Risk Environment for G-Cloud 6

Reference:	Reference / Version Number 2.0
Date:	16th April 2015
Author:	Richard Ellis, CLAS Consultant
Service Owner:	Greg Roberts / Director, Office 365 Governance, Risk and Compliance

1. Introduction

The intention of this document is to provide potential G-Cloud users of Microsoft's Office 365 service with an overview of the risk environment. It aims to provide the same level of information as contained in the Risk Management and Accreditation Document Set (RMADS) for previous iterations of G-Cloud accreditation and similarly relies on the ISO 27001 certification for the Office 365 service.

A statement of compliance against CESG's Cloud Security Principles is included in Appendix C.

1.1. Limitations

This report is based on documentation supplied by Microsoft and discussions with staff. Every effort has been made to ensure that all statements and information contained herein are accurate; however, the work completed did not constitute an audit and the controls were not tested to ensure they are working as stated.

2. ISO/IEC 27001:2013 Certification Status

The Office 365 service has been certified to ISO 27001:2013 by BSI, a UKAS recognised authority. Office 365 depends on Microsoft's Cloud Infrastructure and Operations (MCIO)[1] data centres for physical security, environmental services and power and network cabling. MCIO is included within the scope of this document and has separate ISO 27001 certification. Both Office 365 and MCIO have also been accredited by the Pan Government Accreditor (PGA) for previous versions of G-Cloud.

In addition to ISO 27001, Office 365 has achieved compliance with the ISO 27018 standard – the Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Compliance with this standard has been verified by BSI.

2.1. Scope

The ISO/IEC 27001 Certificates for the MCIO and Office 365 can be verified using the links in Appendix A of this document. The scope of the certifications are as follows:

Office 365:

"*The management of Information Security Management System (ISMS) for Microsoft Office 365 Services development, operations and support in accordance with Office 365 ISMS Statement of Applicability dated November 16, 2012*."

GFS:

"The management of information security for Microsoft Global Foundation Services Infrastructure encompassing data centers listed in this report and specific teams comprised of Online Services Security and Compliance, Data Center Services, Global Networking Services, Data Center Software Services, OpsCenter Service Desk, Operations Systems Support Group, and Asset Management and Deployment, in accordance with Microsoft GFS ISMS Statement of Applicability version 2013.01 dated 2/20/2014."

The following diagram depicts the service using the modelling techniques described in HMG's Information Assurance Standard No. 1 (IS1):

[1] MCIO was formerly known as Global Foundation Service (GFS) which is the name referred to in the ISO documentation. Throughout this document, the names MCIO and GFS should be considered synonymous.

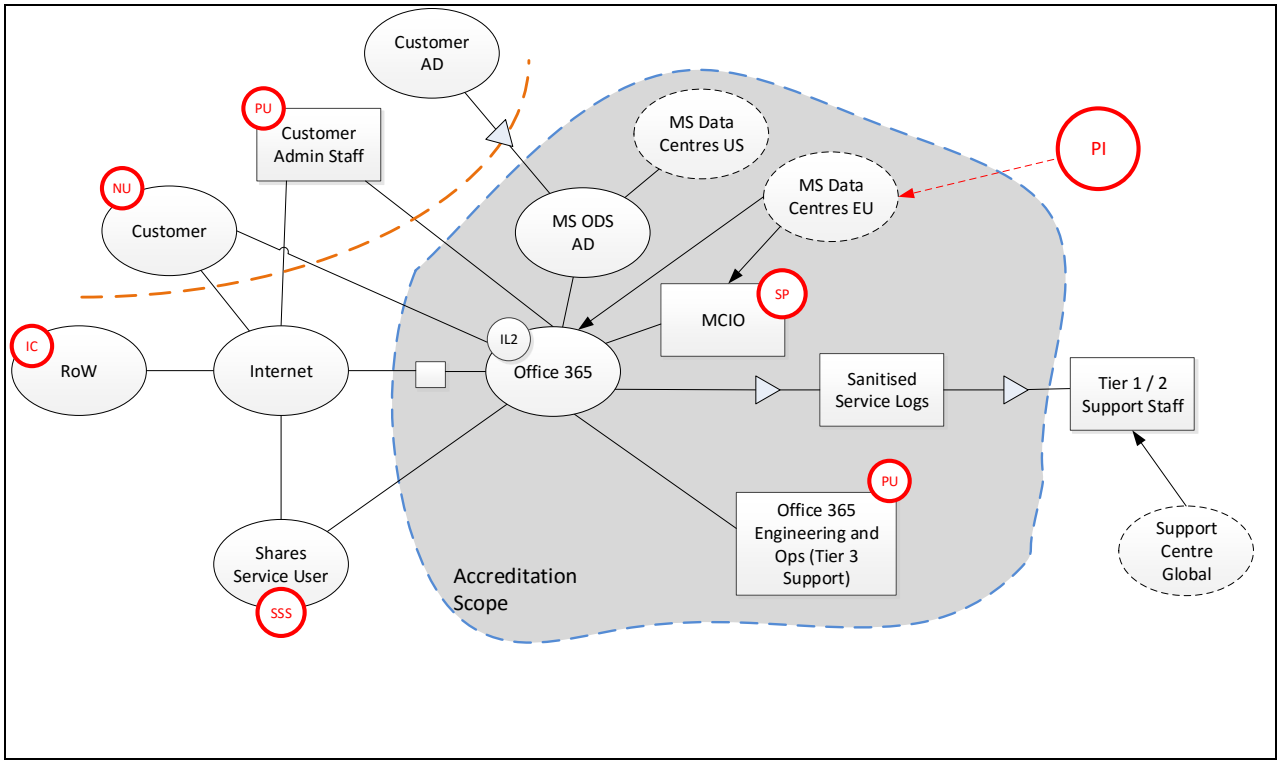

Figure 1: Model Diagram

Note: Microsoft Office 365 utilises Tier 1 and 2 support functions already utilised by UK Government for on premises software support, as they do not have access to customer data within the service they are excluded from the scope of accreditation.

