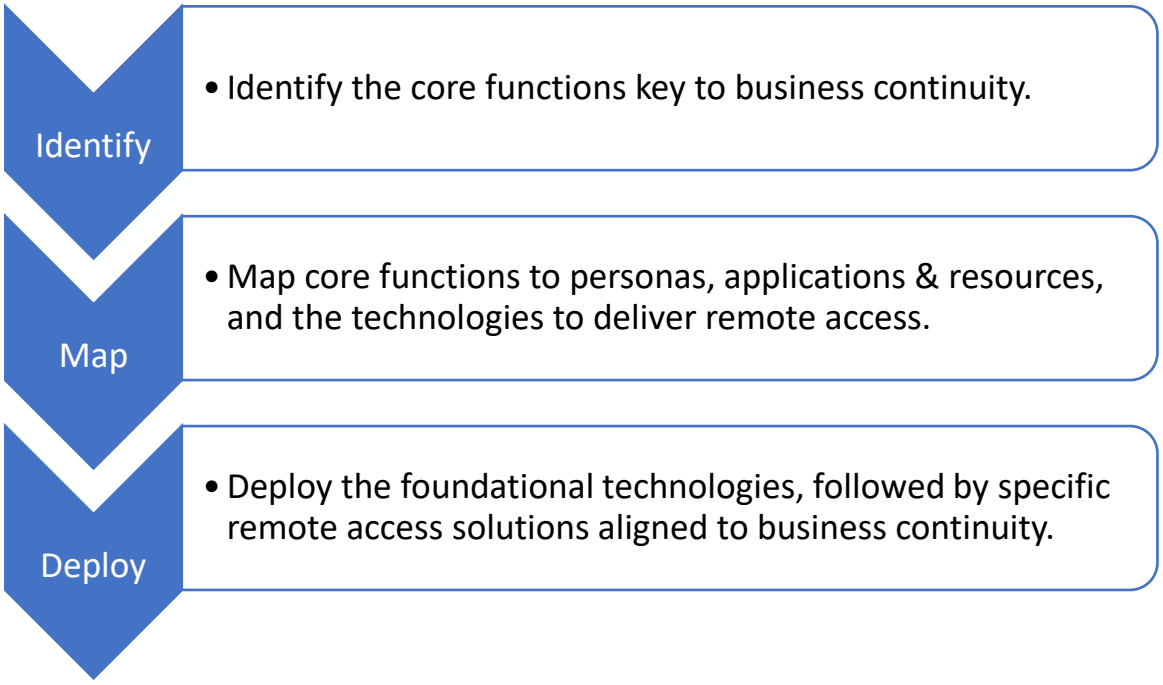
Microsoft

Rapid deployment of remote worker scenarios with Microsoft 365

March 2020

Executive Summary

This paper recommends an approach to identifying core business functions, mapping them through to technologies to deliver remote access, and providing steps to deploy these technologies in the most secure, cost, and time effective manner. Facilitating a rapid response to potentially business continuity impacting events such as natural disasters, public health emergencies, or damage to business facilities.



The advice in this paper is designed to be actionable in-house by enterprise IT departments. However, Microsoft are available to answer questions and connect customers with skilled Microsoft partners to provide on-the-ground assistance as needed.

Sequence of Activities

Context

In times of natural disaster, public health emergency, or physical damage to buildings and facilities an organisation may need to rapidly deploy remote work scenarios to continue to deliver mission critical business functions remotely (typically from home or from temporary facilities).

As of March 2020, many organisations still rely on traditional network perimeter-based security controls that do not permit large scale remote access scenarios. Limiting factors may be a lack of remote access infrastructure, insufficient scale of remote access infrastructure to support remote work at scale, or a lack of authorised IT equipment allocated to staff to perform remote work.

Through Microsoft 365 Enterprise licensing, many organisations have access to a number of technologies in the Microsoft Cloud that can be rapidly deployed to facilitate remote access to critical business functions allowing remote work without compromising the internal network operations or security posture of the organisation.

Solutions recommended in this paper are built on the Microsoft Cloud platform, assessed under the Australian Government IRAP program as appropriate to host Australian Government classified data at up to and including PROTECTED security classification.

This paper is intended as a recommended practices guide for organisations seeking to quickly establish such capability in the event of impending or likely need for large-scale remote work deployment of staff.

