Business Continuity in a Box

Guidance: Continuity of Communications
# Contents

**Introduction** ................................................................. 3

Purpose .................................................................................. 3

Overview ................................................................................. 3

How to use this document .................................................... 4

**Guidance** ........................................................................... 5

Stage 1: Review Pack and Verify Prerequisites ....................... 5

Stage 2: Provision Microsoft 365 Business Standard Tenant ....... 7

Stage 3: Configure Organisation Settings ............................... 14

Stage 4: Run Automated Configuration of Environment .......... 19

Stage 5: Validate Environment .............................................. 22

**Contact** ............................................................................. 23

**Appendix A: acronyms, abbreviations and definitions** ............. 23

---

**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.
Introduction

Purpose

In modern organisations, email is the most common function for internal and external communications. In the case of a systems outage during a cyber incident, email (and other communications) functionality is often lost. To ensure business continuity and coordinate an effective response to the incident, organisations must rapidly re-establish basic internal and external communications.

Continuity of Communications focuses on keeping communications flowing during a cyber incident by assisting organisations to establish basic communications functions quickly and securely. It provides guidance to organisations on how to deploy a Microsoft 365 tenant and Exchange Online configuration when core systems, such as user directory and email, become unusable or unavailable.

NOTE: If you are an existing Microsoft 365 or Google Workspace customer, we do not recommend use of Business Continuity in a Box. In these instances, we suggest contacting the relevant hosting provider for support.

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) – is an interim solution to be deployed by either the organisation or its Managed Service Provider (MSP). Successful implementation of Continuity of Communications entails provisioning and configuring of a Microsoft 365 Business Standard tenant and requires a basic level of computing knowledge.

The implementation steps within this guidance will enable an organisation to provision a trial Microsoft 365 Business Standard tenant which includes Microsoft Entra ID (formerly Azure Active Directory), Exchange Online, and associated security services. The guidance also steps through the establishment of a ‘catch-all’ email inbox, established as a priority to ensure critical communications sent to an organisation can continue to be received while other communications systems are unavailable.

Once the Microsoft 365 tenant has been provisioned, the guidance steps through how to deploy the accompanying automation tool – preconfigured security settings and system configurations via PowerShell scripts.

The tool provides a mechanism to automatically configure the Microsoft 365 tenant so that it is secure and functional. This reduces the workload on system administrators, allowing them to better focus on other recovery efforts for the organisation.

The tool automates the configuration of the Microsoft 365 tenant by:

• Applying settings to the Microsoft 365 tenant to secure the organisation and its users.

• Securely configuring Exchange Online and Microsoft Defender to protect the organisation from malicious and spam emails and attachments.

• Creating a temporary ‘catch-all’ mailbox to ensure all emails sent to the organisation’s email address are captured.
Creating an emergency account which should be used in situations where existing administrators are unable to log into their accounts. The configuration provides a secure foundation for organisations to expand on as needed. This may include enabling additional Microsoft 365 services or provisioning additional cloud capabilities to enable restoration of other business services such as financial management or human resource management (see: Business Continuity in a Box - Guidance: Continuity of Applications).

What is Microsoft 365?

Microsoft 365 is a suite of cloud-based productivity tools and services. It includes several online services and capabilities required for business activities. Access to these services and capabilities is dependent on the licence type. This guidance focuses on the Microsoft 365 Business Standard plan. Microsoft offers a range of other plans depending on an organisation’s requirements, size and type. For a comprehensive comparison of all Microsoft 365 plans see:


The Continuity of Communications package uses the following Microsoft 365 services:

- **Microsoft Entra ID** provides centralised Identity and Access Management capabilities for an organisation to secure systems, identities, and data.
- **Exchange Online** provides an organisation with enterprise email and calendar capabilities. Access to Exchange Online can be via a traditional desktop email client or via Outlook Web Access through the user’s internet browser.
- **Microsoft Defender** is an integrated security solution across the Microsoft 365 suite, which offers protection against phishing emails, malware and other threats across Office 365 applications, Exchange Online, SharePoint Online and managed devices.

The following Microsoft 365 services are out of scope of the Continuity of Communications package:

- **Office Applications** are the online versions of the equivalent desktop applications. These include Word, Excel, PowerPoint and OneNote.
- **SharePoint Online** and **OneDrive for Business** offer document management and collaboration capabilities.
- **Teams** provides a platform for unified communications and collaboration.