2.2. ISO 27001 Statement of Applicability

The latest Office 365 Statement of Applicability (SOA)[2] states that all the ISO 27002 security controls are considered applicable to the service. Some of the controls are dependent on MCIO as described above. Other controls rely on the various corporate departments outside the Office 365 organisation: HR, Legal and Corporate Affairs (LCA) and the Risk Management Office (RMO). These controls, together with those for MCIO are included in the Office 365 SOA and have been sampled in the latest ISO 27001 Continuous Assessment Audit carried out during November 2014.

The latest audit concluded that the areas assessed were effective, that there were no outstanding nonconformities to review and no new nonconformities were identified. In summary, the Office 365 service is compliant with all the controls in the ISO/IEC 27001 standard. See Appendix B for the full Statement of Applicability.

[2] The SOA used in the latest Continual Assessment Audit carried out by BSI is dated October 2014. It has been updated to conform with the latest version of the ISO 27001 standard and differs to that listed on th certificate.

3. Basic Information

3.1. Description of Service

Microsoft Office 365 is a cloud based solution that provides access to Microsoft collaboration technologies (Exchange, SharePoint, Lync/Skype for Business[3] and Microsoft Office) through an internet based service. This service is hosted in Microsoft data centres in Dublin and Amsterdam for UK Government customers and guarantees a 99.9% uptime. Office 365 has several service plans that offer different levels of service provision depending on subscription level.

3.1.1. Hardware

Microsoft uses a range of industry standard hardware to provide its Office 365 services.

3.1.2. Software

The service includes the following Microsoft applications/suites:

- Microsoft Office Professional Plus with the ability to access documents and email stored in the Office 365 cloud. It includes Office Web Apps which allows users to view and edit documents through a web-browser interface;
- Exchange Online with built in antivirus and anti-spam filters;
- SharePoint Online provides a central resource where documents and information can be shared between teams or organisations;
- Skype for Business[3] messaging tool.
- The underlying operating system is Windows Server.

3.1.3. Communications

Office 365 is accessed using the public Internet as the transport mechanism from the customer site to the Microsoft data centre. A number of network and encryption protocols are used depending on the service being accessed. The following diagram shows the data flows and protocols used; further details are included in the subsequent table (the figure also shows the federation trust required for single sign-on):

[3] Lync Online has been rebranded to Skype for Business, updates to branding are currently inflight