This paper is divided into the following chapters:

- **Chapter 1: Assumptions**
  This chapter outlines all the assumptions that have been made in the development of the configuration guidance contained within the paper.

- **Chapter 2: Business function mapping**
  This chapter describes the initial planning to attribute personas to various business groups to understand which scenarios you will deploy and in what order of prioritisation.

- **Chapter 3: Scenarios**
  Each customer will have a variety of differing application types and remote work scenarios; this chapter walks through some core scenarios. Each of these require the foundations of Chapter 4 to be in place.

- **Chapter 4: Foundations**
  This chapter addresses the common foundational elements required to implement any of the scenarios described in Chapter 3.

- **Chapter 5: References**
  Further detail is provided in this chapter on all technologies referred to in the individual scenarios. Additional links to further reading and information on licensing is also provided here.

Chapter 1: Assumptions

The following assumptions were considered in the development of this paper.

1. **Remote workforce requirement**
   Circumstances are dictating the facilitation of wide-spread remote work scenarios for a large proportion of staff in an environment that does not presently support this mode of operating.

2. **Virtual Private Networking (VPN)**
   If an existing VPN is in place it is assumed that it is not scaled appropriately, or configured and deployed widely enough to facilitate a rapid adoption of remote work by a large proportion of staff.

   This could be due to one or more of the following factors:
   a. VPN infrastructure has not been "right-sized" for large scale concurrent usage.
   b. VPN access has not been provisioned to a large proportion of staff and cannot be provisioned in the timeframes or budgets permitted.
   c. Other network infrastructure or perimeter security constraints will prevent large scale use of the VPN by remote staff, for example bandwidth limitations on networks and infrastructure.
   d. BYO device scenarios have not previously been enabled within the organisation.

3. **Connectivity**
   Given the nature of emergency remote work facilitation and the assumption that a customer's internal network infrastructure is not presently configured and scaled to support at-scale remote work, it is assumed that Internet connectivity will be utilised to facilitate remote work in temporary facilities, over mobile devices, or from home Internet connections.

4. **End User Devices**
   Suitable end user devices will be available and could be any combination of laptop or desktop computer (PC / Mac), phone or tablet (IOS / Android). End user devices may be work issued and managed, or personal and unmanaged. Every organisation will need to balance their remote work needs with device availability and their own security & compliance posture. The technologies presented in this paper will be suitable for all of the above device scenarios.

5. **Microsoft 365 Enterprise Licensing**
   The technology solutions presented in this paper require that Microsoft 365 Enterprise licenses be activated for remote workers. A minimum of Microsoft 365 Enterprise E3 is assumed. Further license guidance is provided in Chapter 5.

Chapter 2: Business function mapping

Before any customer starts deploying technology an alignment between that technology and their specific business continuity requirements must be established. This paper does not intend to provide an holistic approach to digital transformation, but instead to assist in deploying simple technologies to quickly meet the remote worker scenarios that are critical to short term business continuity.

Step 1 — Identify critical business functions

- Establish a list of the critical business functions that must be accessible to remote workers for the duration of the business continuity impacting event.

Step 2 — Develop staff profiles aligned to critical business functions

- Describe the critical business functions in terms of a collection of staff profiles.
- Staff profiles will be a useful shorthand for addressing common sets of requirements, which in turn can be mapped to a list of staff members associated to that profile.

Step 3 — Determine core applications and resources by staff profile

- Understanding the core applications and resources each staff profile will need access to will allow mapping to remote access scenarios in the next step and allow for prioritisation of efforts based on criticality of business continuity and impact to the greatest number of staff.
- Being able to quantify the staff volumes will assist in sequencing and capacity planning for various remote access scenarios.

Step 4 — Link applications and resources to remote access scenarios

- Finally, understanding the remote access scenarios from Chapter 4 that will enable the application and resource access requirements, will allow for the generation of a targetted set of activities that must be completed and assist in understanding the impact of each of those activities on business continuity.

Chapter 3: Scenarios

The scenarios below provide for various ways to facilitate business continuity in the face of wide-spread remote work requirements. Each has its own technology prerequisites and licensing requirements. As there are a number of common technology and licensing requirements within the scenarios below, they are described with further information in Chapter 5.

Scenario 1: Remote access to internal web applications

Customers can enable remote access to internal web applications (HTTP/HTTPS) through the deployment of **Azure Application Proxy**, a light-weight service to facilitate remote access.

Azure Application Proxy publishes access to an internal web application via Azure Active Directory, thereby leveraging the Microsoft Cloud as the gatekeeper to the service and Azure Active Directory as the strong access control mechanism. This provides an ability to overlay **Conditional Access** rules and security policy not natively supported by the application via **Microsoft Cloud App Security**. For example, an application that would ordinarily allow files to be downloaded by the user may be restricted to block file downloads for staff connecting from home.

Azure Application Proxy creates an outbound connection to the Microsoft Cloud to facilitate user connectivity. The service is scalable for high availability and load balancing.

Scenario 2: Remote access to rich client applications

Taking internal rich client applications and making them work remotely can be particularly challenging due to the varied ways in which rich client applications can interact with the IT landscape around them. Allowing staff to run sensitive business applications locally on an uncontrolled endpoint, like an unmanaged home computer, is rarely advisable.

Where existing Remote Desktop Services exist on the internal network Azure Application Proxy may be a viable option for providing access.

Alternatively, **Windows Virtual Desktop** delivers a virtual desktop and virtual application hosting platform in Azure that takes advantage of Windows Enterprise licensing to avoid additional license costs. Customers can stand up multi-user virtual desktops or stream single virtualised applications from Microsoft Azure and only pay for the resource consumption that this generates, when the desktops are in use or the application is streaming. Desktops and applications can stream to remote staff through a client desktop app or even a standard web browser. Again, access control is managed by the Azure Active Directory.

Scenario 3: Remote access to internal file shares

There are a number of Microsoft native capabilities for providing remote access to file shares.

1. **Migrate or replicate critical content to SharePoint Online**
   SharePoint Online provides enterprise customers with a large amount of file storage and many advanced information management and collaboration features, such as version history, simultaneous co-authoring, offline synchronisation, and enterprise search.
   By migrating or replicating critical files into SharePoint Online, greater resiliency can be achieved as user access can be offloaded from the internal network and provided by simple internet access. Further, the content becomes resilient to internal network infrastructure disruptions.
   The free SharePoint Migration Tool enables customers to quickly 'lift-and-shift' directories from their file servers and SharePoint Servers into SharePoint Online.
   Consider ***migration*** of content to SharePoint Online to transfer capability there. Any content migrated should then be either sole-sourced from SharePoint Online going forward or migrated back at a later date to avoid duplication.
   For content that only requires read-only access by remote staff a ***replication*** approach may suffice, whereby the data is copied once, or on a schedule, into SharePoint Online but not removed from the source. This provides a separate copy independent of the internal network, thereby removed from internal network availability or capacity constraints.

2. **Azure Files**
   Microsoft Azure Files is a fully managed file share service running on the Microsoft cloud. By migrating file shares to Azure customers can have the same benefits of an internal file share, delivered directly from the Microsoft cloud. This solution provides a like-for-like experience for existing internal file shares, whereas migration to SharePoint Online does alter the user experience. Therefore, the Azure Files experience may be a more familiar option for end users but does forgo the productivity value-adds of SharePoint Online.

3. **Work Folders**
   Microsoft **Work Folders** is a Window Server role that can be activated to enable remote staff to connect in and access their file share content when outside the network without the use of a VPN. If staff have domain joined devices with Windows 10, and the file shares are hosted by Windows Server, this may be a relatively simple option for providing access to the files without moving them.

Scenario 4: Remote access for staff 'home drives'

Giving remote staff access to their day-to-day working files can be a critical component of end-user productivity. Instead of using the Work Folders functionality, there is an opportunity to migrate staff home drives into Office 365.

This scenario is identical to Scenario 2 for SharePoint Online, except that instead of SharePoint Online being the target location for home drive content, **OneDrive for Business** is the destination. OneDrive for Business is a separate special purpose SharePoint Online site for each user, with all the same collaboration features of SharePoint Online, but with substantial storage capacity dedicated to each individual user and distinct from the SharePoint Online storage allocation.

Scenario 5: Communications and collaboration

Critical to success in remote work scenarios is the ability for staff to communicate and collaborate freely. Taking all the natural communication that would happen face to face, in meetings, or over internal chat services and pushing that through email in a remote work scenario could be detrimental to staff productivity.

However, taking the opportunity to introduce a modern collaboration platform such as **Microsoft Teams** not only provides a faster method for communicating, but also allows the facilitation of voice and video conferencing, along with file management and collaboration in one tool. As Microsoft Teams is hosted in Office 365, access doesn't need to enter the internal network and can connect directly over the user's local Internet connection.

Australian Government customers at the State, Territory, or Federal level can also make use of the Department of Finance GovTEAMS platform for inter-agency collaboration in Microsoft Teams. GovTEAMS is a ready-to-go implementation of Microsoft Teams built for government collaboration.

Chapter 4: Foundations

To utilise the capabilities described throughout this paper a number of foundational elements must be in place. This chapter establishes those foundational components and provides a roadmap to begin enabling the scenarios described in Chapter 3.

Identity & Authentication

To enable staff to access the functionality outlined in Chapter 3, an operational **Azure Active Directory** instance must be in place to provide remote user authentication.

Customers with an existing Azure Active Directory / Office 365 tenancy should review the steps in this foundation item to ensure consistency and completeness of the configuration of their existing tenancy. Customers without an existing tenancy should ensure completion of each step.

Step 1: Identify potential identity issues

Before establishing Azure Active Directory identity, a quick scan of your existing Active Directory should be performed to identify any potential issues that may require remediation ahead of time.

Customers should download and run Microsoft IdFix to generate a report on potential issues. All identity issues should be addressed before progressing beyond Step 2.

Step 2: Create Azure Active Directory tenancy

Customers without an existing Azure Active Directory or Office 365 tenancy should activate their Microsoft entitlement to create an Office 365 tenancy and utilise the Azure Active Directory this establishes.

Enterprise customers should request assistance in activating their Microsoft Cloud entitlements by contacting their Microsoft team.

Customers that do not have a Microsoft Cloud entitlement can create a tenancy with trial licensing whilst working to procure an entitlement. In this instance Microsoft recommends creating an Office 365 E5 trial from an “in-private” / “incognito” browser session to avoid interference with any service the user is already logged in to.

Customers should then add an EMS E5 trial whilst logged into the new tenancy. This will ensure that all security and compliance features and controls referenced subsequently in this paper are available. License requirements are detailed for each scenario in this paper to help customers understand what is possible with their existing licensing today and where an uplift may be warranted to meet organisation objectives for supporting remote work in the near future.

Trial licenses last for 30 days, giving customers time to procure and/or provision paid entitlements. Customers that need more time or immediate access to a larger quantity of trial licenses should contact their Microsoft team to request a time and/or user count extension.

Step 3: Deploy Azure AD Connect

Customers should deploy Azure AD Connect to synchronise user identity with Azure Active Directory. Azure AD Connect is a light-weight software install with a simple configuration wizard that can be deployed into an enterprise environment quickly and with little preparation.

Customers should use Express Settings for rapid deployment of the Microsoft recommended configuration.

Express Settings will deploy recommended practice configuration for Azure Active Directory identity. This includes the use of Password Hash Synchronisation for user sign on, globally recognised as a best practice for cloud identity[1]. This is the quickest to deploy and has the least impact on the internal network. Therefore, the recommendation is unchanged in this paper's context of rapid deployment for remote work.

The Azure AD Connect service is deployed into the internal network to periodically synchronise the user objects and credentials into Azure Active Directory. The result is a secure, resilient method for authenticating remote staff and providing them access to applications and resources without complex gateways or federation services.

With Password Hash Synchronisation in place, cloud hosted applications and data (Microsoft and 3rd party) can remain accessible during internal network infrastructure outages.

Step 4: Configure Multi-Factor Authentication for all user accounts.

Customers may choose to deploy more sophisticated Conditional Access policies at this step, time permitting. However, at a minimum (and for minimal effort) customers should enable Azure Multi-Factor Authentication for all staff, including administrator accounts. Though MFA can be configured with little effort, customers should familiarise themselves with the online documentation to inform their configuration choices.

[1] UK NCSC: Securing Office 365 with Better Configuration

Chapter 5: References

Technologies referenced in the Chapter 3 scenarios are listed here with further information, links to online documentation, and any licensing requirements described.

Azure Application Proxy

Azure Application Proxy provides an alternative access method to traditional reverse proxies and VPNs. Instead of opening ports in external firewalls to allow users directly into the corporate network, Azure Application Proxy creates an out-bound connection to the Microsoft Cloud which then plays the role of authentication and access control to the internal application or file storage.