How to use this document

This document is divided into five consecutive stages. It is recommended that the reader reviews the document in its entirety before commencing Stage 1.

This document uses the below callout boxes to highlight various information.

- **NOTE:** Information to assist the reader in understanding the document, including justification for a particular decision, key considerations, and other important details.

- **WARNING:** Highlights information that requires careful attention, such as implementation of a change or configuration that may impact users or the organisation’s information technology operations.
Guidance

Stage 1: Review Pack and Verify Prerequisites

This document forms one component of the Continuity of Communications implementation guidance. An additional repository containing the automation tool and associated configuration files is also required to make full use of the guidance. Before continuing with this guidance, review all the content in this document, ensuring to prepare and verify additional prerequisites for each stage.

This document is divided into five consecutive stages. The term ‘operator’ refers to the person responsible for implementation of the Business Continuity in a Box solution within their organisation. The below diagram represents the staged process and the prerequisites for each stage.

Computer

This guidance assumes the operator will use a Microsoft Windows-based personal computer (PC) running Windows 10 or Windows 11 using the Microsoft Edge browser to perform the steps. Instructions within this guidance can be completed using alternative solutions. However, the operator will need to interpret the steps for the specific operating system and browser.

Business Continuity in a Box is designed for use during a cyber incident that has affected access to or trust of an organisation’s systems. The selected PC must therefore be independent from the organisation’s IT environment, including network and Internet connection.

The automation tool within this guidance uses the command-line shell scripting language and configuration management framework called PowerShell. Configuration of the automation tool is done via supplied configuration files which have the ‘.config’ file extension.

Phone

During the setup process, Microsoft will either text or call a verification code to a phone. Voice over internet protocol (VOIP) systems generally do not allow the receiving of the verification phone call. Microsoft recommends not using a VOIP phone number for the verification process.

Email

During the setup process, Microsoft will email an account confirmation to the email address provided during the setup process. To receive the confirmation email, the operator must have access to the email account.
NOTE: Whilst ordinarily it would be preferred to avoid use of a personal email account, the nature of the cyber incident may restrict alternatives. If the operator does not have access to an appropriate email account, the operator could choose to sign up for a new email account using providers such as Microsoft Outlook or Google Mail.

WARNING: Do not use an email address associated with the affected organisation.

Organisation Information

Continuity of Communications will provision and configure Exchange Online to enable an organisation to capture all incoming emails to their existing domain name. To redirect emails to Exchange Online, the operator will require access to the organisation's public Domain Name Service (DNS) hosting provider in order to modify the text (TXT) and mail exchange (MX) records.

NOTE: Given the scenario in which Business Continuity in a Box should be used, we do not recommend creating new domain records. To receive email messages sent to the organisation's existing email addresses, only the relevant domain(s) for those email addresses should be modified to update the TXT and MX records.

WARNING: Incorrectly configuring, adding or removing an organisation's DNS records can result in further impacts to the availability of a system.

Configuration steps for modifying DNS records vary depending on the hosting provider. The organisation will be required to supply the operator with the appropriate credentials to access the hosting platform. If the organisation cannot provide the necessary credentials, they must contact their hosting provider prior to proceeding further. If the hosting provider cannot be located, a DNS lookup using a free service such as www.mxtoolbox.com depicted in the image below may assist.

![DNS Lookup Example](image-url)
Financial Delegation

The Microsoft 365 Business Standard plan is valid as a free trial for 30 days. Registration requires an organisation to provide valid credit card credentials. Microsoft will automatically bill the credit card after the trial period if the organisation does not cancel the subscription beforehand. For full terms and conditions regarding Microsoft billing, please refer to:


Stage 2: Provision Microsoft 365 Business Standard Tenant

Overview

This stage walks through the process for setting up a trial Microsoft 365 Business Standard tenant and redirecting emails to the new tenant.

NOTE:

This stage of the guidance provisions a trial Microsoft 365 Business Standard tenant. The trial provides up to 25 user licences for 30 days. Microsoft allows a one-time extension of the trial period for an additional 30 days within 15 days of the trial expiry date. A paid Microsoft 365 Business Standard plan allows for the provision of up to 300 user licences. If the 25-user license limit offered by the trial plan is insufficient for an organisation's needs, the organisation can, at any time, convert the trial to a paid subscription to gain access to the full user license allowance.