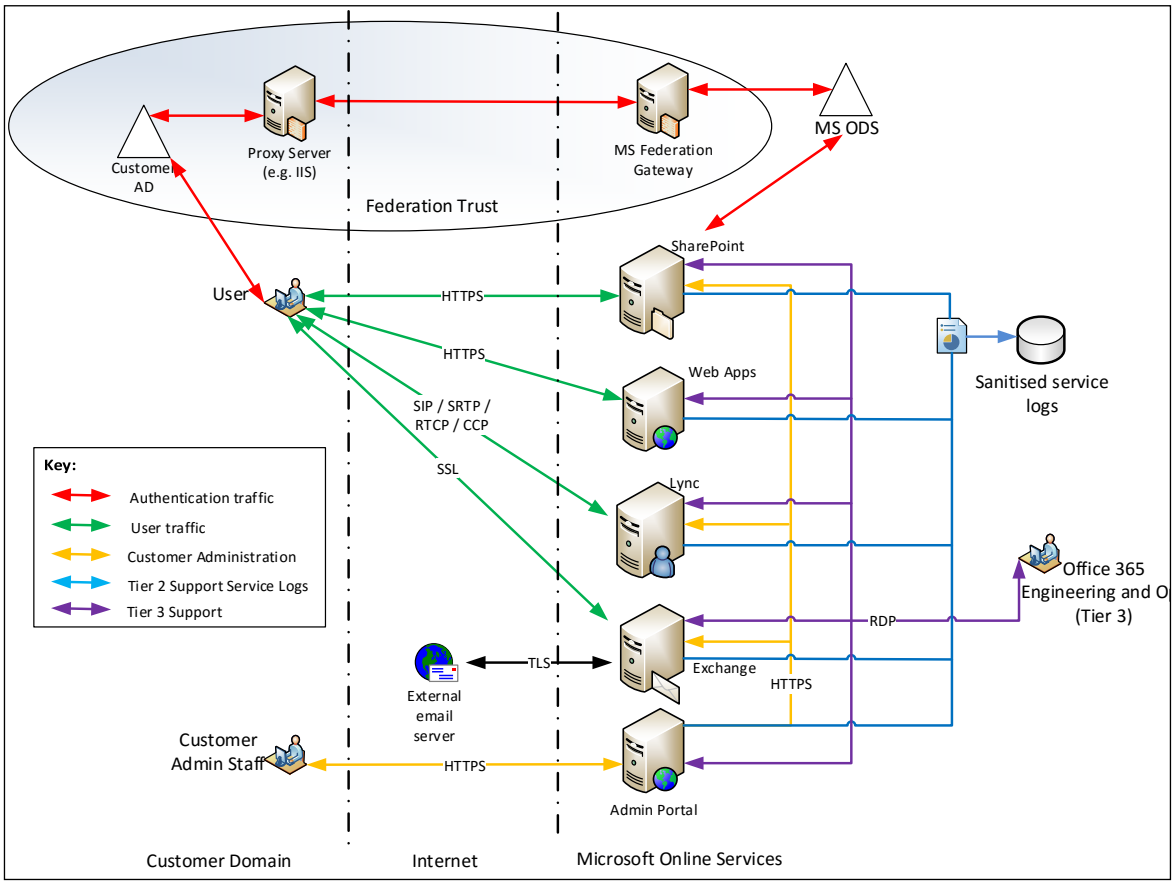

Figure 2: Data flows and federation trust

Communication	Protocol	Comments
Email: client to Exchange Online	SSL/TLS[4]	TLS is used for encrypting Outlook, Outlook Web App, Exchange ActiveSync, and Exchange Web Services traffic, using TCP port 443. SSL is also used for POP3 and IMAP, using TCP port 995.
Email: Exchange Online to external server	TLS	Exchange Online supports opportunistic TLS for inbound and outbound email, and this feature is enabled by default. It also supports forced TLS for both inbound and outbound connections but enabling this may cause connectivity issues.
Client to SharePoint online	HTTPS	User access to the customer's SharePoint web site hosted on Office 365.

[4] SSL 3.0 is currently being disabled in response to Poodle

Communication	Protocol	Comments
Web Apps	HTTPS	The Web Apps allow documents on SharePoint to be edited in a web browser window.
Lync	SIP/SRTP/ RTCP/CCP	Lync provides instant messaging, audio / video calling with audio, video and web conferencing.
Azure Active Directory Sync Tool (formally DirSync)	TLS	Azure Active Directory Sync Tool is used to synchronise the on-premises Active Directory (AD) contents with the Microsoft Online AD. It uploads the AD objects and then synchronises any updates to the customer's AD. Together with ADFS, DirSync provides single-sign on for Office 365.
Active Directory Federation Service (ADFS)	HTTPS	ADFS federates with the Office 365 services federation gateway. This provides single sign-on allowing users whose identities are based in the federated domain to use their existing corporate logon information to automatically authenticate to Office 365.
Microsoft Support	RDP	Microsoft Tier 3 support use the remote desktop protocol to access the Office 365 servers.
Data centre to data centre	TLS/IPSec	All communication between data centres take place over Microsoft internal private networks encryption is used as appropriate to the data classification

Table 1: Communications

3.1.4. People

The following table lists the user groups that will interact with the Office 365 service:

User group	Role	Organisation	Background checks
Customer staff	Customer employees who are authorised users of the customer's Office 365 environment.	Customer	Customer responsibility.

User group	Role	Organisation	Background checks
Customer admin	Customer employees who have administrative access to the customer's Office 365 environment. (See **Error! Reference source not found.** below for further information.)	Customer	Customer responsibility.
Tier 1 / 2 support	Tier 1/2 support staff who have access to sanitised service logs only (see 3.3 for more detailed information).	Microsoft	None.
Office 365 Engineering and operations Tier 3 support	Support staff who may have access to customer authored data. Such staff require a Microsoft issued smartcard with a valid certificate and a valid domain account in order to establish a remote access session.	Microsoft	Yes (See 4.3 below for details).
Data centre staff	Data centre staff may have authorised physical access to hardware but no logical access at the operating system or application level.	Microsoft	None.
Shared service subscriber	Organisations with authorised access to their own instance of Office 365 but no authorised access to that of the customer. Users may include Office 365 administrators as above.	Unknown.	Unknown.
Internet user	Members of the public with an indirect connection to the service via the Internet.	None.	None.

Table 2: User groups

3.1.5. Locations

The following table lists the locations that are relevant to the Office 365 service. For further details regarding off-shoring see section 3.3 below

Place	Geographic location	Comments
Customer premises	Customer specific	Locations from which customer staff access the Office 365 service.

Place	Geographic location	Comments
EU data centres	Ireland Netherlands Finland Austria	Data centres from which the Office 365 service for UK Government customers is hosted and where data will be located. Data stored in Exchange will be stored in Ireland, Netherlands, Finland and Austria. Data stored in SharePoint may be located in either the Dublin or Amsterdam data centres which provide backup for each other.
US data centre	United States	The Active Directory data is stored in both the Dublin and US data centres. Customer contact data for billing, support, escalation etc. is held in the US.
Tier 1/2 support centres	Worldwide	Support centres from which first and second line support staff operate. Sanitised service logs may be held in these locations (see below).
US support centre	United States	Support centre in the US where third line support staff are located who may have access to customer authored data.

Table 3: Locations

3.2. Dependencies and Interconnecting Services

The Office 365 service is supplied by Microsoft Ireland, managed and operated by Microsoft Corporation. The data centres hosting the service are operated by Microsoft's Cloud Infrastructure and Operations (MCIO) which is a wholly owned division of Microsoft. In addition to the physical data centres MCIO provide the network, hardware, power and environmental controls.

The service is accessed from the customer's premises via the public Internet.

To provide single-sign-on functionality, the customer's AD is synchronised with Microsoft's Azure Active Directory Service (previously called MSODS) using the DirSync software which, after the initial upload, will subsequently synchronise any updates made in the customer domain. To achieve automatic authentication of the users when they access an Office 365 service, the customer must enable the ADFS service to federate the two domains. The customer must set up an explicit federation trust with Microsoft's federation gateway and publish the edge of the ADFS via a proxy server.

Dial-in audio conferencing is the ability to dial into a scheduled Lync meeting/conference from fixed-line or mobile phones. This capability is not provided natively in Lync Online, but can be achieved through interoperability with leading third-party audio conferencing services. Customers wishing to use this functionality will need to purchase a separate audio conferencing service from a compatible supplier.

