subscription. Doing so may provide for a more tailored solution than is offered in the Continuity of Communications guidance.

Further guidance on better practice security configuration is detailed below:

- ASD's ACSC Cloud Computing Security Considerations at cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-considerations
- ASD's ACSC Guidelines for System Hardening at cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening
- CISA Secure Cloud Business Applications (SCuBA) Project at cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
- CISA Microsoft 365 Secure Configuration Baseline Assessment (SCuBAGear) Tool at cisecurity.org/benchmark/microsoft_windows_desktop
- CIS Secure Configuration Guidelines at cisecurity.org/benchmark/microsoft_windows_desktop
- CIS Microsoft 365 Benchmark at cisecurity.org/benchmark/microsoft_365
- Microsoft Entra Verified ID – Manage Emergency Access Accounts at learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access

Continuity of Applications

Communications flow, while important, is not the only functionality that an organisation needs in order to continue basic operations. Other critical functionalities may include office productivity suites, accounting, human resource management and payroll systems.

The Continuity of Applications package includes guidance on:

- Determining critical functions and requirements to ensure continued business operations.
- Determining an appropriate platform for each required interim application.
- Deploying a secure cloud-hosted Infrastructure-as-a-Service (IaaS) solution for each major cloud hosting provider, enabling organisations to take advantage of existing software licenses as well as organisational knowledge and skills.

Contact

For any enquiries concerning this guidance or to provide feedback, please navigate to cyber.gov.au/about-us/about-asd-acsc/contact-us. Select 'General enquiry or feedback', and choose 'Business Continuity in a Box' from the drop-down menu under 'Your enquiry/feedback type'.

If you or your organisation are victim of a data breach or cyber incident, follow relevant cyber incident response and communication plans, as appropriate.

- **Australian organisations** impacted by, or requiring assistance relating to, a cyber incident can contact ASD's ACSC via 1300 CYBER1 (1300 292 371), or by using ReportCyber at cyber.gov.au/report-and-recover/report.
- **United States organisations** may report cyber incidents to CISA's 24/7 Operations Center at report@cisa.dhs.gov, cisa.gov/report, or (888) 282-0870. When available, please include information regarding the incident: date, time and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organisation; and a designated point of contact.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre