Microsoft

Blueprint

Office 365 Security and Compliance Blueprint - UK-OFFICIAL

12/12/2018

Version 1.0 Final

Prepared by

Microsoft Services UK

Table of Contents

Table of Tables

Table of Figures

1 Overview

Microsoft provides a secure cloud service and has numerous independently verified attestation on its configuration state, from ISO the ISO 27000 family of standards, guidelines published by the National Institute of Standards and Technology (NIST) like NIST 80053, and others. Our security framework enables customers to evaluate how Microsoft meets or exceeds its security standards and implementation guidelines. Microsoft's Information Security Policy also aligns with ISO 27002, augmented with requirements specific to Office 365, the external attestation and other evidence can be found here:

https://servicetrust.microsoft.com.

The UK Government's NCSC and Cabinet Office; created the 14 cloud security principles to help customers evaluate cloud services and provide a broad non-definitive list of controls that could be used by generic cloud providers to meet the security obligations when operating at UK OFFICIAL.

This document came out of a need to help UK Government departments configure Office 365 in a way that helps them meet their obligations and leverages the features and capabilities that are present within the service. It draws on broad experience across UK government, industry and draws heavily in already existing "best practice.

It is not intended to be a step by step guide, rather it is intended to help the reader, understand how the 14 cloud security principles can be supported natively within the service."

1.1 Document Structure

The following sections of this document take each of the 14 cloud security principles and firstly state where responsibility for the security principle lies. This is either, **Customer**, **Microsoft** or **Shared**. There is then a table that describes what the **Customer** needs to do in order to meet the minimum recommended controls for each security principle as well as what security controls **Microsoft** uses as part of operating Office 365, Azure AD or the underlying Azure services on which these services run.

The recommended security controls described in this document are broken down into two groups. The basic capability is available with the Microsoft M365 E3 license, where additional capability is recommended that is available with the Microsoft Security and Compliance Package it is clearly identified in the document.

An example is illustrated in the section below.

1.2 NCSC Cloud Security Principle N: Security Principle

Description of the Cloud Security Principle

Table 1: Cloud Security Principle

Responsibility: *Customer /Microsoft / Shared*	
Customer	Describes security configuration or controls that should be implemented by the customer to achieve the minimum configuration recommended. **Recommendation 1 -** used to describe the recommended security control. **Security and Compliance Package enhanced control –** describes a recommended security control that is available when customers have purchased the Security and Compliance Package
Provider	Describes relevant security controls that Microsoft, as the cloud service provider, utilises as part of operating Office 365 and associated cloud services.

1.3 Summary of responsibilities

Table 2 below provides a summary of where the responsibility lies for the individual Cloud Security Principle.

Table 2: Summary of responsibility against Cloud Security Principle

Cloud Security Principle		Responsibility
Data in Transit Protection		Microsoft
Asset Protection and Resilience	Physical Location and Legal Jurisdiction	Customer
	Datacenter Security	Microsoft
	Data at Rest Protection	Microsoft
	Data Sanitisation	Microsoft
	Equipment Disposal	Microsoft
	Physical Resilience and Availability	Microsoft
Separation between users		Microsoft
Governance framework		Microsoft
Operational Security	Configuration and change Management	Shared

Cloud Security Principle		Responsibility
	Vulnerability Management	Microsoft
	Protective Monitoring	Shared
	Incident management	Shared
Personnel Security		Shared
Secure Development		Microsoft
Supply chain security		Microsoft
Secure user management	Authentication of Users to Management Interfaces and within support Channels	Shared
	Separation and Access Control within Management Interfaces	Shared
Identity and Authentication		Customer
External Interface Protection		Shared
Secure Service Administration		Shared
Audit Information for Users		Shared
Secure Use of the Service		Customer

1.4 Summary of customer controls

Table 3 below provides a summary of the recommended controls that organisations should consider meeting the minimum-security standard outlined in this document.

Table 3: Summary of controls recommended for each of the cloud security principles

Cloud Security Principle	Basic capability	Enhanced capability
Data in Transit Protection		
Asset Protection and Resilience		
• Physical Location and Legal Jurisdiction	Choice of whether UK Geo is chosen	
Datacenter Security		
Data at Rest Protection		Use of Customer Key

Cloud Security Principle	Basic capability	Enhanced capability
Data Sanitisation		
Equipment Disposal		
Physical Resilience and Availability		
Separation between users		
Governance framework		
Operational Security		
Configuration and change Management	Use of Azure AD Utilisation of RBAC model	Azure AD Privileged Identity Management
Vulnerability Management		
Protective Monitoring	Azure Security Center Cloud App Security	
Incident management		
Personnel Security		
Secure Development	Security Development Lifecycle	
Supply chain security		
Secure user management	Use dedicated account for administration Use Privileged Access Workstations Enforce MFA for Administrators	Use Azure AD Privileged Identity Management
Authentication of Users to Management Interfaces and within support Channels	Use dedicated account for administration Use Privileged Access Workstations Limit the number of accounts that are Global Admins Utilise Office 365 RBAC model Enforce MFA for Administrators	Use Azure AD Privileged Identity Management
Separation and Access Control within Management Interfaces		

Cloud Security Principle	Basic capability	Enhanced capability
Identity and Authentication	Use Azure AD Conditional Access Turn off legacy authentication protocol support Enable Extranet Lockout in ADFS Use Privileged Access Workstations	
External Interface Protection	Use Conditional Access backed MFA Utilise Office 365 RBAC Turn off legacy authentication protocol support	Azure AD Identity Protection Azure AD Privileged Identity Management
Secure Service Administration	Use Privileged Access Workstations Use Conditional Access backed MFA Utilise Office 365 RBAC Define emergency break glass accounts Turn off legacy authentication protocol support	Azure AD Identity Protection Azure AD Privileged Identity Management
Audit Information for Users	Enable Mailbox auditing Enable Office 365 Cloud App Security	
Secure Use of the Service	Use Conditional Access backed MFA Turn off legacy authentication protocol support Reduce use of passwords Use Office 365 Secure Score	

2 NCSC Cloud Security Principles

The following sections describe how Office 365 meets the NCSC’s 14 cloud security principles and specific configuration guidance for customers to ensure that their use of Office 365 aligns with appropriate recommended security controls.

2.1 NCSC Cloud Security Principle 1: Data in Transit Protection

User data transiting networks should be adequately protected against tampering and eavesdropping.

This should be achieved through a combination of:

- network protection - denying your attacker the ability to intercept data
- encryption - denying your attacker the ability to read data

Responsibility: *Microsoft Office 365*	
Customer	Microsoft Office 365 only allows connections over secure connections. Customers are not able to change this.
Provider	Microsoft and by inheritance Office 365 uses the industry-standard Transport Layer Security (TLS) 1.2 protocol with 2048-bit RSA/SHA256 encryption keys, as recommended by NCSC, to encrypt communications both between the customer and the cloud, and internally between Microsoft systems and datacentres. For example, when administrators use the Office Admin Center portal to manage the service for their organization, the data transmitted between the portal and the administrator's device is sent over an encrypted TLS channel. When an email user connects to https://outlook.office365.com using a standard web browser, the HTTPS connection provides a secure channel for receiving and sending email.

2.2 NCSC Cloud Security Principle 2: Asset Protection and Resilience

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

The aspects to consider are:

1. Physical Location and Legal Jurisdiction
2. Datacentre Security
3. Data at Rest Protection
4. Data Sanitisation
5. Equipment Disposal
6. Physical Resilience and Availability

2.2.1 NCSC Cloud Security Principle 2.1: Physical Location and Legal Jurisdiction

To understand the legal circumstances under which your data could be accessed without your consent you must identify the locations at which it is stored, processed and managed. You will also need to understand how data-handling controls within the service are enforced, relative to UK legislation. Inappropriate protection of user data could result in legal and regulatory sanction, or reputational damage.

Responsibility: *Customer*

> NOTE:
>
> Office 365 services are deployed regionally, and customers can configure certain Office 365 services to store customer data only in a single region. Microsoft Office 365 provides a list of globally available datacentres to provide availability and reliability on a global scale. All Office 365 datacentres have been certified against the ISO/IEC 27001:2013. The UK Geo consists of 2 regions: UK South and UK West.

Customer	Microsoft Office 365 prompts the administrator for the geographical region to deploy Microsoft Office 365 services into when it is initially set up. The recommended Geo region for new Microsoft Office 365 tenant is United Kingdom. Refer to Where is your data located? for more details of where Microsoft Office 365 stores core customer data at rest for new customers when United Kingdom Geo is selected as the location for their new Office 365 tenant. Some services may store customer data at rest in other locations The following services are currently available in the UK Geo:

Responsibility: *Customer*

Cloud Service	Location
Exchange Online	Durham, England London, England
OneDrive for Business	Durham, England London, England
SharePoint Online	Durham, England London, England
Microsoft Teams	London, England Cardiff, Wales
Azure Active Directory	Ireland Netherlands United States

> IMPORTANT:
>
> Currently Azure Active Directory is not hosted in UK Geo.

The Office 365 data maps page informs only new customers or tenants. Existing customers may be in a Geo or datacentre location other than what is documented here. This could be a result of your tenant being provisioned before Microsoft established the UK Geo.

You can verify the location of customer data for your current tenants in the Data Location card on the Organization Profile page in the Office 365 Admin Center, https://portal.office.com/AdminPortal/Home#/companyprofile .

New Office 365 tenants are defaulted to a datacentre geography (Geo) based on the country of the transaction associated with that tenant's first subscription

Provider Not Applicable

Further reading

For more details regarding where Office 365 services are hosted refer to https://products.office.com/en-us/where-is-your-data-located?geo=UnitedKingdom#UnitedKingdom

2.2.2 NCSC Cloud Security Principle 2.2: Datacentre Security

Locations used to provide cloud services need physical protection against unauthorized access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.

Responsibility: *Microsoft*	
Customer	Customers do not have physical access to any system resources in Azure datacentres; datacentre security protection measures are implemented and managed by Microsoft Azure. This principle is inherited from Microsoft Azure.
Provider	Microsoft Office 365 runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft online services. Each facility is designed to run 24x7x365 and employs various industry standard measures to help protect operations from power failure, physical intrusion, and network outages. These datacentres comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel Microsoft Office 365 customers can be confident that physical security controls are in place at all Microsoft Office 365 datacentres due to Microsoft Office 365 holding certificates at all datacentres for the ISO/IEC 27001:2013 standard. The UK Geo consists of two regions: UK South and UK West.

Further reading

For more details regarding where Office 365 services are hosted refer to https://products.office.com/en-us/where-is-your-data-located?geo=UnitedKingdom#UnitedKingdom

2.2.3 NCSC Cloud Security Principle 2.3: Data at Rest Protection

To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service should be protected regardless of the storage media on which it's held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.

Responsibility: *Microsoft*

Customer

Some customers might have legal or regulatory requirements that stipulate that data at rest must be protected so that only the customer is able to access the data. For these customers, the use of the Customer Key option in Service Encryption is available

Customer Key enables multi-tenant services to provide per-tenant key management. Using Customer Key, you can generate your own cryptographic keys using either an on-premises Hardware Security Module ((HSM) or Azure Key Vault. Regardless of how the key is generated, customers use Azure Key Vault to control and manage the cryptographic keys used by Microsoft Office 365. Once the customer's keys are stored in Azure Key Vault, the keys can be assigned to workloads such as Exchange Online and SharePoint Online and used to encrypt the data.

Customer Key helps you meet compliance obligations because you control the encryption keys that Microsoft Office 365 uses to decrypt data, refer to https://support.office.com/en-us/article/service-encryption-with-customer-key-for-office-365-faq-41ae293a-bd5c-4083-acd8-e1a2b4329da6 for more details.

> IMPORTANT:
>
> The use of Customer Key is not necessary to meet the OFFICIAL threat model the security controls implemented in Service Encryption are sufficient.

> NOTE:
>
> Customer Key is included in the Security Compliance Package although customers must also purchase the appropriate license for using Azure Key Vault.

Provider

For other customers who do not have that legal or regulatory requirement to use Customer Key for Service Encryption Microsoft Office 365 is protected by several technologies and processes, including various forms of encryption. Microsoft uses volume-level and file-level service-side technologies in Office 365 that encrypt customer content[1] at rest.

In addition to the baseline, volume-level encryption that's enabled through BitLocker and Distributed Key Manager (DKM), Office 365 offers an added layer of encryption,

[1] Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), SharePoint Online site content and the files stored within sites, and files uploaded to OneDrive for Business.

called *service encryption*, at the application level for customer content in Office 365, including data from Exchange Online, Skype for Business, SharePoint Online, and OneDrive for Business. Service Encryption allows for two key management options:

- Microsoft manages all encryption keys.
- The customer supplies root keys used with service encryption and the customer manages these keys using Azure Key Vault. Microsoft manages all other keys. This option is called Customer Key.

Service encryption provides multiple benefits. For example, it:

- Provides separation of Windows operating system administrators from access to customer data stored or processed by the operating system.
- Enhances the ability of Office 365 to meet the demands of customers that have compliance requirements regarding encryption.

Lockbox

Although it is extremely rare, a customer could request assistance from Microsoft that may expose a Microsoft engineer to the customer's content to assist them with an issue. To control access to Exchange Online (which includes any Skype for Business data stored in the users' mailboxes[2]) and SharePoint Online (which includes OneDrive for Business), Microsoft uses an access control system called Lockbox. Before any Microsoft engineer can access any Exchange Online or SharePoint Online systems or data, they must submit an access request using Lockbox.

Using Lockbox is required for all elevated access to Exchange Online or SharePoint Online.

Lockbox processes requests for permissions that grant engineers the ability to perform operational and administrative functions within the service. Engineers submit requests through Lockbox, which must be approved by a manager prior to the engineer gaining the ability to access Customer Data. Upon manager approval, the engineer has time-limited and scope-limited access to Customer Data to work on the customer's issue.

[2] Skype for Business coverage does not include Skype Meeting Broadcast recordings or content uploaded to meetings by users.

Responsibility: *Microsoft*

Enhanced Security and Compliance Package capability

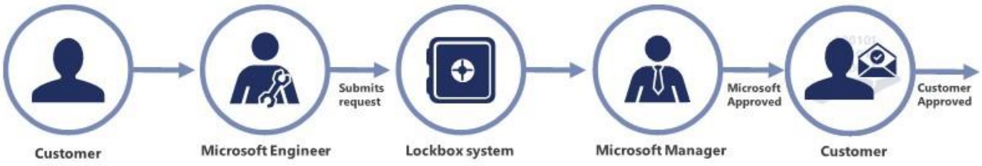
The following are suggested controls that will enhance the secure administration of Azure AD and Office 365 but require additional components that are not included in Office 365 E3 subscription

Customer Lockbox for Office 365

Customer Lockbox for Office 365 can help you meet compliance obligations, such as those found in FedRAMP and HIPAA, if you need procedures in place for explicit data access authorization. In the rare instance when a Microsoft service engineer needs access to your data, you grant that access only to data required to resolve the issue and for a limited amount of time. Actions taken by the support engineer are logged for auditing purposes and are accessible via the Office 365 Management Activity API and the Security and Compliance Center. Customer Lockbox inserts the customer into the Lockbox approval process and provides them with the ability to control authorization of Microsoft access to their Exchange Online or SharePoint Online content for service operations.

All service requests for Exchange Online and SharePoint Online are handled by the Lockbox system. And with Customer Lockbox, any service operation necessitating access to these services with exposure to Customer Data goes through the Lockbox approval process, and then enables the customer to approve or reject the request thereafter.

Figure 1: Customer Lockbox Workflow



If the request is rejected by the customer, the Microsoft engineer will not have access to the customer’s content and will not be able to complete the service operation. If the request is approved by the customer, the Microsoft engineer will have limited just-in-time access to the customer’s content through monitored and constrained management interfaces. With both Lockbox and Customer Lockbox, all approved access is traceable to a unique user, making engineers accountable for their handling of Customer Data.

> NOTE:
>
> Customer Lockbox for Office 365 is included in the Security Compliance Package although customers must also purchase the appropriate license for using Azure Key Vault.

Further reading

For more details on encryption use in Microsoft Office 365 refer to the following documents:

Content Encryption in Microsoft Office 365 – https://aka.ms/office365ce

Encryption in the Microsoft Cloud – https://aka.ms/mcsce

2.2.4 NCSC Cloud Security Principle 2.4: Data Sanitisation

The process of provisioning, migrating and de-provisioning resources should not result in unauthorized access to user data.

Inadequate sanitization of data could result in:

- User data being retained by the service provider indefinitely
- User data being accessible to other users of the service as resources are reused
- User data being lost or disclosed on discarded, lost or stolen media.

Responsibility: *Microsoft*	
Customer	Customers do not have physical access to any system resources in Office 365 datacentres; equipment disposal procedures are implemented and managed by Microsoft Office 365. This principle is inherited from Microsoft Office 365.
Provider	Microsoft has a Data Handling Standard policy for Office 365 that specifies how long customer data will be retained after being deleted. Generally, within Office 365, there are two scenarios in which customer data is deleted: 1. **Active Deletion** A user deletes data, or data private to a user is deleted after that user is deleted by the administrator of an active tenant. 2. **Passive Deletion** The tenant subscription ends. The Data Handling Standard policy also addresses the recycling and disposal of disk drives and failed or retiring servers. Before re-using any disk drives within Office 365, Microsoft performs a physical sanitization process that is compliant with NIST SP 800-88.[3] Disk drives that cannot be re-used are disposed of using a physical destruction process that is performed on-site within the datacentre containing the disks being destroyed. Microsoft uses data erasure units from Extreme Protocol Solutions (EPS). EPS software supports NIST SP 800-88 requirements for cleansing and purging/secure erasure. Prior to cleansing or destruction, an inventory is created by the Microsoft

[3] These procedures are performed by Microsoft Cloud Infrastructure & Operations (MCIO). For more information, see the MCIO audit reports on the Service Trust Preview.

asset manager. If a vendor is used for destruction, the vendor provides a certificate of destruction for each asset destroyed, which is validated by the asset manager.

Failed disks used within Office 365 datacentres are physically destroyed[4] and audited through the ISO process. For hard drives that can't be wiped, Microsoft uses a destruction process that destroys the hard drives (e.g., disintegrates, pulverizes, or incinerates) and renders the recovery of information impossible. Microsoft also retains all records of the destruction. Microsoft performs a similar sanitization process on servers that are being re-used within Office 365. These guidelines encompass both electronic and physical sanitization.

Exchange Online and SharePoint Online have built-in mechanisms for rendering hard-deleted data unrecoverable.

Exchange Online

Exchange Online utilises two distinct types of deletion: soft deletions and hard deletions which apply to both mailboxes and items in a mailbox.

Soft Deletion is when a mailbox has been deleted using the Office 365 Admin Center or Remove-Mailbox PowerShell cmdlet and remains in the Azure Active Directory recycle bin for less than 30 days

Hard Deletion is the next step and occurs under the following circumstances:

- The mailbox has been soft-deleted for more than 30 days and the user account has been hard deleted in Azure Active Directory. All mailbox content will be deleted when this occurs
- The user account has been hard-deleted from Azure Active Directory and the mailbox associated with the user has been soft-deleted for 30 days. If during the 30-day period, a new Azure Active Directory user is synchronized from original recipient account the original mailbox will be hard deleted permanently deleting all mailbox content

> IMPORTANT:
>
> The above deletion scenarios assume that the mailbox is not subject to any legal or eDiscovery hold states if there is any hold type on the mailbox then the mailbox cannot be deleted.

Exchange Online utilizes Page Zeroing as the mechanism to make the deleted data more difficult to recover.

SharePoint Online

When content is deleted form SharePoint Online it is not deleted immediately but is sent to a Site Recycle bin, by default it is retained for 90 days. If the content is deleted form the Site Recycle Bin it is transferred to the Site Collection Recycle Bin,

[4] The appropriate means of disposal is determined by the asset type.

Responsibility: *Microsoft*	
	where it is retained for a further 30 days. A site Collection itself can be recovered by a Site Collection Administrator for 30 days. Hard deletion occurs the when a user purges deleted items form the Site Recycle Bin, and, any retention and backup periods expire, or hen an Administration permanently deletes a site collection. When hard deletion occurs, all encryption keys for the deleted chunks are also deleted, the blocks on the disks where the chucks were previously stored are then marked as unused and available for re-use.

Further reading

For more details on data sanitization in Microsoft Office 365 refer to the following document:

https://aka.ms/office365drdd

For more details on how content is encrypted in Microsoft Office 365 refer to the following document:

http://aka.ms/Office365CE

2.2.5 NCSC Cloud Security Principle 2.5: Equipment Disposal

Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service

Responsibility: *Microsoft*	
Customer	Customers do not have physical access to any system resources in Office 365 datacentres; equipment disposal procedures are implemented and managed by Microsoft Office 365. This principle is inherited from Microsoft Office 365.
Provider	Microsoft implements this principle on behalf of customers and is therefore inherited by Microsoft Office 365. Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling procedures and hardware disposal processes to help assure that no hardware that may contain customer data is made available to untrusted parties. Microsoft Azure follows the NIST SP800-88r1 disposal process with data classification aligned to FIPS-199 Moderate. NIST provides for Secure Erase approach (via hard drive firmware) for drives that support it. For hard drives that can't be wiped Microsoft destroys them and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. All Microsoft cloud services utilize approved media storage and disposal management services.

Further reading

For more details on data sanitization in Microsoft Office 365 refer to the following documents:

https://aka.ms/office365drdd

2.2.6 NCSC Cloud Security Principle 2.6: Physical Resilience and Availability

Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business

Responsibility: *Microsoft*	
Customer	Customers do not have physical access to any system resources in Office 365 datacentres; equipment disposal procedures are implemented and managed by Microsoft Office 365. This principle is inherited from Microsoft Office 365.

Responsibility: *Microsoft*	
	Customers can obtain service specific availability data via the Office Admin Portal, https://portal.office.com/adminportal/home#/servicehealth
Provider	Microsoft Office 365 services have been designed to have redundancy built in thus moving the services beyond the traditional strategy of relying on complex physical infrastructure. By designing the software to be more intelligent less complex physical infrastructure is necessary to achieve the same levels of data resiliency into the services and deliver high availability.

Further reading

For more details on resiliency use in Microsoft Office 365 refer to the following:

Transparent operations from Office 365 - https://products.office.com/en-us/business/office-365-trust-center-operations

Data Resiliency in Microsoft Office 365 - https://aka.ms/Office365DR

2.3 NCSC Cloud Security Principle 3: Separation Between Users

A malicious or compromised user of the service should not be able to affect the service or data of another.

Factors affecting user separation include:

- where the separation controls are implemented - this is heavily influenced by the service model (e.g. IaaS, PaaS, SaaS)
- who you are sharing the service with - this is dictated by the deployment model (e.g. public, private or community cloud)
- the level of assurance available in the implementation of separation controls

Responsibility: *Microsoft*	
Customer	Microsoft Office 365 ensures isolation for each user to prevent one malicious or compromised user from affecting the service or data of another. As such this principle is inherited from Microsoft Azure Active Directory
Provider	One of the primary benefits of cloud computing is concept of a shared, common infrastructure across numerous customers simultaneously, leading to economies of scale. This concept is called *multitenancy*. Microsoft works continuously to ensure that the multi-tenant architecture of Microsoft Office 365 supports enterprise-level security, confidentiality, privacy, integrity, and availability standards. Based upon the significant investments and experience gathered from Trustworthy Computing and the Security Development Lifecycle, Microsoft cloud services, including Office 365, were designed with the assumption that all tenants are potentially hostile to all other tenants, and Microsoft has implemented security measures to prevent the actions of one tenant from affecting the security or service of another tenant, or accessing the content of another tenant. The two primary goals of maintaining tenant isolation in a multi-tenant environment are: 1. Preventing leakage of, or unauthorized access to, customer content across tenants; and 2. Preventing the actions of one tenant from adversely affecting the service for another tenant Multiple forms of protection have been implemented throughout Office 365 to prevent customers from compromising Office 365 services or applications or gaining unauthorized access to the information of other tenants or the Office 365 system itself, including:

Responsibility: *Microsoft*

- Logical isolation of customer content within each tenant for Office 365 services is achieved through Azure Active Directory authorization and role-based access control.
- SharePoint Online provides data isolation mechanisms at the storage level.
- Office 365 uses service-side technologies that encrypt customer content at rest and in transit, including BitLocker, per-file encryption, Transport Layer Security (TLS) and Internet Protocol Security (IPsec). For specific details about encryption in Office 365, see Data Encryption Technologies in Office 365.

Isolation and Access Control in Azure Active Directory

Azure Active Directory was designed to host multiple tenants in a highly secure way through logical data isolation. Access to Azure Active Directory is gated by an authorization layer. Azure Active Directory isolates customers using tenant containers as security boundaries to safeguard a customer's content so that the content cannot be accessed or compromised by co-tenants. Three checks are performed by Azure Active Directory's authorization layer:

1. Is the principal enabled for access to Azure Active Directory tenant?
2. Is the principal enabled for access to data in this tenant?
3. Is the principal's role in this tenant authorized for the type of data access requested?

No application, user, server, or service can access Azure Active Directory without the proper authentication and token or certificate. Requests are rejected if they are not accompanied by proper credentials.

Effectively, Azure Active Directory hosts each tenant in its own protected container, with policies and permissions to and within the container solely owned and managed by the tenant.

Further reading

For more details on Tenant Isolation use in Microsoft Office 365 refer to the following:

Tenant Isolation in Microsoft Office 365 – http://aka.ms/Office365TI

2.4 NCSC Cloud Security Principle 4: Governance Framework

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined. Having an effective governance framework will ensure that procedure, personnel, physical and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments and the appearance of new threats.

Responsibility: *Microsoft*	
Customer	Microsoft Office 365 maintains a documented security governance framework for Office 365 services.
Provider	Microsoft Office 365 service teams develop, document, and maintain under configuration control a current baseline configuration of their production systems. Baseline images are reviewed at least annually and changes to baseline images are reviewed and approved before they are moved into production. Azure which hosts Microsoft Office 365 complies with a broad set of international as well as regional and industry-specific compliance standards, such as ISO 27001, FedRAMP, SOC 1, and SOC 2. Compliance with the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations. Azure is designed with a compliance strategy that helps customers address business objectives as well as industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Office 365 has established a risk management framework, and related processes, for assessing the applicable IT risks and performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and the risk from these threats is formally assessed. This involves monitoring ongoing effectiveness and improvement of the Information Security Management System (ISMS) control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions

Further reading

For more details on governance use in Microsoft Office 365 refer to the following:

Mapping of Cloud Security Alliance Cloud Control Matrix - https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=f7ea9d76-59d2-408e-9bef-c4abf5b30f89&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_Compliance_Guides

2.5 NCSC Cloud Security Principle 5: Operational Security

The service needs to be operated and managed securely to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

There are four elements to consider:

- Configuration and Change Management - you should ensure that changes to the system have been thoroughly tested and authorised. Changes should not unexpectedly alter security properties
- Vulnerability Management - you should identify and mitigate security issues in constituent components
- Protective Monitoring - you should put measures in place to detect attacks and unauthorised activity on the service
- Incident Management - ensure you can respond to incidents and recover a secure, available service

2.5.1 NCSC Cloud Security Principle 5.1: Configuration and change Management

You should have an accurate picture of the services which are being utilized within Microsoft Office 365, along with their configurations and dependencies. Changes which could affect the security of the service should be identified and managed. Unauthorised changes should be detected. Where change is not effectively managed, security vulnerabilities may be unwittingly introduced to a service. And even where there is awareness of the vulnerability, it may not be fully mitigated.

Responsibility: *Shared*	
Customer	Azure Active Directory account privileges are implemented using role-based access control (RBAC) by assigning users to roles providing strict control over which users can view and configure Office 365 services. To be compliant with this principle, further configuration is required by the customer to define the precise RBAC model that is suitable for use in production. As such, these configurations will need to be a part of the customer's change management process.

Responsibility: *Shared*

Office 365 comes with a set of admin roles that you can assign to users in your organization. Each admin role maps to common business functions, and gives people in your organization permissions to do specific tasks in the Office 365 admin centre, for details of the roles refer to About Office 365 admin roles - Office 365

With Azure Active Directory (AD) Privileged Identity Management, you can manage, control, and monitor access within your organization. This includes access to resources in Azure AD, Azure Resources (Preview), and other Microsoft Online Services like Office 365 or Microsoft Intune, refer to Configure Azure AD Privileged Identity Management for further details.

> IMPORTANT:
>
> When you enable Privileged Identity Management for your tenant, a valid Azure AD Premium P2 or Enterprise Mobility + Security E5
>
> This is included in Security Compliance Package

Historically, you could assign a user to an admin role through the Azure portal, other Microsoft Online Services portals, or the Azure AD cmdlets in Windows PowerShell. As a result, that user becomes a **permanent admin**, always active in the assigned role. Azure AD Privileged Identity Management introduces the concept of an **eligible admin**. Eligible admins should be users that need privileged access now and then, but not all-day, every day. The role is inactive until the user needs access, then they complete an activation process and become an active admin for a predetermined amount of time. More and more organizations are choosing to use this approach for reducing or eliminating "standing admin access" to privileged roles.

Careful configuration of the available Azure Active Directory and Office 365 administrative roles is critical to the ongoing configuration and change management control of Azure Active Directory and Office 365. Ensuring that people do not have excessive administrative capabilities by implementing a least privileged approach will significantly improve the overall security posture of the service. If licensed look to implement Azure Active Directory Privileged Identity Management to reduce standing access to privileged roles.

Provider

Microsoft Office 365 and the Azure services that provide the infrastructure and operating system components that the Office 365 services run on perform reviews and update configuration settings and baseline configurations of hardware, software and network devices annually. Changes are developed, tested, and approved prior to entering the production environment from a development and/or test environment.

Microsoft Azure applies baseline configurations using the change and release process for Microsoft Azure software components (e.g. OS, Fabric, RDFE, XStore, etc.) and bootstrap configuration process for hardware and network device

Responsibility: *Shared*	
	components entering Microsoft Azure production environment as outlined below. The baseline configurations required for Azure-based services are reviewed by the Azure Security and Compliance team and by service teams as part of testing prior to deployment of their production service Our standard baseline configuration requirements for servers, network devices, and other Microsoft applications are documented where the standards outline the use of a standard package. These packages are pretested and configured with security controls. Changes, such as updates, hotfixes, and patches made to the production environment, follow the same standard change management process. Patches are implemented within the time frame specified by the issuing company. Changes are both reviewed and evaluated by our review teams and the Change Advisory Board for applicability, risk, and resource assignment prior to being implemented.

2.5.2 NCSC Cloud Security Principle 5.2: Vulnerability Management

Service providers should have a management processes in place to identify, triage and mitigate vulnerabilities. Services which don't, will quickly become vulnerable to attack using publicly known methods and tools.

Responsibility: *Microsoft*	
Customer	Not applicable
Provider	Security update management helps protect systems from known vulnerabilities. Office 365 uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Office 365 is also able to draw on the resources of the Microsoft Security Response Center (MSRC), which identifies, monitors, responds to, and resolves security incidents and cloud vulnerabilities around the clock, each day of the year. All vulnerabilities identified by the vulnerability scanning process are classified by risk. Vulnerability remediation is conducted in accordance with Office 365 policy. • High-risk vulnerabilities are mitigated within 30 days. • Medium-risk vulnerabilities are mitigated within 90 days.

Responsibility: ***Microsoft***

Changes, such as updates, hotfixes, and patches made to the production environment, follow the same standard change management process. Patches are implemented within the time frame specified by the issuing company.

The use of anti-malware software is a principal mechanism for protection of your assets in Office 365 from malicious software. The software detects and prevents the introduction of computer viruses and worms into the service systems. It also quarantines infected systems and prevents further damage until remediation steps are taken. Anti-malware software provides both preventive and detective control over malicious software.

Further reading

For details of how Office 365 patches the environment refer to [Office 365 - MT FedRAMP System Security Plan v5]

2.5.3 NCSC Cloud Security Principle 5.3: Protective Monitoring

A service which does not effectively monitor for attack, misuse and malfunction will be unlikely to detect attacks (both successful and unsuccessful). As a result, it will be unable to quickly respond to potential compromises of your environments and data

Responsibility: ***Shared***

Customer

The customer is responsible for establishing an incident management process for customer-deployed resources that interface with Microsoft Office 365 services.

The customer implementation statement should address reporting incidents and alerts, supporting timely incident responses, and forwarding information to the PGA and other HMG organizations as appropriate.

The use of Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks

For more advanced capabilities organisations could consider Microsoft Advanced Threat Protection (ATP) suite of products, Office, Windows Defender, and Azure.

> IMPORTANT:
>
> The ATP suite is included in the Security Compliance Package

Responsibility: *Shared*

Provider

Microsoft Azure Security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include the Monitoring Agent (MA) and System Center Operations Manager (SCOM), which are configured to provide-time alerts to Microsoft Azure Security personnel in situations that require immediate action.

Microsoft also performs extensive monitoring and auditing of all delegation, all use of privileges, and all operations that occur within Office 365. Office 365 access control is an automated process built on the principle of least privilege and to incorporate data access controls and audits:

- All permitted access is traceable to a unique user, making administrators accountable for their handling of customer content.
- Access control requests, approvals, and administrative operations logs are captured for analysis of security insights and malicious events.
- Access levels are reviewed in near real-time based on security group membership to ensure that only users who have authorized business justifications and meet the eligibility requirements have access to the systems.
- Office 365, its access controls, and supporting services, including Azure Active Directory and our physical datacentres, are regularly audited by independent third-parties for compliance with ISO/IEC 27001, ISO/IEC 27018, SOC, FedRAMP, and other standards.
- Office 365 engineers are required to take yearly security training reviewing elevated access best practices and risks and acknowledge Microsoft's security and privacy policies to continue maintaining their entitlements to the service.

Automated alerts are triggered when suspicious activity is detected, such as multiple failed logins within a short period. The Office 365 Security Response team uses machine learning and big data analysis to review and analyse activity for irregular access patterns and to proactively respond to anomalous and illicit activities. Microsoft also employs a dedicated team of penetration testers and engages in periodic red team and blue team exercises to find security and access control issues in the service. Customers may also verify the effectiveness of access control systems by using audit reports and the management activity API provided by Office 365.

Further reading

For more information, see Office 365 Management Activity API reference and Auditing and Reporting in Office 365.

2.5.4 NCSC Cloud Security Principle 5.4: Incident Management

Unless carefully pre-planned incident management processes are in place, poor decisions are likely to be made when incidents do occur, potentially exacerbating the overall impact on users. These processes needn't be complex or require large amounts of description, but good incident management will minimise the impact to users of security, reliability and environmental issues with a service

Responsibility: *Shared*

Customer

The customer is responsible for establishing an incident management process for customer-deployed resources (to include applications, operating systems, databases, and software). The customer implementation statement should address reporting incidents and alerts, supporting timely incident responses, and forwarding information to the PGA and other HMG organizations as appropriate.

Establish incident/emergency response plan owners

Performing incident response effectively is a complex undertaking. Therefore, establishing a successful incident response capability requires substantial planning and resources. It is essential that you continually monitor for cyber-attacks and establish procedures for prioritizing the handling of incidents. Effective methods of collecting, analysing, and reporting data are vital to build relationships and to establish communication with other internal groups and plan owners.

In the event of an incident occurring contact your Microsoft Technical Account Manager and raise a support request in the Office Admin Portal

Provider

Microsoft has implemented a security incident management process to facilitate a coordinated response to incidents should one occur.

If Microsoft becomes aware of any unauthorized access to any customer data stored on its equipment or in its facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of customer data, Microsoft has stated that it will:

- Promptly notify the customer of the security incident;
- Promptly investigate the security incident and provide the customer with detailed information about the security incident; and
- Take reasonable and prompt steps to mitigate the effects and minimize a damage resulting from the security incident.

The Office 365 Security team and the service teams work together on and take the same approach to security incidents, which is based on the NIST 800-61 response management phases:

- Preparation Refers to the organizational preparation that is needed to be able to respond, including tools, processes, competencies, and readiness.

Responsibility: *Shared*

- Detection & Analysis   Refers to the activity to detect a security incident in a production environment and to analyse all events to confirm the authenticity of the security incident.
- Containment, Eradication, Remediation   Refers to the required and appropriate actions taken to contain the security incident based on the analysis done in the previous phase. Additional analysis may also be necessary in this phase to fully remediate the security incident.
- Post-Incident Activity   Refers to the post-mortem analysis performed after the remediation of a security incident. The operational actions performed during the process are reviewed to determine if any changes need to be made in the Preparation or Detection & Analysis phases.

Further reading

Security incident management in Microsoft Office 365 – http://aka.ms/Office365SIM
http://aka.ms/Office365SIM

2.6 NCSC Cloud Security Principle 6: Personnel Security

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel. The service provider should subject personnel to security screening and regular security training. Personnel in these roles should understand their responsibilities. Providers should make clear how they screen and manage personnel within privileged roles

Responsibility: *Shared*	
Customer	The customer is responsible for screening individuals and providing regular security training for individuals with access to customer-deployed resources. The customer implementation statement should address the screening criteria for roles and the frequency of security training Attention should be paid to any individual who has privileged access to any of the Office 365 services but especially Azure AD.
Provider	Microsoft personnel who operate Office 365 services and provide customer support (or Microsoft subcontractors who assist with platform operations, troubleshooting, and technical support) undergo a Microsoft standard background (or equivalent) check to evaluate employee education, employment, and criminal history. The background checks are broadly in line with the requirements of the UK Government's BPSS/BS7858. They do not specifically include a formal identity check. Microsoft includes nondisclosure provisions in its employee and subcontractor contracts. All appropriate Microsoft employees and subcontractors take part in a Microsoft Azure sponsored security-training program that informs staff of their responsibilities for information security. Microsoft Azure, and by association Microsoft Office 365, services staff or subcontractors suspected of committing breaches of security and/or violating the Information Security Policy are subject to an investigation process and appropriate disciplinary action up to and including termination. If the circumstances warrant it, Microsoft may refer the matter for prosecution by a law enforcement agency. To supplement this system of background checks and security education, Microsoft deploys combinations of preventive, defensive, and reactive controls to help protect against unauthorized developer and/or administrative activity, including the following mechanisms: • Tight access controls on sensitive data, including a requirement for two-factor smartcard-based authentication to perform sensitive operations. • Combinations of controls that enhance independent detection of malicious activity. • Multiple levels of monitoring, logging, and reporting.

Further reading

For more details of how Office 365 administrator personnel controls are performed refer to https://aka.ms/Office365AAC

2.7 NCSC Cloud Security Principle 7: Secure Development

Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity

Responsibility: *Microsoft*	
Customer	Whilst the customer is not responsible for developing Microsoft Office 365 services a core consideration is any 3rd party applications that integrate with Microsoft Office 365 services or are built on top of the underlying services should also follow a secure development process. Any inhouse applications that tightly integrate with Office 365 should also follow Microsoft Security Development Lifecycle (SDL) to ensure that underlying services cannot be compromised as a result of weaknesses in the custom code.
Provider	The Microsoft Security Development Lifecycle (SDL) is a comprehensive security assurance process that informs every stage of design, development, and deployment of our software and services, including Office 365. Through design requirements, analysis of attack surface, and threat modelling, the SDL helps us predict, identify, and mitigate vulnerabilities and threats from before a service is launched through its entire BitLocker production lifecycle. We continuously update the SDL using the latest data and best practices to help ensure that new services and software associated with Office 365 are highly secure from day one.

2.8 NCSC Cloud Security Principle 8: Supply Chain Security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement. Cloud services often rely upon third party products and services. Consequently, if this principle is not implemented, supply chain compromise can undermine the security of the service and affect the implementation of other security principles

Responsibility: *Microsoft*	
Customer	The customer is responsible for providing secure supply chain documentation for any third-party acquired software and operating systems used in their Azure subscription. The customer implementation statement should address the exception to follow processes identified by this supply chain documentation.
Provider	The Microsoft Cloud Supply Chain (MCSC) group consists of six unique teams each contributing to protecting Microsoft Office 365 from threats to the Supply Chain. • Procurement • Customer Operations • Deployment Quality • Supplier Relationship Management • Spares

Further reading

For more information regarding Microsoft's MCSC group, refer to https://servicetrust.microsoft.com/ViewPage/UKBlueprints?command=Download&downloadType=Document&downloadId=f7ad3784-3399-4fb6-b504-430d96bf835d&docTab=1326d870-3360-11e8-8c4a-e9dddee860a6_IaaS

2.9 NCSC Cloud Security Principle 9: Secure User Management

Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.

The aspects to consider are:

- Authentication of users to management interfaces and support channels
- Separation and access control within management interfaces

2.9.1 NCSC Cloud Security Principle 9.1: Authentication of Users to Management Interfaces and within support Channels

To maintain a secure service, users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the service. These activities may be conducted through a service management web portal, or through other channels, such as telephone or email. They are likely to include such functions as provisioning new service elements, managing user accounts and managing user data. Service providers need to ensure that all management requests, which could have a security impact, are performed over secure and authenticated channels. If users are not strongly authenticated then an imposter may be able to successfully perform privileged actions, undermining the security of the service or data

Responsibility: *Shared*	
Customer	When administrators access the Microsoft Office 365 Admin or Azure AD blade in Azure portal to manage Office 365 services and Azure AD resources for their organization, the data transmitted between the portal and the administrator's device is sent over an encrypted Transport Layer Security (TLS) channel using 2048-bit RSA/SHA256 encryption keys, as recommended by NCSC. Before an Administrative User can access the management interfaces for Microsoft Office 365 they must first be authenticated against Azure Active Directory. Details of the authentication and identity configuration options that are available in Microsoft Office 365 https://support.office.com/en-us/article/Understanding-Office-365-identity-and-Azure-Active-Directory-06a189e7-5ec6-4af2-94bf-a22ea225a7a9 Once Authentication has successfully completed access to administration interfaces is granted based on the enforced logical access authorizations using role-based access control enforced by Azure Active Directory by assigning users to roles. Azure Active Directory roles assigned to users or groups control logical access to resources within Office 365 Services as well as Azure AD.

Responsibility: *Shared*

Refer to Section **Error! Reference source not found.** for further guidance on recommended configuration of how authentication is configured to meet NCSC guidance when using Office 365.

The integrity of the Administrative Accounts that are used to manage Microsoft Office 365 services, including Azure Active Directory, is a core component to the security of the data that is stored in the services.

Use dedicated administrative accounts

Ensure that administrators always do their day-to-day business and standard "unprivileged" users by ensuring that the use dedicated administrative accounts.

These accounts should be anchored in Azure AD, Cloud ID using .onmicrosoft.com namespace and as such will not have any privileges in the on-premises AD DS.

All cloud administration accounts should be assigned to appropriate privileged roles in Azure AD or Office 365, e.g. Exchange Administrator.

Use Privileged Access Workstations to administer cloud services

The customer is responsible for ensuring a secure workstation for administration of their Azure AD and Office 365 tenant. Attackers may attempt to target privileged accounts to gain access to an organization's data and systems, so they can disrupt the integrity and authenticity of data, through malicious code that alters the program logic or snoops the admin entering a credential. Privileged Access Workstations (PAWs) provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket. By deploying privileged access workstations, you can reduce the risk that admins enter admin credentials except on a desktop environment that has been hardened. For more information, see Privileged Access Workstations.

Enforce MFA for all privileged cloud administrative accounts

The customer is responsible for enforcing multi-factor authentication for all privileged administrative accounts. It is recommended that MFA is enforced through a conditional access policy, scoped to any (all) applications and services and a group of administrative users. It is also recommended that the policy requires a domain-joined or managed device, again enforced through the same conditional access policy. Such a policy would implement two grant controls, MFA and domain-joined / managed, and mandates that administrative users access resources from trusted (managed) systems and utilise a more secure authentication mechanism.

Responsibility: *Shared*

> NOTE:
>
> Azure Active Directory Premium P1, which is included with Enterprise Mobility + Security (EMS) E3 is a requirement for Conditional Access and Multi-Factor Authentication.

Enhanced Security and Compliance Package capability

The following are suggested controls that will enhance the secure administration of Azure AD and Office 365 but require additional components that are not included in Office 365 E3 subscription

Azure AD Privileged Identity Management

To further enhance the security of Global Administrator and other privileged accounts organisations should consider using Azure AD Privileged Identity Management (PIM).

> NOTE:
>
> PIM is available to customer with Azure Active Directory Premium P2, which is included with Enterprise Mobility + Security (EMS) E5 or you can purchase individual licenses for Global Administrator accounts.
>
> Also included in Security Compliance Package

Rather than having any Global Administrator accounts be permanently assigned the global administrator role they become eligible administrators. The global administrator role is inactive until someone needs it. You then complete an activation process to add the global administrator role to the global administrator account for a predetermined amount of time. When the time expires, PIM removes the global administrator role from the global administrator account.

Using PIM and this process significantly reduces the amount of time that your global administrator accounts are vulnerable to attack and use by malicious users.

Whilst the guidance above focuses on accounts that are members of the Global Administrator role the same recommendations apply to an account that have wide-ranging permissions to access data or make configuration changes in Office 365, e.g. eDiscovery Administrator or security / compliance administrator accounts, should also be protected in the same manner.

For more information, see Configure Azure AD Privileged Identity Management.

Provider Microsoft has invested heavily and accordingly in systems and controls that automate most Office 365 operations while intentionally limiting Microsoft's access to customer content. Humans govern the service, and software operates the service. This enables Microsoft to manage Office 365 at scale, as well as

Responsibility: *Shared*	
	manage the risks of internal threats to customer content such as malicious actors, the spear-phishing of a Microsoft engineer, and so forth. By default, Microsoft engineers have zero standing administrative privileges and zero standing access to customer content in Office 365. A Microsoft engineer can have limited, audited, and secured access to a customer's content for a limited amount of time, but only when necessary for service operations, and only when approved by a member of Microsoft senior management (and for customers that are licensed for the Customer Lockbox feature, the customer).

Further reading

Refer to https://aka.ms/Office365AAC

2.9.2 NCSC Cloud Security Principle 9.2: Separation and Access Control within Management Interfaces

Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If users are not adequately separated within management interfaces, one user may be able to affect the service, or modify the data of another. Your privileged administrative accounts probably have access to large volumes of data. Constraining the permissions of individual users to those necessary can help to limit the damage caused by malicious users, compromised credentials or compromised devices. Role-based access control provides a mechanism to achieve this and is likely to be a particularly important capability for users managing larger deployments. Exposing management interfaces to less accessible networks (e.g. community rather than public networks) makes it more difficult for attackers to reach and attack them, as they would first need to gain access to one of these networks. Guidance on assessing the risks of exposing interfaces to different types of networks is provided under Principle 11.

Responsibility: *Shared*	
Customer	Customers administer their Microsoft Office 365 resources through the Office Admin Portal, Azure AD blade and Intune management blade in the Azure Admin Portal. In addition to the web interfaces listed above there are also PowerShell interfaces to administer the services listed above. Web access to the Azure portal is secured by industry-standard Transport Layer Security (TLS) 1.2 connections using 2048-bit RSA/SHA256 encryption keys, as recommended by NCSC. Underpinning the identity and authorization controls is Azure AD. Establishing a robust delegation of administration model is an important aspect of securing the services. Azure AD, and Office 365 services support a Role-based access controls

(RBAC) model that should be configured to enable customers to provide limited access to Azure and Office 365 management resources for specific users and groups.

Office 365 allows you to manage your data much in the same way data is managed in on-premises environments.

> IMPORTANT:
>
> The person who signs up an organization for Office 365 automatically becomes a global administrator (admin).

The global admin has access to all features in the management portals (e.g., admin centres and remote PowerShell), and can create or edit users, assign admin roles to others, reset user passwords, manage user licenses, manage domains, and approve Customer Lockbox requests, among other things. At a minimum it is recommended that each organization designate at least two admin account, refer to Managing emergency access administrative accounts in Azure AD. Depending on the size of your organization, you may want to designate several admins who serve distinct functions.

For information about assigning admin roles and permissions, see Assigning admin roles in Office 365 and About Office 365 admin roles.

For access control purposes, Office 365 data is categorized as either Customer Data or other types of data. Customer Data is all data provided by or on behalf of a customer through the customer's use of Office 365 services, examples of customer data are listed below:

1. Customer content, content directly created or uploaded by Office 365 users including emails, SharePoint Online content, instant messages, calendar items, documents, and contacts stored in Office 365
2. End-user identifiable information (EUII), data that is unique to a user or that is linkable to an individual user but does not include customer content

Other types of data include

1. Account data includes administrative data, which is the information provided by administrators when they sign-up or purchase services, and payment data, which is information about payment instruments, such as credit card details
2. organizationally identifiable information, Data that can be used to identify a tenant; or usage data; it is not linkable to an individual user and does not include customer content

Responsibility: *Shared*

3. System metadata includes service logs that contain configuration settings, system status, Microsoft IP addresses, and technical information about subscriptions and tenants

Use dedicated administrative accounts

Ensure that administrators always do their day-to-day business and standard "unprivileged" users by ensuring that the use dedicated administrative accounts.

These accounts should be anchored in Azure AD, Cloud ID using .onmicrosoft.com namespace and as such will not have any privileges in the on-premises AD DS.

All cloud administration accounts should be assigned to appropriate privileged roles in Azure AD or Office 365, e.g. Exchange Administrator.

Limit the number of accounts that are Global Admins

Ensure that the number of accounts that are members of Global Admin groups for Azure AD and Office 365 are kept to a minimum, it is suggested that no more than 5 accounts are members of Global Admin roles.

Turn on multi-factor authentication for admin accounts

Require Azure Multi-Factor Authentication (MFA) at sign-in for all individual users who are permanently assigned to one or more of the Azure AD admin roles: Global administrator, Privileged Role administrator, Exchange Online administrator, and SharePoint Online administrator.

Utilise role-based access control to reduce standing privilege of accounts

Office 365 Enterprise follows a role-based access control (RBAC) model: permissions and capabilities are defined by management roles. The person who signs up for Office 365 for his or her organization automatically becomes a global administrator, or top-level administrator. There are five administrator roles: global administrator, billing administrator, password administrator, service administrator, and user management administrator. For more information about administrator roles in Office 365 Enterprise, including how they apply to Exchange Online, SharePoint Online, and Skype for Business Online administration, see Assigning administrator roles.

Enhanced Security and Compliance Package capability

The following are suggested controls that will enhance the secure administration of Azure AD and Office 365 but require additional components that are not included in Office 365 E3 subscription

Azure AD Privileged Identity Management

Responsibility: *Shared*

To further enhance the security of Global Administrator accounts organisations should consider using Azure AD Privileged Identity Management (PIM).

> NOTE:
>
> PIM is available to customer with Azure Active Directory Premium P2, which is included with Enterprise Mobility + Security (EMS) E5 or you can purchase individual licenses for Global Administrator accounts.

Rather than having any Global Administrator accounts be permanently assigned the global administrator role they become eligible administrators. The global administrator role is inactive until someone needs it. You then complete an activation process to add the global administrator role to the global administrator account for a predetermined amount of time. When the time expires, PIM removes the global administrator role from the global administrator account.

Using PIM and this process significantly reduces the amount of time that your global administrator accounts are vulnerable to attack and use by malicious users.

Whilst the guidance above focuses on accounts that are members of the Global Administrator role the same recommendations apply to an account that have wide-ranging permissions to access data or make configuration changes in Office 365, e.g. eDiscovery Administrator or security / compliance administrator accounts, should also be protected in the same manner.

For more information, see Configure Azure AD Privileged Identity Management.

Provider

Microsoft has established access control mechanisms to ensure that no one has unapproved access to Customer Data or Access control data, which is used to manage access to other types of data or functions within the environment, including access to customer content or EUII. It includes Microsoft passwords, security certificates, and other authentication-related data or unapproved physical, logical, or remote access to the Office 365 production environment.

The access controls used by Microsoft for operating Office 365 can be grouped into three categories:

1. Isolation Controls
2. Personnel Controls
3. Technology Controls

When combined, these controls help prevent and detect malicious actions in Office 365. While this document focuses on the isolation, personnel, and technology controls used by Microsoft, there is a fourth category of controls: those implemented by customers.

Further reading

For information about how Microsoft implements logical isolation of tenant data within Office 365, see Tenant Isolation in Office 365.

2.10 NCSC Cloud Security Principle 10: Identity and Authentication

All access to service interfaces should be constrained to authenticated and authorised individuals. Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service. Importantly, authentication should occur over secure channels. Email, HTTP or telephone are vulnerable to interception and social engineering attacks

Responsibility: *Customer*

Customer

This blueprint employs a combination of on-premises Active Directory Domain Services and cloud Azure Active Directory for account management, as is typical with Hybrid Identity. User accounts are mastered in the on-premises directory and synchronised to Azure Active Directory and authenticate using the on-premises Active Directory Domain Services user credentials. Azure Active Directory has in-built token replay mitigation for SAML tokens in the federated use case, whereas the Kerberos protocol used by Active Directory Domain Services itself is not subject to replay attacks when either authenticating the user to Active Directory Federation Services (federated use case) or in the Seamless Single Sign-On use-case in conjunction with Pass-Through Authentication.

In Kerberos authentication, the authenticator sent by the client contains additional data, such as an encrypted IP list, client timestamps, and ticket lifetime. If a packet is replayed, the timestamp is checked. If the timestamp is earlier than, or the same as a previous authenticator, the packet is rejected.

Similar protections are used within Azure AD to protect against SAML token replay attacks – each SAML token consumed is first checked against a cache to ensure it has not been previously consumed.

Use Conditional Access to control access to Authentication Interfaces

The customer is responsible for strengthening the authentication experience by including additional controls such as multi-factor authentication or device context. Enhancing the standard credential with either MFA or device authentication reinforces the validity of the user authentication.

Responsibility: *Customer*

Device-based conditional access provides support for two use cases: bring your own and corporate, managed devices. The latter use case relates to Windows 7 and Windows 8.1 automatic workplace joined devices and Windows 10 Hybrid AAD joined devices. Windows 7, Windows 8.1 and Windows 10 Hybrid Joined devices utilise the Active Directory domain to register in the Azure AD tenant; Windows 10 subsequently obtains a primary refresh token, akin to a Kerberos Ticket Granting Ticket, which facilitates both Desktop Single Sign On and introducing the device context to the authentication such that Conditional Access policies can only grant access to apps from domain-joined devices. The default control for device registration is that domain-joined devices locate the correct Azure AD tenant via the Active Directory domain, by searching for a service connection point that describes the relevant endpoints. The registration is typically controlled via Group Policy, i.e. it is scoped or phased. Further controls can be introduced into the surrounding systems such as limiting domain join operations to privileged users, only allowing computers that are members of groups to register both by controlling the feature with Group Policy and constraining obtaining tokens from the Active Directory Federation Services service to specified groups.

Turn off legacy Authentication Protocol support

The customer is responsible for restricting access to legacy clients that cannot support modern authentication and benefit from the CA approach, described previously. It is recommended that CA policies are used to block or deny access to legacy clients.

In the federated use case the simplest approach is to disable the username and password endpoint from being proxied to the Internet, however the CA approach is more flexible in that it blocks at token issuance thus supporting blocking clients from specific apps and services while still allowing and enabling others.

Enable ADFS Web Application Proxy Extranet Lockout

There are several potential attacks open to attackers when the Active Directory Federation Services password change endpoint is proxied to the Internet. The AD FS extranet lockout feature helps mitigate these attacks by facilitating soft-lockout protection, i.e. lockout the username and password attempt at the proxy layer without locking out the Active Directory Domain Services user account. The customer is responsible for mitigating password spray and bulk lockout attacks by enabling an extranet lockout policy using bad password values that are lower than those used in the Active Directory Domain Services domain/forest.

Use Privileged Access Workstations to administer cloud services

The customer is responsible for ensuring a secure workstation for administration of their Azure AD and Office 365 tenant. Attackers may attempt to target privileged accounts to gain access to an organization’s data and systems, so they can disrupt the integrity and authenticity of data, through malicious code that alters the program logic or snoops the admin entering a credential. Privileged Access Workstations (PAWs)

Responsibility: *Customer*	
	provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket. By deploying privileged access workstations, you can reduce the risk that admins enter admin credentials except on a desktop environment that has been hardened. For more information, see Privileged Access Workstations.
Provider	Azure AD is a comprehensive identity and access management service for the cloud that helps secure access to data in on-premises and cloud applications. Azure AD also simplifies the management of users and groups by combining core directory services, advanced identity governance, security, and application access management.

Further reading

For information about how Microsoft implements Identity and Authentication within Office 365:

Security in Office 365 whitepaper

Use conditional access in Azure AD

2.11 NCSC Cloud Security Principle 11: External Interface Protection

All external or less trusted interfaces of the service should be identified and appropriately defended. If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be more significant. You can use different models to connect to cloud services which expose your enterprise systems to varying levels of risk

Responsibility: *Shared*

Customer

Access to Management interfaces controlled using Conditional Access and MFA for Global Administrators (GA) or anyone with privileged access in Microsoft Office 365 services.

Office 365 service delivery interfaces and management interfaces are all exposed to the internet. Whilst there is nothing that a customer can do directly to configure the security of the external interfaces used for management of Office 365 there are some configuration controls that are recommended to increase the operational security of the privileged accounts used to administer the customers Office 365 tenant.

Control bring-your-own-device device access

The increase in bring-your-own-device (BYOD) and work-from-home policies and the growth of wireless connectivity in businesses mandates effective monitoring of who is connecting to the network. Conditional Access policies are used to control access to resources and support different bring your own and choose your own models. Examples of options are as follows:

- **Grant access to compliant devices**. Users can authenticate to services from devices enrolled into Microsoft Intune that have reported an up-to-date compliance status
- **Grant access to enlightened applications**. Users can authenticate to services from managed applications on unenrolled devices
    - This control is typically used when Intune App Protection Policies are in use – such policies constrain corporate data to the apps, e.g. copy and paste between Word and Outlook (with organisational credentials) but not between Outlook (personal credentials) and Basecamp

Controlling bring your own and choose your own is primarily the scope of the mobile application and mobile device service. Conditional Access is a part of this holistic approach and utilises compliance status or the protections afforded by Intune enlightened apps.

The CA policies applied or enforced within a given authentication are captured and detailed in Azure AD auditing and reporting, which allows for reporting on whom can access what.

Responsibility: *Shared*

The use of CA to control access to applications also includes access to the administration interfaces, UI and PowerShell, as well as the end user interfaces. In addition, the CA policy can be applied to specific Azure AD Roles, e.g. Global Administrator or Exchange Administrator

For example, a correctly configured CA policy would require a device to be compliant and the user performed MFA in order to access the Exchange Admin Portal or establish a PowerShell session remotely.

Use Multi-Factor Authentication (MFA)

It is important to remember to turn of legacy authentication when implementing MFA.

MFA adds an additional layer of protection to a strong password strategy by requiring users to acknowledge a phone call, text message, or an app notification on their smart phone after correctly entering their password. With MFA in place, Office 365 user accounts are still protected against unauthorized access even if a user's password is compromised. Accounts are protected because access is not granted to an account until after the additional challenge has been satisfied. A compromised or stolen password is not enough to access Office 365 services. Refer to Plan for multi-factor authentication for Office 365 Deployments and Set up multi-factor authentication for Office 365 users

In ADFS 2016, you have the ability use Azure MFA as primary authentication for passwordless authentication. This is a great tool to guard against password spray and password theft attacks: if there's no password, it can't be guessed. This works great for all types of devices with various form factors.

Additionally, you can now use password as the second factor only after your OTP has been validated with Azure MFA. Learn more about using password as the second factor here.

Using Role-Based Access control

Azure Active Directory account privileges are implemented using role-based access control (RBAC) by assigning users to roles providing strict control over which users can view and configure Office 365 services.

To be compliant with this principle, further configuration is required by the customer to define the precise RBAC model that is suitable for use in production. As such, these configurations will need to be a part of the customer's change management process.

Office 365 comes with a set of admin roles that you can assign to users in your organization. Each admin role maps to common business functions, and gives people in your organization permissions to do specific tasks in the Office 365 admin centre, for details of the roles refer to About Office 365 admin roles - Office 365

Turn off legacy Authentication Protocol support

Responsibility: *Shared*

The customer is responsible for restricting access to legacy clients that cannot support modern authentication and benefit from the Conditional Access (CA) approach, described previously. Legacy authentication protocols don't have the ability to enforce MFA, so the best approach is to block them from the extranet. This will prevent password spray attackers from exploiting the lack of MFA on those protocols

In the federated use case the simplest approach is to disable the username and password endpoint from being proxied to the Internet, however the CA approach is more flexible in that it blocks at token issuance thus supporting blocking clients from specific apps and services while still allowing and enabling others.

It is recommended that CA policies are used to block or deny access to legacy clients.

Enhanced Security and Compliance Package capability

The following are suggested controls that will enhance the secure administration of Azure AD and Office 365 but require additional components that are not included in Office 365 E3 subscription

The controls listed below are included in the Security and Compliance Package.

Azure AD Identity Protection

Azure AD Identity Protection is an algorithm-based monitoring and reporting tool that you can use to detect potential vulnerabilities affecting your organization's identities. You can configure automated responses to those detected suspicious activities and take appropriate action to resolve them. For more information, see Azure Active Directory Identity Protection.

Risk-based multi-factor authentication

Azure AD Identity Protection uses the sign-in data mentioned above and adds on advanced machine learning and algorithmic detection to risk score every sign-in that comes in to the system. This enables enterprise customers to create policies in Identity Protection that prompt a user to authenticate with a second factor if and only if there's risk detected for the user or for the session. This lessens the burden on your users and puts blocks in the way of the bad guys.

Later this year on-premises customers will be able to utilise banned passwords in hybrid Azure AD-Active Directory environments. Banned password lists will be synchronized from the cloud to your on-premises environments and enforced on every domain controller with the agent.

An additional enhancement to management interfaces would be to extend the use of MFA for other privileged users.

Azure AD Privileged Identity Management

Responsibility: *Shared*	
	Consider using Azure AD Privileged Identity Management (PIM) to enhance the security of administrator accounts organisations should. Rather than having any Global Administrator accounts be permanently assigned the global administrator role they become eligible administrators. The global administrator role is inactive until someone needs it. You then complete an activation process to add the global administrator role to the global administrator account for a predetermined amount of time. When the time expires, PIM removes the global administrator role from the global administrator account. Using PIM and this process significantly reduces the amount of time that your global administrator accounts are vulnerable to attack and use by malicious users. Whilst the guidance above focuses on accounts that are members of the Global Administrator role the same recommendations apply to an account that have wide-ranging permissions to access data or make configuration changes in Office 365, e.g. eDiscovery Administrator or security / compliance administrator accounts, should also be protected in the same manner. For more information, see Configure Azure AD Privileged Identity Management. When combining Azure AD with RBAC this allows management of the system without requiring standing GA privilege, For information about assigning admin roles and permissions, see Assigning admin roles in Office 365 and About Office 365 admin roles.
Provider	Microsoft has invested heavily and accordingly in systems and controls that automate most Office 365 operations while intentionally limiting Microsoft's access to customer content. Humans govern the service, and software operates the service. This enables Microsoft to manage Office 365 at scale, as well as manage the risks of internal threats to customer content such as malicious actors, the spear-phishing of a Microsoft engineer, and so forth. By default, Microsoft engineers have zero standing administrative privileges and zero standing access to customer content in Office 365. A Microsoft engineer can have limited, audited, and secured access to a customer's content for a limited amount of time, but only when necessary for service operations, and only when approved by a member of Microsoft senior management (and for customers that are licensed for the Customer Lockbox feature, the customer) In addition to the controls described above Microsoft advocates and highlights the need for preparing for the impact of current and future threats by simulating real-world attacks and exercising Tactics, Techniques and Procedures (TTPs) that determined and persistent adversaries use during breaches. Rather than simply adopting the traditional approach of preventing security incidents from occurring, Prevent Breach model, Microsoft assumes that it is a case of when and not if these breaches occur. This approach is Microsoft Assume Breach methodology. Assume

Responsibility: *Shared*

breach is a mindset that guides security investments, design decisions and operational security practices. A critical part of the Assume Breach mentality is that it limits the trust placed in applications, services, identities and networks by treating them all, internal and external, as insecure and already compromised.

Whilst Prevent Breach approaches such as Threat Modelling , code reviews and security testing are still useful as part of Microsoft Security Development Lifecycle, Assume Breach provides numerous advantages that help account for overall security by exercising and measuring reactive capabilities in the event of a breach.

At Microsoft, we set out to accomplish this through ongoing war-games exercises and live site penetration testing of our security response plans with the goal of improving our detection and response capability. Microsoft regularly simulates real-world breaches, conducts continuous security monitoring, and practices security incident management to validate and improve the security of Office 365, Azure, and other Microsoft cloud services.

Microsoft executes its Assume Breach security strategy using two core groups:

- Red Teams (attackers)
- Blue Teams (defenders)

Both Microsoft Azure and Office 365 staff operate full-time red teams and blue teams.

Referred to as "Red Teaming", the approach is to test Azure and Office 365 systems and operations using the same tactics, techniques and procedures as real adversaries, against the live production infrastructure, without the foreknowledge of the Engineering or Operations teams. This tests Microsoft's security detection and response capabilities, and helps identify production vulnerabilities, configuration errors, invalid assumptions, and other security issues in a controlled manner. Every red team breach is followed by full disclosure between both teams to identify gaps, address findings, and improve breach response. For more details on Microsoft Assume Breach and Red Teaming refer to Microsoft Enterprise Cloud Red Teaming

Microsoft publishes details of Pen Test and Security Assessments that are performed on its cloud services annually. The latest report can be found here, Office 365 End of Year Security Report and Pen Test Summary for 2017.

2.12 NCSC Cloud Security Principle 12: Secure Service Administration

Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. The design, implementation and management of administration systems should follow enterprise good practice, whilst recognising their high value to attackers

Responsibility: *Shared*

Customer

The integrity of the privileged accounts that are used to administer and manage Microsoft Office 365 is no less important than those used to administer traditional on-premises IT Systems. The security of most or all business intellectual property in a hybrid or cloud-based organization depends upon the integrity of these administrators.

Cyber-attackers focus on privileged access to infrastructure systems (such as Active Directory and Azure Active Directory) to gain access to an organization's sensitive data. For cloud services, prevention and response are the joint responsibilities of the cloud service provider and the customer.

Privileged administrative accounts are effectively in control of this new "security perimeter." It's critical to protect privileged access, regardless of whether the environment is on-premises, cloud, or hybrid on-premises and cloud hosted services. Protecting administrative access against determined adversaries requires you to take a complete and thoughtful approach to isolating your organization's systems from risks.

Securing privileged access requires changes to

- Processes, administrative practices, and knowledge management
- Technical components such as host defences, account protections, and identity management

Use Privileged Access Workstations to administer cloud services

The customer is responsible for ensuring a secure workstation for administration of their Azure AD and Office 365 tenant. Attackers may attempt to target privileged accounts to gain access to an organization's data and systems, so they can disrupt the integrity and authenticity of data, through malicious code that alters the program logic or snoops the admin entering a credential. Privileged Access Workstations (PAWs) provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-

Ticket. By deploying privileged access workstations, you can reduce the risk that admins enter admin credentials except on a desktop environment that has been hardened. For more information, see Privileged Access Workstations.

Securing the Global Admin accounts

By default, the first account that is used to create an Office 365 tenant is assigned the Global Administrator (GA) role, this, means that you have complete control over the Office 365 suite of products and the Azure AD associated with the Office 365 subscription. As such these accounts are extremely valuable to attackers and the following guidance should be followed to ensure that these accounts are secured appropriately.

All Office 365 Global Administrator accounts should be dedicated accounts that are used for this purpose only and not have mailboxes associated with them nor should they be used for general internet browsing.

The first control recommended for Global Administrator accounts is to ensure that there are no more than 5 members of Azure AD Admins group. This should be carried across to individual Office 365 services, e.g. Exchange Online and SharePoint Online.

The second control is to use Multi-factor authentication (MFA) for Global Administrator accounts. Enabling MFA for Global Administrators ensures that additional information beyond the account name and password is required before access to the administrative portal is granted. To enable MFA for Office 365 refer to the following article, Set up multi-factor authentication for Office 365 users. to configure each dedicated global administrator account for the appropriate verification method refer to the following article set up 2-step verification for Office 365.

Define at least two emergency access accounts

Ensure that you do not get into a situation where they could be inadvertently locked out of the administration of your Azure AD tenant due to an inability to sign in or activate an existing individual user's account as an administrator. For example, if the organization is federated to an on-premises identity provider, that identity provider may be unavailable, so users cannot sign in on-premises. You can mitigate the impact of accidental lack of administrative access by storing two or more emergency access accounts in your tenant.

Emergency access accounts help organizations restrict privileged access within an existing Azure Active Directory environment. These accounts are highly privileged and are not assigned to specific individuals. Emergency access accounts are limited to emergency for 'break glass' scenarios where normal administrative accounts cannot be used. Organizations must ensure the aim of controlling and reducing the emergency account's usage to only that time for which it is necessary.

Responsibility: *Shared*

Evaluate the accounts that are assigned or eligible for the global admin role. If you did not see any cloud-only accounts using the *.onmicrosoft.com domain (intended for "break glass" emergency access), create them. For more information, see Managing emergency access administrative accounts in Azure AD.

Conduct an inventory of services, owners, and admins

With the increase in bring-your-own-device (BYOD) and work-from-home policies and the growth of wireless connectivity in businesses, it is critical that you monitor who is connecting to your network. This is especially important for privileged accounts that are used to manage the Office 365 tenancy. An effective security audit often reveals devices, applications, and programs running on your network that are not supported by IT, and therefore potentially not secure. For more information, see Azure security management and monitoring overview. Ensure that you include all the following tasks in your inventory process.

- Identify the users who have administrative roles and the services where they can manage.
- Use Azure AD PIM to find out which users in your organization have admin access to Azure AD.
- Beyond the roles defined in Azure AD, Office 365 comes with a set of admin roles that you can assign to users in your organization. Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the Office 365 admin centre. Use the Office Admin Center to find out which users in your organization have admin access to Office 365, including via roles not managed in Azure AD. For more information, see About Office 365 admin roles and Security best practices for Office 365.
- Perform the inventory in other services your organization relies on, such as Azure, Intune, or Dynamics 365.
- Ensure that your admin accounts (accounts that are used for administration purposes, not just users' day-to-day accounts) have working email addresses attached to them and have registered for Azure MFA.
- Ask users for their business justification for administrative access.
- Remove admin access for those individuals and services that don't need it.

Use Conditional access to control ability to connect to Azure and Office portals

Access to the Azure AD blade in Azure portal and Microsoft Office 365 Admin portals should be restricted to authorized administrators only. Whilst this can be achieved in a basic manner by ensuring that administrative users have a dedicated account that has MFA enabled Conditional Access provides additional access control decisions to determine whether a user is able to access the resource requested or not.

Responsibility: *Shared*

Typically, conditional access is used to control access to cloud apps. However, it is also possible to set up policies to control access to Azure management based on certain conditions (such as sign-in risk, location, or device) and to enforce requirements like multi-factor authentication.

To create a policy for Azure management, you select **Microsoft Azure Management** under **Cloud apps** when choosing the app to which to apply the policy.

Refer to Conditional Access in Azure Active Directory for more details on the capabilities of Conditional Access.

One of the apps that can be gated as part of the Conditional Access decision process is the Azure Admin Portal.

Turn off legacy Authentication Protocol support

The customer is responsible for restricting access to legacy clients that cannot support modern authentication and benefit from the Conditional Access (CA) approach, described previously. Legacy authentication protocols don't have the ability to enforce MFA, so the best approach is to block them from the extranet. This will prevent password spray attackers from exploiting the lack of MFA on those protocols

In the federated use case the simplest approach is to disable the username and password endpoint from being proxied to the Internet, however the CA approach is more flexible in that it blocks at token issuance thus supporting blocking clients from specific apps and services while still allowing and enabling others.

It is recommended that CA policies are used to block or deny access to legacy clients.

Enhanced Security and Compliance Package capability

The following are suggested controls that will enhance the secure administration of Azure AD and Office 365 but require additional components that are not included in Office 365 E3 subscription

The following are suggested controls that will enhance the secure administration of Azure AD and Office 365 but require additional components that are not included in Office 365 E3 subscription

> IMPORTANT:
>
> The additional controls described below are available as part of the Security and Compliance Package

Azure AD Privileged Identity Management

To further enhance the security of Global Administrator accounts organisations should consider using Azure AD Privileged Identity Management (PIM).

Responsibility: *Shared*

Rather than having any Global Administrator accounts be permanently assigned the global administrator role they become eligible administrators. The global administrator role is inactive until someone needs it. You then complete an activation process to add the global administrator role to the global administrator account for a predetermined amount of time. When the time expires, PIM removes the global administrator role from the global administrator account.

Using PIM and this process significantly reduces the amount of time that your global administrator accounts are vulnerable to attack and use by malicious users.

Whilst the guidance above focuses on accounts that are members of the Global Administrator role the same recommendations apply to an account that have wide-ranging permissions to access data or make configuration changes in Office 365, e.g. eDiscovery Administrator or security / compliance administrator accounts, should also be protected in the same manner.

For more information, see Configure Azure AD Privileged Identity Management.

Using Role-Based Access control

Azure Active Directory account privileges are implemented using role-based access control (RBAC) by assigning users to roles providing strict control over which users can view and configure Office 365 services.

To be compliant with this principle, further configuration is required by the customer to define the precise RBAC model that is suitable for use in production. As such, these configurations will need to be a part of the customer's change management process.

Office 365 comes with a set of admin roles that you can assign to users in your organization. Each admin role maps to common business functions, and gives people in your organization permissions to do specific tasks in the Office 365 admin centre, for details of the roles refer to About Office 365 admin roles - Office 365

Azure AD Identity Protection

Azure AD Identity Protection is an algorithm-based monitoring and reporting tool that you can use to detect potential vulnerabilities affecting your organization’s identities. You can configure automated responses to those detected suspicious activities and take appropriate action to resolve them. For more information, see Azure Active Directory Identity Protection.

Risk-based multi-factor authentication

Azure AD Identity Protection uses the sign-in data mentioned above and adds on advanced machine learning and algorithmic detection to risk score every sign-in that comes in to the system. This enables enterprise customers to create policies in Identity Protection that prompt a user to authenticate with a second factor if and only

Responsibility: *Shared*

if there’s risk detected for the user or for the session. This lessens the burden on your users and puts blocks in the way of the bad guys.

Later this year on-premises customers will be able to utilise banned passwords in hybrid Azure AD-Active Directory environments. Banned password lists will be synchronized from the cloud to your on-premises environments and enforced on every domain controller with the agent.

Provider

Microsoft has invested heavily and accordingly in systems and controls that automate most Office 365 operations while intentionally limiting Microsoft’s access to customer content. Humans govern the service, and software operates the service. This enables Microsoft to manage Office 365 at scale, as well as manage the risks of internal threats to customer content such as malicious actors, the spear-phishing of a Microsoft engineer, and so forth.

By default, Microsoft engineers have zero standing administrative privileges and zero standing access to customer content in Office 365. A Microsoft engineer can have limited, audited, and secured access to a customer’s content for a limited amount of time, but only when necessary for service operations, and only when approved by a member of Microsoft senior management (and for customers that are licensed for the Customer Lockbox feature, the customer)

Microsoft has established access control mechanisms to ensure that no one has unapproved access to Customer Data or access control data[5] or unapproved physical, logical, or remote access to the Office 365 production environment.

The access controls used by Microsoft for operating Office 365 can be grouped into three categories:

1. Isolation Controls
2. Personnel Controls
3. Technology Controls

Further Reading

For more information on the controls used for administrative access in Office 365, see Office 365 Administrative Access Controls.

[5] Used to manage access to other types of data or functions within the environment, including access to customer content or EUII. It includes Microsoft passwords, security certificates, and other authentication-related data.

2.13 NCSC Cloud Security Principle 13: Audit Information for Users

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales

Responsibility: *Shared*

Customer Microsoft Office 365 includes several auditing and reporting features that customers should use to track user and administrative activity within an Office 365 tenant. The audit settings allow changes made to Exchange Online and SharePoint Online tenant configuration settings, and changes made by users to documents and other items. Customers should use the audit information and reports available in Office 365 Security & Compliance Center to more effectively manage the user experience, mitigate risk, and fulfil compliance obligations.

Using an Office 365 admin account the Security & Compliance Center is located at http://protection.office.com .

The Security & Compliance Center includes navigation panes that provide access to several features:

- **Permissions** Enables organisations to assign permissions such as Compliance Administrator, eDiscovery Manager, and others to people in the organization so that they can perform tasks in the Security & Compliance Center. Most features can be assigned in the Security & Compliance Center, but other permissions must be configured using the Exchange admin centre and SharePoint admin centre.
- **Security policies** Enables ability to create and apply device management policies using Office 365 Mobile Device Management and to set up Data Loss Prevention (DLP) policies in tenant.
- **Data management** Enables ability to import email or SharePoint data from other systems into Office 365, configure archive mailboxes, and set retention policies for email and other content in tenant.
- **Search & investigation** Provides content search, audit log and eDiscovery case management tools to quickly drill into activity across Exchange Online mailboxes, groups and public folders, SharePoint Online, and OneDrive for Business.
- **Reports** Enables ability to quickly access reports for SharePoint Online, OneDrive for Business, Exchange Online, and Azure AD.
- **Service assurance** Provides information about how Microsoft maintains security, privacy, and compliance with global standards for Office 365, Azure, Microsoft Dynamics CRM Online, Microsoft Intune, and other cloud services. Also includes access to third-party ISO, SOC, and other audit reports, as well

as Audited Controls, which provides details about the various controls that have been tested and verified by third-party auditors of Office 365.

Enable Mailbox Auditing

Enable mailbox auditing for all users that have mailboxes in your tenancy. By default, all non-owner access is audited, but you must enable auditing on the mailbox for owner access to also be audited. This will allow you to discover illicit access of Exchange Online activity if a user's account has been breached

Provider

In addition to the events and log data described above that is available for customers, there is also an internal log data collection system that is available to Office 365 engineers. Several types of log data are uploaded from Office 365 servers to an internal, big data computing service called Cosmos. Each service team uploads audit logs from their respective servers into the Cosmos database for aggregation and analysis.

Service teams use Cosmos as a centralized repository to conduct an analysis of application usage, to measure system and operational performance, and to look for abnormalities and patterns that may indicate problems or security issues. Each service team uploads a baseline of logs into Cosmos, depending on what they are looking to analyse, that often include:

- Event logs
- AppLocker logs
- Performance data
- System Center data
- Call detail records
- Quality of experience data
- IIS Web Server logs
- SQL Server logs
- Syslog data
- Security audit logs

Prior to uploading data into Cosmos, the ODL application uses a scrubbing service to obfuscate any fields that contain customer data, such as tenant information and end-user identifiable information, and replace those fields with a hash value. The anonymized and hashed logs are rewritten and then uploaded into Cosmos. Service teams run scoped queries against their data in Cosmos for correlation, alerting, and reporting. The period of audit log data retention in Cosmos is determined by the service teams; most audit log data is retained for 90 days or longer to support security incident investigations and to meet regulatory retention requirements.

This data transfer occurs over a FIPS 140-2-validated TLS connection on specifically approved ports and protocols using a proprietary automation tool called the Office Data Loader (ODL).

Further Reading

For more information on auditing and reporting in Office 365, see Auditing and Reporting in Office 365

2.14 NCSC Cloud Security Principle 14: Secure Use of the Service

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected. The extent of your responsibility will vary depending on the deployment models of the cloud service, and the scenario in which you intend to use the service. Specific features of individual services may also have bearing. For example, how a content delivery network protects your private key, or how a cloud payment provider detects fraudulent transactions, are important security considerations over and above the general considerations covered by the cloud security principles.