3.3. Third Party Arrangements and Off-Shoring

The Office 365 service for UK Government clients will be hosted in Microsoft's EU data centres in Ireland, Finland, Austria and Netherlands. Data centre staff have physical access to the servers hosting Office 365 but no logical access to the operating system or data.

Active Directory data is stored in Ireland, Netherlands and the United States.

Microsoft is a member of the U.S. Safe Harbour program as agreed by the EU and the US Department of Commerce. This requires Microsoft to comply with the EU Data Protection Directive and allows it to transfer data outside of the EU to the US in order to provide Microsoft Online Services. Microsoft is also willing to sign the standard contractual clauses created by the European Union (called the "EU Model Clauses") with all customers. EU Model Clauses address international transfer of data to areas outside the EU.

Office 365 has been designed to use service logs, rather than direct access to customer data, for purposes of providing, maintaining, and troubleshooting the online services. Service logs record errors and performance issues, and may contain limited customer data such as email addresses, subject lines of emails, file names, and site URLs to identify the source of the error or performance issue being recorded. Service logs do not contain customer-authored data such as customer documents, email message bodies or attachments, website content, or IM/voice conversations. Service logs that contain customer data are stored in the datacenters identified above. Occasionally, access is required from another location to address a specific service issue. Microsoft personnel have access to the service logs as follows:

- Staff in Ireland, the Netherlands, and the United States can access these logs in the form they are created in the data centres;
- Staff in Canadian facilities have access to logs for the Exchange Online Protection for Exchange service;
- Support staff elsewhere do not have access to these logs or have access only to logs that have been filtered to remove customer data.

Tier 1 support staff who answer help-desk calls are located globally future.. These employees do not have access to customer data. Customers phoning the help-desk can, after the call has been logged, ask the location of the support engineer and request that the call be transferred elsewhere.

Customer authored data can only be accessed by Office 365 Engineering and Operation support staff[5] in the US. Such staff are subject to pre-employment and on-going background checks including:

- Education history (not carried out on existing staff);
- Employment History (not carried out on existing staff);
- Social Security;
- Criminal Convictions;
- Office of Foreign Asset Control list;

[5] Microsoft has recently announced enhanced capabilities to require explicit customer approval for customer authored data access, this and other announcements related to activity logs and encryption options are excluded from this document. Details are available http://blogs.office.com/2015/04/21/enhancing-transparency-and-control-for-office-365-customers/

- Bureau of Industry and Security list;
- Office of Defence Trade Controls debarred list (DDTC).

Contractors etc. who may have access to customer authored data are subject to these same checks.

The above information is summarised in the following table:

Data	Support level	Location from which it is accessed	Background checks completed on staff?
Sanitised service logs.	Tier 1	Worldwide	No.
Service logs (may contain email addresses, URLs etc. but no customer data).	Tier 1/2	Ireland, Netherlands, US, Canada	No
Customer authored data.	Tier 3	US	Yes.

3.4. Privacy Impact Assessment

Microsoft does not have oversight or knowledge of the data stored by Customers in the Office 365 service. It provides a secure environment in which Customers manage and control their own data.

The Information Commissioner has stated that cloud service providers, Microsoft in this case, are Data Processors within the meaning of the Data Protection Act and process data on behalf of the service consumer. The service consumer remains the Data Controllers and retains responsibility for ensuring their processing complies with the Act.

In consequence it is the Customer, and not Microsoft, who must remain responsible for any personal information stored in Office 365 and for conducting a Privacy Impact Assessment should such an assessment be necessary.

Office 365 has achieved compliance with the ISO 27018 standard – the Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Compliance with this standard has been verified by BSI.

3.5. Roles, Responsibilities & Functions

Greg Roberts, Office 365 Governance, Risk and Compliance Director, Microsoft Corporation

4. Consuming Organisation IA Requirements

4.1. SyOps for Consuming Organisations

Some of the responsibility for the secure management of Office 365 lies with the customer who will need to extend certain internal policies and procedures to include the service or introduce new one where they do not already exist. The following controls should be in place to ensure the security of customer data:

4.1.1. User management

Customers are responsible for the management of user IDs and passwords and access control.

- **Account management**: If AD federation is used, then most of the technical controls will be replicated to the Online AD, however these controls will need to be configured by the customer in its own AD infrastructure. If AD federation is not employed, the customer must configure on-line IDs for each user. The account management controls should include:
  - Account setup and deletion;
  - Password complexity;
  - Password expiry and history;
  - Account lockout.
- **Access control**: Customers are responsible for ensuring that their access control policy is implemented in SharePoint etc. and in particular the granting, revoking and review of a user's access rights. It is normal to grant access based on the "need to know" principal. Additional controls that may need to be introduced include:
  - Guest users should not be invited to SharePoint as these Users cannot be positively authenticated;
  - Customers should not enable anonymous access rights in SharePoint;
  - Office 365 content should only be shared with authenticated Users.
- **Segregation of duties**: Customers are responsible for maintaining appropriate segregation of duties by configuring the level of access for each user according to their job function. Customers will need to appoint appropriate staff to manage access control etc.
- **Support Requests**
  As with existing support processes utilised by UK Government for on premises software support, customers should not include sensitive or restricted data in the support request.