Stage Prerequisites

The operator completing this stage will require:

1. PC with a connection to the Internet
2. Up-to-date web browser
3. Valid email address to use during the registration process (must not be associated with or hosted on the network experiencing disruption)
4. Phone that can receive a phone call or a SMS verification code (non-VOIP)
5. Valid credit card
Process


2. Select 'Try free for one month'.

3. In the next screen, ensure that only one person is selected and click 'Next'.

NOTE: Selecting one user at this stage does not restrict the number of users that an organisation can add to the tenant. The trial allows for an additional 24 users. Selecting one user at this stage will simplify the setup and configuration process until the organisation has configured the remainder of the Microsoft 365 tenant.
4. In the next screen, enter an email address to use for account verification and click ‘Next’.

5. Click ‘Set up account’.
6. Enter the required information and click ‘Next’.

NOTE: The country or region selected on this screen will determine the data centre region for data storage. Set this entry to the appropriate country or region to meet your data storage requirements.

7. Enter a phone number that can receive a phone call or SMS verification code and click ‘Send verification code’.
8. Enter the code received into the text box and click ‘Verify’.

9. Enter a username, domain name and password, and then click ‘Next’. This will create a ‘Global Administrator’ account with the chosen username and password required in later stages of this guidance.

**NOTE:** Username: The username on this screen will be the primary administrator account to gain access to the Microsoft 365 administration portal.

Domain Name: Microsoft requires initial use of ‘.onmicrosoft.com’. After setup, the organisation’s own domain name can replace this.
WARNING:
Ensure to record the username, domain name and password in a secure location (location must not be associated with or hosted on the network experiencing disruption). Until additional users are added to the tenant with appropriate access permissions, loss of the credentials will result in an inability to access the Microsoft 365 environment.

10. Microsoft requires a valid credit card to register a Business Standard subscription, click 'Add Payment method', complete the payment information, and click 'Save'.

NOTE: Microsoft will not bill the credit card within the trial period. However, Microsoft will verify the validity of the card and create a billing account. The billing account is used to manage account settings, invoices, update payment methods and purchases. For more information about billing accounts, see:


At the end of the free trial period, the trial subscription will automatically convert to a paid subscription, defaulting to the same plan selected for the trial period. Charges to the credit card will not be incurred if the trial subscription is cancelled prior to the end of the free trial period. The trial will automatically expire at the end of the 30-day period and the credit card will not be charged.
11. Review the information and click ‘Start trial’.

12. After a short period, the screen will update to show a confirmation that the Microsoft 365 Business Standard subscription process is active. Ensure the information is saved to a location where it can be accessed in the future (location must not be associated with or hosted on the network experiencing disruption), and then click ‘Start using Microsoft 365 Business Standard’.

13. The Microsoft 365 Business Standard trial is now active.
Stage 3: Configure Organisation Settings

Overview

This step configuring the organisation’s existing DNS information to point to the new Microsoft 365 Business Standard tenant, enabling email routing.

Stage Prerequisites

The operator completing this stage will require:

1. PC with a connection to the Internet
2. Up-to-date web browser
3. Access to and ability to edit the organisation’s DNS settings in the provider portal

Process

1. Continuing from Stage 2, the operator will have the opportunity to install Microsoft 365 desktop applications. Installation and operation of the desktop applications are not in scope for this guidance, so click ‘Continue’. 
2. To enable creation of the catch-all mailbox, the organisation's existing DNS records need to be updated to point to the new Microsoft 365 Exchange Online endpoints for the organisation. In the available text box enter the organisation's domain name and click ‘Use this domain’.

3. To verify ownership of the domain, Microsoft requires the addition of a TXT record or an MX record to the DNS settings. This guidance uses the first option, ‘Add a TXT record to the domain’s DNS records’, but the processes for adding an MX record is similar. Click ‘Continue’ after selecting the desired option.

**NOTE:** Microsoft allows for the upload of a text file to the organisation's website. However, this guidance assumes that the website is not available.
4. Microsoft will attempt to identify the DNS hosting provider. If known, they will provide the steps to edit the DNS records or a link to the DNS provider's guidance documentation. To continue with this step, in a separate internet browser window or tab, go to the organisation's DNS hosting provider portal and add the identified TXT record information. After editing the DNS record information on the hosting provider portal, return to the Microsoft 365 page and click 'Verify'.

**WARNING:** It is important not to edit existing records at this stage. The DNS record entry is to be added to existing entries only.