Through this mechanism the follow benefits are achieved:

1. No reliance on VPN infrastructure.
2. User authentication is handled in the Microsoft Cloud, allowing for more sophisticated Conditional Access controls and detection of suspicious activity.
3. Denial of Service mitigations are provided by the Microsoft Cloud.
4. Additional security controls not natively provided by the application can be applied through Microsoft Cloud App Security.

Licensing

Azure Application Proxy is a feature of Azure Active Directory Premium Plan 1, EMS E3, or full Microsoft 365 E3 suite. Australian Government VSA 4 participants own this capability through their Microsoft 365 E3 entitlement.

Further Information

- https://docs.microsoft.com/azure/active-directory/manage-apps/what-is-application-proxy

Azure Files

Azure Files is an alternative to internal file shares that provides a like-for-like user experience, essentially providing for cloud “lift-and-shift” of file shares without breaking applications or user expectations. Windows, macOS, and Linux can directly mount Azure file shares, making it a suitable remote work solution for managed devices.

Licensing

Azure Files is a pay-as-you-go cloud consumption service, it is not covered by any Microsoft subscription licensing. Customers use their storage sizes to calculate the ongoing cost.

Further Information

- https://docs.microsoft.com/azure/storage/files/storage-files-introduction

Conditional Access

Conditional Access policies allow tighter control of user authentication and per-session controls with a rules engine. Outcomes of Conditional Access policies can include:

- Access allowed or denied
- Multi-Factor Authentication required
- Reporting an access attempt to IT security
- Requiring a user password reset
- Session controls that limit functionality for the duration of that session (i.e. blocking file downloads from home or other unmanaged devices).

Licensing

Conditional Access is a feature of Azure Active Directory Premium Plan 1, EMS E3, or full Microsoft 365 E3 suite. Australian Government VSA 4 participants own this capability through their Microsoft 365 E3 entitlement.

Further Risk-Based Conditional Access rule types are available in Azure Active Directory Premium Plan 2, EMS E5, Microsoft 365 E5 Security, or full Microsoft 365 E5 suite. Australian Government VSA 4 participants can add any of these license types through the VSA agreement.

Further Information

- https://docs.microsoft.com/azure/active-directory/conditional-access/overview
- https://docs.microsoft.com/azure/active-directory/active-directory-conditional-access-conditions#sign-in-risk

OneDrive for Business

OneDrive for Business is a Microsoft Cloud service that provides staff with unlimited personal work storage. Delivered from Office 365, OneDrive for Business provides a safe and secure copy of content that can be accessed from anywhere with an internet connection or even synchronised for offline access on appropriate devices.

Licensing

OneDrive for Business is a feature of all Office 365 Enterprise license types, and Microsoft 365 suites. Australian Government VSA 4 participants own this capability through their Microsoft 365 E3 entitlement.

Further Information

- https://docs.microsoft.com/OneDrive/plan-onedrive-enterprise

SharePoint Online

SharePoint Online is a Microsoft Cloud service that helps organisations share, collaborate on, and manage content, knowledge, and applications. Enterprise customers receive over 1 TB[2] of fully backed storage in SharePoint Online to put towards these workloads.

Licensing

SharePoint Online is a feature of all Office 365 Enterprise license types, and Microsoft 365 suites. Australian Government VSA 4 participants own this capability through their Microsoft 365 E3 entitlement.

Further Information

- https://docs.microsoft.com/sharepoint/introduction

Microsoft Cloud App Security

Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy. Microsoft Cloud App Security can wrap enterprise security controls, auditing, and policy enforcement around in-house, Microsoft Cloud, and 3rd party applications.

Licensing

Microsoft Cloud App Security is available as a stand-alone add-on for enterprise customers, or as part of EMS E5, Microsoft 365 E5 Security, Microsoft 365 E5 Compliance, or full Microsoft 365 E5 suite. Australian Government VSA 4 participants can add any of these license types through the VSA agreement.

Further Information

- https://docs.microsoft.com/cloud-app-security/what-is-cloud-app-security

Microsoft Teams

Microsoft Teams is a chat-based workspace to facilitate frictionless collaboration, content sharing, meetings, unified communications, and telephony hosted entirely from the Microsoft Cloud.