4.1.2. Awareness and training

Customers are responsible for ensuring that their employees are aware of what information can be stored on Office 365 based on the Business Impact Level (BIL) of that information. In addition, users should be made aware of the risks involved in:

- Improperly forwarding documentation through Exchange;
- Improperly securing documentation hosted in Sharepoint;
- Circumventing, disabling, or downgrading session-level encryption.
- Inappropriate use of optional features, configurations or add-ons to the Office 365 Services in a manner resulting in sensitive or restricted customer data leaving the Office 365 compliance boundary

4.1.3. Data Aggregation

HMG's guidance regarding aggregated datasets is that in most circumstances they should be managed within the same infrastructure as that used to store information classified at OFFICIAL; there is no threshold where aggregated data will result in an uplift in the classification level.

However, it is important to realise that the impact to the business of a compromise involving aggregated data is likely to be higher than that involving a single record. It is the customer's responsibility to ensure that data stored within its Office 365 environment does not result in the risk appetite of the organisation being exceeded through aggregation.

Microsoft Office 365 has built its service and processes to be resistant to attacks or issues resulting from the storage of significant volumes of customer's data. Microsoft Office 365 monitors traffic to and within the service to ensure that it is legitimate and ensures that it can meet its contractual obligations; for example that the customers data is theirs and will not be used for datamining purposes

Each customers data is logically isolated at either customer level or mailbox level from other users data within the service. Verification of access control is tested frequently as part of standard operation procedure, auditing of the processes and any residual risk is managed through both the ISO27001 audit and SSAE16 audit cycles provided by the service.

Microsoft Office 365 provides processes to prevent the large scale offboarding of data, customers whom elect to transfer data from the service at the end of tenancy should plan for a throttled offboard of data. Microsoft Office 365 does not provide or allow direct access to disks/hardware to support other mechanisms for offboarding or removal of data from the data center. All disks and hardware are logically wiped (using US Department of Defense approved software) prior to secure physical destruction being conducted.

4.1.4. Systems and Information Integrity

Customers are responsible for:

- Ensuring anti-virus software is running on all workstation used to access the Office 365 environment;
- Ensuring that any SharePoint functionality that bypasses network-level encryption is not enabled;
- Ensuring that users only use Office Web Apps functionality through Exchange or SharePoint Online;
- Ensuring that any data stored, features enabled and used within the service, or add-ons enabled and used from the service, are appropriate to the impact levels for which the service has been accredited.

4.1.5. Security Incidents

A customer must opt-in to receive notifications of security incidents. It is the responsibility of the customer to forward that information to other organisations as appropriate.

4.1.6. SSL certificates

In order to use federated authentication between the customer's AD and MS ODS, an SSL certificate (also referred to as a Server Authentication Certificate) will be required. This is a standard SSL certificate that will be used for securing communications between federation servers, clients, and federation server proxy computers. As this certificate must be trusted by clients of ADFS and Office 365 service, the certificate must be issued by a public (third-party) Certificate Authority (CA) or by a CA that is subordinate to a publicly trusted root.

SyOps for the management of the SSL certificate should be developed.

4.1.7. Contractual Clauses

The EU Model Clauses on the transfer of personal data outside the EU should be included in any contract with Microsoft for Office 365 services. These contractual clauses have been approved by the UK Information Commissioner as a means of ensuring adequacy under Principle 8 of the Data Protection Act (DPA); however this approval only extends to use of the model contractual clauses as they stand. Any modifications to the clauses may invalidate this approval. Appropriate legal advice should be sought.

4.2. Incident Management Procedures

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

- Unauthorised access to customer data stored on Microsoft equipment resulting in the loss, disclosure or alteration of that data;
- E-mail viruses, malware and worms;
- Denial of service attacks against the service; and
- Any unauthorised access involving Microsoft computer networks or data processing equipment.

All Microsoft permanent and contract staff are required to report any security incident and any instance of a security weaknesses or malfunction that affects Office 365.

Policies and procedures have been defined for security incident management and consist of the following steps:

- **Identification**: All system and security alerts will be collected, correlated, and analysed. Events are investigated by Microsoft Online operational and security teams. If an event indicates a security issue, the incident is assigned a severity classification and escalated within Microsoft. This escalation will include product, security, and engineering specialists as appropriate. If the customer has opted in to receiving notice of security incidents affecting its data, Microsoft will inform the customer when such an incident occurs. It is the responsibility of the customer to forward that information to the PGA and other organisations as appropriate.
- **Containment** – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using forensic software and industry best practices.
- **Eradication** – Once the incident has been contained, the escalation team will attempt to eradicate any damage caused by the security breach and identify the root cause.
- **Recovery** – During recovery, software or configuration updates may be applied to the system so that the service is returned to full working capacity.
- **Lessons Learned** – Each security incident is analysed so that possible future reoccurrences can be avoided.

Microsoft Office 365 provides customers direct access to scoped activity logs from within each service, logging features vary by service and are documented in the service descriptions. Microsoft

will not provide full and unrestricted access to log file data in the event that a security incident has occurred and a forensic investigation is needed. Office 365 is a multi-tenanted solution and such log files may include other customers' data. Microsoft has stated that in such circumstances it will work with a customer on a case by case basis. If an in-depth investigation is required together with possible legal action, content can be collected from the systems involved using forensic software and industry best practices.

4.3. Deployment Options

4.3.1. Authentication

Customers can choose between either of the following authentication methods:

- **On-line identities**: Each user of the online Office 365 service must have an on-line ID created. This has the disadvantage or requiring the customer to maintain two authentication databases and the administrative overhead that this will involve. Customers may elect to use password hash synchronisation to minimise user impact
- **Federation**: A customer's AD can be synchronised with MSODS to provide single sign-on to Office 365 and allow a user to authenticate automatically when accessing the online service. The customer must enable the ADFS service to federate the two domains and set up an explicit trust with Microsoft's federation gateway.