With IaaS and PaaS offerings, you are responsible for significant aspects of the security of your data and workloads. For example, if you procure an IaaS compute instance, you will normally be responsible for installing a modern operating system, configuring that operating system securely, securely deploying any applications and maintaining that instance through applying patches or performing maintenance required

Responsibility: *Customer*	
Customer	The customer is responsible for securing access to its Office 365 tenant both for normal users access the services as well as for Administrative tasks. Ensure security updates are applied for Operating System, https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb and Office ProPlus The single most important change that organisations can make to securing use of Office 365 is to move away from using username and password to access the services. Without a password, a password can't be guessed. That said unfortunately passwords are still a thing and as such the passwords that users have need to be made harder to guess. It is often difficult for users to know how to create suitable passwords and this is often compounded by password policies that force complexity and even worse users to change passwords regularly, the chances are that the new password will be similar to the old one. Refer to The problems with forcing regular password expiry for more details. Azure AD includes a banned password checker that when a password change is submitted it is fuzzy-matched against a list of words that are known weak passwords,

e.g. L3tMe1N!, or from known compromised passwords. This the password matches, it is rejected, and the user is asked to choose a different password. The list of passwords is updated frequently.

Later this year Microsoft will extend this functionality to on-premises Domain Controllers in hybrid Azure AD – Active Directory Domain Services (AD DS) environments. The banned password list will be synchronised from Azure AD to your on-premises Domain Controllers with an agent. This will help raise the quality of passwords used in environments where user's identities are anchored to AD DS.

Update password policy to reflect latest guidance

A lot of common conceptions about what makes a good password are wrong. Usually something that should help mathematically actually results in predictable user behaviour: for example, requiring certain character types and periodic password changes both result in specific password patterns. Refer to NCSC's guidance on passwords, Password Guidance: Simplifying Your Approach which is part of NCSC's broader guidance on passwords. Download the NCSC Infographic on Passwords here.

Reduce the use of passwords

Whilst raising the bar through helping users create passwords that are less easy to guess the aim is to reduce the use of password and eventually eliminate them altogether.

The approaches described below illustrate how non-password-based authentication methods can be used to access Office 365 services. The solutions are available for environments that are configured using the Federated model where ADFS and the Web Application Proxy are used:

- Certificate based authentication allows username/password endpoints to be blocked completely at the firewall. Learn more about certificate based authentication in ADFS
- Azure MFA, as mentioned above, can be used to as a second factor in cloud authentication and ADFS 2012 R2 and 2016. But, it also can be used as a primary factor in ADFS 2016 to completely stop the possibility of password spray. Learn how to configure Azure MFA with ADFS here
- Windows Hello for Business, available in Windows 10 and supported by ADFS in Windows Server 2016, enables completely password-free access, including from the extranet, based on strong cryptographic keys tied to both the user and the device.
  This is also available for corporate-managed devices that are Azure AD joined or Hybrid Azure AD joined as well as personal devices via "Add Work or School Account" from the Settings app.

Responsibility: *Customer*

Windows Hello for business

Windows Hello for Business (WHfB) is a Windows 10 feature that replaces passwords with strong two-factor authentication on PCs.

Windows Hello addresses the following problems with passwords:

- Strong passwords can be difficult to remember, and users often reuse passwords on multiple sites.
- Server breaches can expose symmetric network credentials (passwords).
- Passwords are subject to replay attacks.
- Users can inadvertently expose their passwords due to phishing attacks.

Windows Hello lets users authenticate to:

- a Microsoft account.
- an Active Directory account.
- a Microsoft Azure Active Directory (Azure AD) account.
- Identity Provider Services or Relying Party Services that support Fast ID Online (FIDO) v2.0 authentication (in progress)

After an initial two-step verification of the user during enrolment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify her or his identity. Windows then uses Windows Hello to authenticate users

PIN is tied to the device

One crucial difference between a password and a Hello PIN is that the PIN is tied to the specific device on which it was set up. That PIN is useless to anyone without that specific hardware. Someone who steals your password can sign in to your account from anywhere, but if they steal your PIN, they'd have to steal your physical device too!

Even you can't use that PIN anywhere except on that specific device. If you want to sign in on multiple devices, you must set up Hello on each device.

PIN is local to the device

A password is transmitted to the server -- it can be intercepted in transmission or stolen from a server. A PIN is local to the device -- it isn't transmitted anywhere, and it isn't stored on the server. When the PIN is created, it establishes a trusted relationship with the identity provider and creates an asymmetric key pair that is used for authentication. When you enter your PIN, it unlocks the authentication key and uses the key to sign the request that is sent to the authenticating server.

PIN is backed by hardware

The Hello PIN is backed by a Trusted Platform Module (TPM) chip, which is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper resistant, and malicious software is unable to tamper with the security functions of the TPM. All Windows 10 Mobile phones and many modern laptops have TPM. User key material is generated and available within the Trusted Platform Module (TPM) of the user device, which protects it from attackers who want to capture the key material and reuse it. Because Hello uses asymmetrical key pairs, user's credentials can't be stolen in cases where the identity provider or websites the user accesses have been compromised.

The TPM protects against a variety of known and potential attacks, including PIN brute-force attacks. After too many incorrect guesses, the device is locked.

Use Multi-Factor Authentication (MFA)

It is important to remember to turn of legacy authentication when implementing MFA.

MFA adds an additional layer of protection to a strong password strategy by requiring users to acknowledge a phone call, text message, or an app notification on their smart phone after correctly entering their password. With MFA in place, Office 365 user accounts are still protected against unauthorized access even if a user's password is compromised. Accounts are protected because access is not granted to an account until after the additional challenge has been satisfied. A compromised or stolen password is not enough to access Office 365 services. Refer to Plan for multi-factor authentication for Office 365 Deployments and Set up multi-factor authentication for Office 365 users

In ADFS 2016, you have the ability use Azure MFA as primary authentication for passwordless authentication. This is a great tool to guard against password spray and password theft attacks: if there's no password, it can't be guessed. This works great for all types of devices with various form factors.

Additionally, you can now use password as the second factor only after your OTP has been validated with Azure MFA. Learn more about using password as the second factor here.

Use Certificate-based authentication from mobile devices

Certificate-based authentication enables you to be authenticated by Azure Active Directory with a client certificate on a Windows, Android or iOS device when connecting your Exchange online account to:

- Microsoft mobile applications such as Microsoft Outlook and Microsoft Word
- Exchange ActiveSync (EAS) clients

Configuring this feature eliminates the need to enter a username and password combination into certain mail and Microsoft Office applications on your mobile device.

Responsibility: *Customer*

For more information on configuring certificate-based authentication refer to:

- Azure Active Directory certificate-based authentication on iOS https://docs.microsoft.com/en-us/azure/active-directory/active-directory-certificate-based-authentication-ios
- Azure Active Directory certificate-based authentication on Android https://docs.microsoft.com/en-us/azure/active-directory/active-directory-certificate-based-authentication-android

Turn off legacy Authentication Protocol support

The customer is responsible for restricting access to legacy clients that cannot support modern authentication and benefit from the Conditional Access (CA) approach, described previously. Legacy authentication protocols don’t have the ability to enforce MFA, so the best approach is to block them from the extranet. This will prevent password spray attackers from exploiting the lack of MFA on those protocols

In the federated use case the simplest approach is to disable the username and password endpoint from being proxied to the Internet, however the CA approach is more flexible in that it blocks at token issuance thus supporting blocking clients from specific apps and services while still allowing and enabling others.

It is recommended that CA policies are used to block or deny access to legacy clients.

Enable ADFS Web Application Proxy Extranet Lockout

With this feature, AD FS will "stop" authenticating the "malicious" user account from outside for a period. This prevents your user accounts from being locked out in Active Directory. In addition to protecting your users from an AD account lockout, AD FS extranet lockout also protects against brute force password guessing attacks.

Extranet lockout provides the following key advantages:

- It protects your user accounts from **brute force attacks** where an attacker tries to guess a user's password by continuously sending authentication requests. In this case, AD FS will lock out the malicious user account for extranet access
- It protects your user accounts from **malicious account lockout** where an attacker wants to lock out a user account by sending authentication requests with wrong passwords. In this case, although the user account will be locked out by AD FS for extranet access, the actual user account in AD is not locked out and the user can still access corporate resources within the organization. This is known as a **soft lockout**.

Responsibility: *Customer*

If you do not have extranet lockout in place at the ADFS Web Application proxy, you should enable it as soon as possible to protect your users from potential password brute force compromise.

Enhanced Security and Compliance Package capability

The following are suggested controls that will enhance the secure administration of Azure AD and Office 365 but require additional components that are not included in Office 365 E3 subscription

> INFORMATION:
>
> The additional controls described below are available as part of the Security and Compliance Package

Risk-based multi-factor authentication

For the best experience for users, it is recommended that risk-based multi-factor authentication is used, which is available with Azure AD Premium P2 licenses included in the Security and Compliance Package.

Azure AD Identity Protection uses the sign-in data mentioned above and adds on advanced machine learning and algorithmic detection to risk score every sign-in that comes in to the system. This enables enterprise customers to create policies in Identity Protection that prompt a user to authenticate with a second factor if and only if there’s risk detected for the user or for the session. This lessens the burden on your users and puts blocks in the way of the bad guys. Learn more about Azure AD Identity Protection here

Azure Identity Protection

Most of security breaches take place when attackers gain access to an environment by stealing a user’s identity. Attackers have become increasingly effective in leveraging third party breaches and using sophisticated phishing attacks. As soon as an attacker gains access to even low privileged user accounts, it is relatively easy for them to gain access to important company resources through lateral movement.

Because of this, you need to:

- Protect all identities regardless of their privilege level
- Proactively prevent compromised identities from being abused

Discovering compromised identities is no easy task. Azure Active Directory uses adaptive machine learning algorithms and heuristics to detect anomalies and suspicious incidents that indicate potentially compromised identities. Using this data, Identity Protection generates reports and alerts that enable you to evaluate the detected issues and take appropriate mitigation or remediation actions.

Responsibility: *Customer*

Azure Active Directory Identity Protection is more than a monitoring and reporting tool. To protect your organization's identities, you can configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached. These policies, in addition to other conditional access controls provided by Azure AD and Enterprise Management and Security (EMS), can either automatically block or initiate adaptive remediation actions including password resets and multi-factor authentication enforcement.

Identity Protection capabilities

Detecting vulnerabilities and risky accounts:

- Providing custom recommendations to improve overall security posture by highlighting vulnerabilities
- Calculating sign-in risk levels
- Calculating user risk levels

Investigating risk events:

- Sending notifications for risk events
- Investigating risk events using relevant and contextual information
- Providing basic workflows to track investigations
- Providing easy access to remediation actions such as password reset

Risk-based conditional access policies:

- Policy to mitigate risky sign-ins by blocking sign-ins or requiring multi-factor authentication challenges
- Policy to block or secure risky user accounts
- Policy to require users to register for multi-factor authentication

> NOTE:
>
> It is recommended that risk-based multi-factor authentication is used to provide the best experience for users.

Review Secure Score

Secure Score analyses your Office 365 organization's security based on your regular activities and security settings and assigns a score, access the Secure Score at https://securescore.office.com.

Provider

By default, Microsoft engineers have zero standing administrative privileges and zero standing access to customer content in Office 365. A Microsoft engineer can have limited, audited, and secured access to a customer's content for a limited amount of time, but only when necessary for service operations, and only when approved by a member of Microsoft senior management (and for customers that are licensed for the Customer Lockbox feature, the customer).