Changes to DNS record information can take some time for Microsoft to find. If Microsoft cannot find the new DNS record after clicking ‘Verify’, keep retrying. Depending on the DNS hosting provider, changes can generally take anywhere from a few minutes to 48 hours.
5. Once Microsoft successfully verifies the domain, the page will automatically update to enable the adding of users and assigning of licenses. By default, the initial account created during Stage 2 will have all relevant licences assigned and will be assigned the role of Global Administrator, see learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles. It is not necessary to create any additional users at this stage of the setup. Click ‘Do this later’.

6. To connect Microsoft 365 to the organisation’s domain, the DNS records require modification in the DNS hosting provider portal. Click the default option ‘Add your own DNS records’. Click ‘Continue’.
7. The next screen provides the DNS record information to implement in the DNS hosting provider portal. Follow the guidance provided on this page and within the organisation DNS hosting provider guidance to add the DNS records. Once complete click ‘Continue’.

**WARNING:** The changes made at this stage will cause all emails sent to the organisation domain to be re-routed to the new Microsoft 365 tenant. Ensure a backup of the DNS information in the hosting provider portal is made to enable the organisation to switch back to the enterprise email solution when possible.

If the organisation can receive emails during the cyber security incident, it is recommended not to proceed with this step until the catch-all mailbox is configured within Exchange Online to minimise the risk of lost email messages during the change.

As with Step 4, changes to DNS record information can take some time for Microsoft to verify. If Microsoft cannot find the new DNS record, keep retrying. Depending on the DNS hosting provider, changes can take anywhere from a few minutes to 48 hours.

8. Once the DNS record information is configured and Microsoft can verify the updates, the setup will finish. The DNS record information is now pointing to the new Microsoft 365 Business Standard tenant.
Stage 4: Run Automated Configuration of Environment

Overview
This stage applies configuration settings to the newly provisioned Microsoft 365 tenant via the automation tool, which comprises a collection of PowerShell scripts that apply a secure baseline.

The automation tool will perform the following actions:

1. Install required Microsoft modules from the PowerShell gallery
2. Create a connection to the Microsoft 365 tenant
3. Apply the specified settings to the Microsoft 365 tenant and associated Exchange Online instance
4. Create a ‘catch-all’ mailbox, associated group, and mail transport rules
5. Create an emergency ‘break glass’ administration account
6. Close the connection to the Microsoft 365 tenant

**WARNING:** The ‘catch-all’ mailbox created by the automation tool is not supported by Microsoft due to its lesser filtering capability and resultant increased risk of spam and undetected phishing attempts.

Access to the catch-all mailbox should therefore be restricted and closely monitored to reduce the likelihood of an unskilled operator accessing a potentially malicious email message.

Where practical, the catch-all mailbox should be provisioned for as short a period as possible. Once all users have been created within the new Microsoft 365 tenant, or business operations are restored, the mailbox should be removed.

To minimise the impact to the Microsoft 365 tenant in the event of accessing a malicious email message held within the catch-all mailbox, a separate user account should be created with minimal access permissions to the remainder of the Microsoft 365 tenant. Ideally, this user should be the only user to access the catch-all mailbox. However, given the limited availability of user licenses within the trial tenant and the cost of an additional user licence, this is something organisations will need to individually determine based on their own risk assessment.

Additionally, the Microsoft 365 Business Standard subscription only allows each user up to 50 GB of mailbox storage per user. Given the nature of the catch-all mailbox, once this size limit is reached, additional mail may be rejected.

Stage Prerequisites
The operator completing this stage will require:

1. PC with a connection to the Internet
2. Up-to-date web browser
4. Username and password of an account with the Global Administrator role

**NOTE:** If continuing from previous stages within this guidance, the account created in Stage 2 of the document has the necessary Global Administrator permissions.
Process

Step 1: Preparation

   a. Press the Windows Key on the keyboard or click the Windows button on the Taskbar.
   b. In the “Search for apps, settings and documents” textbox, type “File Explorer” and click 'Open'.
   c. Navigate to the folder where the automation tool folder was extracted (e.g., Downloads).
2. Extract the contents of the package to a nominated location.


   a. Right click on the file and select 'Properties'.
   b. In the pop-up window that appears locate the ‘Unblock’ checkbox in the bottom right corner and place a tick in the checkbox to select the item.
   c. Click ‘OK’ to return to Windows Explorer.
   d. Right click on the file again and select ‘Extract All...’.
   e. In the pop-up window that appears select the desired location to extract the files.
   f. Click ‘Extract’.