4.3.2. Service Configuration

The service should be configured in accordance with Microsoft's Deployment Guide. If the Customer has any doubts or concerns he should contact a registered Microsoft Partner or Microsoft Consulting who will be able to provide advice on architecture issues.

5. Residual Risk Information

5.1. Risk Tolerance Statement

Microsoft Office 365 takes a balanced approach to risk, it ensures that changes made to the service or operations are assessed and validated prior to release, to help ensure that it can meet its contractual obligations with regards security and compliance.

5.2. Threat Assessment

The threats to the Office 365 service are not thought to be significantly different to those facing any HMG cloud based service. As these threats may vary from time to time, the latest Government threat assessment should be consulted.

5.3. Residual Risks

The ISO 27001 Continuing Assessment Audit dated 5th November 2014 did not identify any new non-conformities and there were no outstanding non-conformities from previous assessments.

A penetration test carried out in February 2015 found no critical or high risk issues. eight moderate and twelve low risk vulnerabilities. In summary, Office 365 was found to be implementing several good security controls and no direct, immediate exploitation vectors were identified

The risks rated at moderate are listed below:

Risk No.	Likeli-hood	Impact	Description	Reason for residual risk
1	Low	Moderate	Whilst in general all access to Office 365 applications was conducted over an encrypted (HTTPS) connection, in some instances data was passed over an unencrypted connection.	Within several parts of the Office 365 application, Microsoft provide access to a Community site from with the Office365 interface that are completed over an unencrypted connection. Personal information like e-mail address and username are sent over an un-encrypted connection. A fix for this issue is due to be completed in May 2015.

Risk No.	Likeli-hood	Impact	Description	Reason for residual risk
2	Low	Moderate	By default Office 365 emails passwords to administrators upon account creation. Office 365 does not enforce a password change upon initial login with the supplied password and hence an end user could continue to use the password supplied in the unencrypted email.	This is by design to meet the right balance of security and usability. Customers who need enhanced account security upon creation can set the checkbox to enforce a password change on initial login, federated authentication is based on the Active Directory configuration and not applicable to this scenario.
3	Low	Moderate	In multiple areas of the Office 365 application suite, HTTP basic authentication is used.	This is by design however Microsoft is continuously improving security and the use of Basic authentication is substantially reduced with the release of Office 365 modern authentication. Customers can enforce complex password policies in Azure to mitigate common dictionary attacks.
4	Low	Moderate	Some cookies used by the applications do not have common security flags set, and this could make them easier for an attacker to steal.	The majority of the cookies reported are not security sensitive or are mitigated by standard browser controls. The issues will be triaged and followed up on as appropriate as part of our normal development lifecycle. A fix for this issue has been developed but not yet deployed.

Risk No.	Likeli-hood	Impact	Description	Reason for residual risk
5	Low	Moderate	Using PowerShell it was possible to bypass restrictions on the use of HTML in Outlook Web Access E-Mails to craft a form which sends entered data to an attacker controlled domain. This could be used as part of a phishing campaign to attempt to get users to pass sensitive data to a malicious 3rd party.	This issue is currently being assessed. It is limited to the Outlook Web App and the behavior is very similar to a malicious Hyperlink since it was not possible to manipulate or use the users session through the Form.
6	Low	Moderate	The Lync application allowed any type of file to be transferred to another user without content checking.	This is by design, the application is blocking based on file extensions. File transfers in Lync are Client to Client so the appropriate malware scanning should be done at the client.
7	Low	Moderate	A stored Cross-Site Scripting issue was noted in Outlook Web Access, which was exploitable via an uploaded file which could run JavaScript code. The mobile version of the Word viewer allows the "javascript:" protocol in the URLs. The viewer did not properly encode links, this caused it to be vulnerable to an XSS issue which could be exploited without user interaction.	It would require a user to complete several manual actions to exploit. This vulnerability has been triaged and will be followed up on as appropriate as part of our normal development lifecycle. The second issue has been fixed has been fixed by implementing code to sanitize the links-.

Risk No.	Likeli-hood	Impact	Description	Reason for residual risk
8	Low	Moderate	The Office 365 login page was found to be vulnerable to reflected or non-persistent cross-site scripting (XSS) attacks via a cookie parameter. This type of vulnerability occurs when data provided by a web client is used immediately by server-side scripts to generate a page of results for the user.	This issue has been addressed but the fix has not yet been deployed. To be exploited the vulnerability require cross domain cookie injection vulnerabilities or local access to a system. This vulnerability did not affect ADFS users.

Appendix A: ISO/IEC 27001 Certificates

Microsoft Global Foundation Service

http://www.bsigroup.com/en-US/Our-services/Certification/Certificate-and-Client-Directory-Search/Certificate-Client-Directory-Search-Results/?searchkey=company%3dMicrosoft&page=1&licencenumber=IS%20533913

Microsoft Office 365

http://www.bsigroup.com/en-US/Our-services/Management-system-sertification/Certificate-and-Client-Directory-Search/Certificate-Client-Directory-Search-Results/?searchkey=standard%3dISO%252fIEC%2b27001%253a2013%26company%3dmicrosoft&licencenumber=IS 552878