Licensing

Microsoft Teams is a feature of all Office 365 Enterprise license types, and Microsoft 365 suites. Australian Government VSA 4 participants own this capability through their Microsoft 365 E3 entitlement.

Further Information

- https://docs.microsoft.com/microsoftteams/teams-overview
- https://docs.microsoft.com/microsoftteams/support-remote-work-with-teams

[2] SharePoint Online storage pool = 1 TB + (10 GB x User Count)

Windows Virtual Desktop

Windows Virtual Desktop is a Microsoft Cloud service that provides for full Windows desktop (Windows 7, 8, or 10) and single application virtualisation. This gives remote staff a full desktop application experience akin to being 'in the office', but from a home computer or mobile device.

Licensing

Windows Virtual Desktop is included in Windows E3 and Microsoft 365 E3. Australian Government VSA 4 participants own this capability through their Microsoft 365 E3 entitlement.
Windows Virtual Desktop does have a pay-as-you-go cloud consumption cost for the storage and compute resources used by the virtual desktop or application, it is not covered by any Microsoft subscription licensing.

Further Information

- https://azure.microsoft.com/services/virtual-desktop/

Work Folders

Work Folders is a Windows Server workload that provides access to internal file shares for remote staff.

Licensing

Work Folders is included in Windows E3 and Microsoft 365 E3. Australian Government VSA 4 participants own this capability through their Microsoft 365 E3 entitlement.

Further Information

- https://docs.microsoft.com/windows-server/storage/work-folders/work-folders-overview

Microsoft Service Trust Portal

The Microsoft Service Trust Portal contains IRAP assessment reports, various global certification reports, and white papers to assist customers in completing their own security assessments and accreditations.

Further Information

- https://aka.ms/stp
- https://servicetrust.microsoft.com/ViewPage/AustraliaV3

Office 365 Security Roadmap

Customers are advised to review and plan to implement the advice contained within the Office 365 Security Roadmap to further harden their Azure Active Directory and Office 365 deployments.

Further Information

- https://docs.microsoft.com/microsoft-365/security/office-365-security/security-roadmap

Office 365 Network Optimisation for Remote Work

Customers should review the advice in the following article to optimise Office 365 traffic for remote users and minimise or eliminate the impact on the internal network.

Further Information

- https://techcommunity.microsoft.com/t5/office-365-blog/how-to-quickly-optimize-office-365-traffic-for-remote-staff-amp/ba-p/1214571

Enterprise business continuity management (EBCM) with cloud services

Customers should update their business continuity plans as they move to cloud services, the resources provided on the following link will help to do this.

Further Information

- https://docs.microsoft.com/en-us/microsoft-365/enterprise/ebcm-understanding-ebcm-with-cloud-services

PROTECTED Office 365 Consumer Guide for Australian Government

Customers seeking to deploy these solutions aligned with Australian Government PROTECTED security classification requirements can obtain a copy of the Consumer Guide for PROTECTED Office 365 through their Microsoft team contacts.

DTA GovDesk for Australian Government

The patterns and practices represented in this paper are aligned with the patterns and practices of the DTA GovDesk program.

Department of Finance GovTEAMS for Australian Government

The Australian Government Department of Finance delivers its GovTEAMS platform to state, territory, and federal government customers as a collaboration platform for government agencies.

Further Information

- https://www.govteams.gov.au/

Appendix 1: Microsoft licensing alignment

The following table provides a quick reference for customers to understand their current and future entitlements aligned to the technologies described within this paper.

Feature	Microsoft 365 E3	Microsoft 365 E5 Compliance	Microsoft 365 E5 Security	Microsoft 365 E5 Suite
Azure Application Proxy	✓	✓	✓	✓
Conditional Access	✓	✓	✓	✓
Risk-Based Conditional Access	✗	✗	✓	✓
OneDrive for Business	✓	✓	✓	✓
SharePoint Online	✓	✓	✓	✓
Microsoft Cloud App Security	✗	✓	✓	✓
Microsoft Teams	✓	✓	✓	✓
Windows Virtual Desktop	✓	✓	✓	✓
Work Folders	✓	✓	✓	✓

- Microsoft 365 E3 forms the Common Cloud Commitment of the Australian Government Volume Sourcing Agreement (VSA 4) with Microsoft.