**NOTE:** Access to the Microsoft 365 tenant is dependent on the account that is used to sign in. As such, there is no configuration required for the script to apply the default configuration settings.

More specific configuration of the Microsoft 365 tenant is possible by editing the configuration settings within the associated configuration files. This guidance does not cover customised tenant configuration.
Step 2: Run the Automation Tool

1. The automation tool can be run using either a Windows Normal User or Windows Administrator account.

2. To run the automation tool with the currently logged-in user, open the extracted package in File Explorer.
   a. Press the Windows Key on the keyboard or click the Windows button on the Taskbar.
   b. In the ‘Search for apps, settings, and documents’ textbox, type ‘File Explorer’ and then click ‘Open’.
   c. Navigate to the folder where the automation tool folder was extracted and open the folder.

3. Locate the file BCiaB.bat and double click the file to begin implementation.

4. A window will appear.

5. Early in the implementation, the operator will be presented with a prompt to enter the username and password for a Microsoft 365 Global Administrator account. This is the username and password created within Stage 2 of the setup process. Enter the username and password details of the user created during Stage 2 and click ‘Sign In’.

6. The automation tool will provide feedback to the operator on the process currently running. Do not exit the open applications or shutdown the computer until the tool has finished.

7. Once the automation tool has finished, the user will be presented with a completion screen with a report summarising the process and the changes, which can be used to troubleshoot any unexpected issues.

8. The new Microsoft 365 Business Standard trial tenant is now configured.

**NOTE:** Some settings may take time to be activated by background Microsoft processes. Microsoft advises that configuration can take up to 24 hours for certain features and capabilities.
Stage 5: Validate Environment

Overview
This stage walks through the process of verifying that the previous stages have been implemented correctly. The operator will log into the new Microsoft 365 tenant, send an email from an external email service to the new tenant, and then send an email from the new tenant to an external email address.

Process
2. Click ‘Sign in’, using the username and password of the Global Administrator account created in Stage 2.
3. Microsoft Outlook will open to the user mailbox.
4. Add the catch-all mailbox to the available folders:
   a. Right click ‘Folders’ in the left-hand navigation pane.
   b. Click ‘Add shared folder or mailbox’.
   c. Type the email address of the catch-all mailbox in the dialog box and select ‘Add’. The catch-all mailbox email address will be ‘catch-all@<domain>’ where <domain> is the organisation domain not the initial ‘onmicrosoft.com’ domain.
5. Open a new internet browser tab and navigate to the email account used for account verification in Stage 1 or another email account not associated with the new Microsoft 365 tenant.
6. Send an email to the Global Administrator email address.
7. Send an email to ‘info@<domain>’ where <domain> is the organisation domain not the ‘onmicrosoft.com’ domain.
   
   NOTE: It is recommended you do not setup any email addresses before this stage, as doing so may potentially create a new mailbox within Exchange Online. If the Microsoft 365 tenant already has an ‘info’ mailbox, replace ‘info@<domain>’ with an alternative email address that does not exist to test that all email messages sent to the organisation are captured within the catch-all mailbox.
8. Return to the tab opened in step 1 of this Stage.
9. Verify receipt of the email from step 6 within the Global Administrator mailbox.
10. Verify receipt of the email sent to ‘info@<domain>’ from step 7 by selecting the catch-all mailbox in the available folders.
11. Create a new email within Outlook and send to the email account used in step 5 of this Stage.
12. Return to the email account in step 5 and verify receipt of the email from the Global Administrator.
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.

Appendix A: acronyms, abbreviations and definitions

This document uses the following acronyms and abbreviations:

<table>
<thead>
<tr>
<th>Acronym or Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
</tr>
<tr>
<td>Microsoft Entra ID</td>
<td>Formerly Azure Active Directory</td>
</tr>
<tr>
<td>MX</td>
<td>Mail Exchange DNS record</td>
</tr>
<tr>
<td>Operator</td>
<td>The person responsible for implementation of the Business Continuity in a Box solution for an organisation.</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>TXT</td>
<td>Text DNS record</td>
</tr>
<tr>
<td>VOIP</td>
<td>Voice over Internet Protocol</td>
</tr>
</tbody>
</table>
Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2023

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

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