Appendix B: Statement of Applicability

ISO 27001 Control	Description	Statement and justification of compliance
5. Information Security Policy		
5.1.1	Policies for information security	The Microsoft Online Services Information Security Policy (the "Policy") exists in order to provide Microsoft Online Services Staff and Contractor Staff with a current set of clear and concise Information Security Policies. These policies provide direction for the appropriate protection of the Microsoft Online Services. The Policy has been created as a component of an overall Information Security Management System (ISMS) for the Microsoft Online Services. The Policy has been reviewed, approved, and is endorsed by Microsoft Online Services management. Each management-endorsed version of the Microsoft Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Microsoft Security Policy is made available to all new and existing Microsoft Services Staff for review. All Microsoft Services Staff represent that they have reviewed, and agree to adhere to, all policies within the Microsoft Security Policy documents. All Microsoft Services Contractor Staff agree to adhere to the relevant policies within the Microsoft Security Policy. Should one of these parties not have access to this policy for any reason, the supervising Microsoft agent is responsible for distributing the policy to them. A customer facing version of the Microsoft Security Policy is made available for customer review through escalation to account or support representative.
5.1.2	Review of the policies for information security	The Microsoft Security Policy undergoes a formal review and update process at a regularly scheduled interval not to exceed 1 year. In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.

ISO 27001 Control	Description	Statement and justification of compliance
6. Organisation of Information Security		
6.1. Internal organisation		
6.1.1	Information security rules and responsibilities.	The Microsoft Security Policy requires that individuals responsible for ensuring the protection of assets and the secure delivery of services are appointed. Roles and responsibilities for all staff and contractors with regard to the security of information assets are documented in the Security Policy. The Policy has been reviewed, approved, and is endorsed by Microsoft management. The Security Policy is applicable to all staff and to all information and processes used in the conduct of Microsoft business. All Microsoft employees and contingent staff are accountable and responsible for complying with these guiding principles within their designated roles.

ISO 27001 Control	Description	Statement and justification of compliance
6.1.2	Segregation of duties	Segregation of duties is implemented for sensitive and/or critical functions in Microsoft Online Services' environments in order to minimize the potential of fraud, misuse, or error. All Microsoft service teams have defined roles as part of a comprehensive role-based access control mechanism. Additionally, each service team has identified any roles that, if shared by a single person, would allow for malicious activity without collusion. A delegated management model provides administrators with only the access they need to perform specific tasks, reducing the potential for error and restricting access to systems and functions on an as-needed basis: • Access to the Office 365 production environment is restricted to operations personnel. Development and test teams may be granted access by exception to production data to help troubleshoot issues; • Access to the Office 365 source code is restricted to engineering personnel; operational staff do not have write access to source code; • Access to Customer data is minimised and internal support teams only have the level of access necessary to perform their role. Access to operational servers is strictly controlled. Support staff may obtain access as a direct result of a service ticket to resolve a problem or to install software or patches. In such cases, an audit log is maintained.
6.1.3	Contact with authorities	The Microsoft Trustworthy Computing Group maintains contact with external parties such as regulatory bodies, service providers and industry forums. Microsoft has a dedicated team for most contacts with law enforcement agencies and the Office 365 service is reliant on the Global Criminal Compliance (GCC) & LCA organisations for contact with these bodies. Roles and responsibilities for managing and maintaining these relationships are defined.
6.1.4	Contact with special interest groups	Microsoft is a member of several industry organisations and both attends and provides speakers to such events and organisations. These include ISC2, RSA Security Conference, and ISACA etc.

ISO 27001 Control	Description	Statement and justification of compliance
6.1.5	Information security in project management	Microsoft's implementation of life cycle support is outlined through Microsoft Security Development Lifecycle (SDL), (SDL) process that is followed by all engineering and development projects. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security review and approval checkpoints are included during the system development life cycle.
6.2. Mobile devices and teleworking		
6.2.1	Mobile device policy	Mobile computing devices (i.e. Laptops, Smart Phones, etc…) are not permitted in, or directly attached to, any Microsoft Online Services production environment, unless those devices have been approved for use by Microsoft Online Services Management. All staff are required to follow appropriate security practices when using mobile computing devices to protect against the risks of using such equipment.
6.2.2	Teleworking	If allowed by function and role, Microsoft Online service supports secure teleworking per corporate standard. Microsoft has implemented a policy and supporting security controls to protect information accessed, processed or stored at teleworking sites. Telecommunicating locations are governed by the Microsoft remote access policy which requires remote access to production Microsoft's online services' networks to employ appropriate authentication mechanisms.

ISO 27001 Control	Description	Statement and justification of compliance
7. Human Resource Security		
7.1. Prior to Employment		
7.1.1	Screening	Microsoft Corporate Human Resources is responsible for screening all new hires per Corporate Policy. Standard background check including but not limited to review of information relating to employee education, employment, and criminal history. Tier 3 support staff with access to Customer data are subject to the following pre-employment and on-going background checks: • Education history (not carried out on existing staff); • Employment History (not carried out on existing staff); • Social Security; • Criminal Convictions; • Office of Foreign Asset Control list; Bureau of Industry and Security list; Office of Defence Trade Controls debarred list (DDTC). No candidate or employee will begin work or be placed on an assignment until the required background checks have been successfully completed. Contractors etc. who have access to Customer data are also subject to these checks.

ISO 27001 Control	Description	Statement and justification of compliance
7.1.2	Terms and conditions of employment	The Acceptable Use Standard, the Non-disclosure Agreement (NDA) and the Employee Handbook include responsibilities for information and asset protection. They also include the consequences of failing to comply with these requirements. Staff are informed that Office 365 security responsibilities extend outside of the work site, and beyond the standard operating hours of their employment and continue for a defined period after employment ends. All Microsoft Online Services staff are required to sign confidentiality and non-disclosure agreements, as well as the Microsoft Employee Handbook as a condition for employment. It is also the duty of Office 365 Staff to be in compliance with regulatory mandates. The on-going communication of these mandates occurs via the Risk Management Team (RMT), Microsoft Legal and Corporate Affairs (LCA), and Microsoft Human Resources.
7.2. During Employment		
7.2.1	Management responsibilities	Microsoft management personnel are responsible for ensuring that employees understand and comply with their obligations with regards security, compliance and confidentiality. Microsoft receives a signed acknowledgement from all staff and contractors indicating that they have read, understand, and agree to abide by policies before access to information and the information system is authorised.
7.2.2	Information security awareness, education and training	All staff are required to enrol in a New Employee Orientation (NEO) security awareness training course, Standards of Business Conduct, within the first 30 days of their employment or transfer into the organisation All relevant staff take part in an Office 365 sponsored security-training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. All contractor staff are required to take any training determined to be appropriate to the services being provided and the role they perform.

ISO 27001 Control	Description	Statement and justification of compliance
7.2.3	Disciplinary process	Microsoft employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. Office 365 staff suspected of committing breaches of security and/or violating the Information Security Policy, equivalent to a Microsoft Code of Conduct violation, are subject to an investigation process and appropriate disciplinary action up to and including termination. Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts. Human Resource is responsible for coordinating disciplinary response.
7.3. Termination and Change of Employment		
7.3.1	Termination or change of employment responsibilities	Responsibilities of management and employees related to completing the terminations including revocation of access, return of smartcards, ID cards, equipment and documentation, etc. are formally documented, and communicated by HR. Microsoft, upon termination of individual employment conducts exit interviews that include a discussion of information security topics.

ISO 27001 Control	Description	Statement and justification of compliance
8. Asset Management		
8.1. Responsibility for Assets		
8.1.1	Inventory of assets	Microsoft Online Services has implemented a formal policy that requires major assets (the definition of which includes data and hardware) used to provide the Office 365 service to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets within the asset inventory including owner or any associated agent, location, and security classification. Asset owners are also responsible for classifying and maintaining the protection of their assets in accordance with the standards. The Asset Management team maintains portions of the hardware asset data on behalf of the asset owner or associated agent and updates certain attributes in the asset management tool such as asset tag, physical location, etc.
8.1.2	Ownership of assets	Asset owners for assets within the Office 365 environment have been appointed in accordance with the Security Policy. Policies and procedures have been developed and implemented to define owner responsibilities.
8.1.3	Acceptable use of assets	Microsoft Online Services (which includes Office 365) have defined and implemented an Acceptable Use Policy (AUP) to supplement Microsoft's corporate standard with service specific requirements for the acceptable use of technology assets, infrastructure components and other services technologies. The policy applies to all Microsoft Online Services Staff, both permanent or contract, that support any of the services offered by Microsoft Online Services. Additionally, the Microsoft General Use Standard defines user responsibilities and establishes expected behaviour when using Microsoft systems. All users, including employees, vendors, and contractors are required to follow the rules of behaviour which are outlined in the General Use Standard.

ISO 27001 Control	Description	Statement and justification of compliance
8.1.4	Return of assets	Employees, contractors and third party users are formally notified to destroy or return, as applicable, any physical materials that Microsoft has provided to them during the term of employment or the period of contractor agreement and any electronic media must be removed from contractor or third party infrastructure. Microsoft, upon termination of individual employment, retrieves all security-related organizational information system-related property. Human Resources Assistants or the employee's manager collect Microsoft badges during the exit interview. Business Administrators and/or managers of the employee collect hardware assets. Microsoft may also conduct an audit to make sure data is removed in an appropriate manner.
8.2. Information Classification		
8.2.1	Classification guidelines	Office 365 standards provide guidance for classifying assets into one of several security categories, and then implementing a standard set of security and privacy attributes. Information assets are classified into one of the following security classification categories: • High Business Impact (HBI) • Moderate Business Impact (MBI) • Low Business Impact (LBI)
8.2.2	Labelling of Information	The asset owner is responsible for classifying and labelling all of their assets into one of these categories. The asset owner then classifies the data as either customer data or Microsoft data, and applies additional security attributes to customer data based on the category above.
8.2.3	Handling of Assets	The Asset Protection Standard defines the safeguards required to protect the confidentiality, integrity, and availability of information assets within Microsoft data centres. This standard includes control requirements for authentication, authorization, encryption, physical, and network communication and apply to those assets within or outside Microsoft Online Services physical boundaries.

ISO 27001 Control	Description	Statement and justification of compliance
8.3 Media Handling		
8.3.1	Management of removable media	O365 utilises approved media storage and disposal management services which are defined by policy. Microsoft does not use removable media within the service or for backups. The Office 365 service has been designed so that all backups are done through directly attached storage devices rather than by removable disks.
8.3.2	Disposal of media	Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. Hard drives that can't be wiped are destroyed which renders the recovery of information impossible. Appropriate means of disposal is determined by the asset type. Records of destruction are retained. MCIO maintains and follows applicable disposal procedures for assets located in data centres. Paper documents are destroyed by approved means at the pre-determined retention period.
8.3.3	Physical media transfer	Microsoft standards prescribe protection standards that are based on asset value: High Business Impact (HBI), Medium Business Impact (MBI) or Low Business Impact (LBI). These standards include control requirements for authentication, authorization, encryption, physical, and network communication and apply to those assets within or outside Microsoft Online Services physical boundaries. Microsoft utilises 3 methods to protect media that is being transported outside the data centre: 1) Secure Transport including tracking and locked tamper proof containers; 2) Encryption; 3) Cleanse, Purge, or Destroy.

ISO 27001 Control	Description	Statement and justification of compliance
9. Access Control		
9.1. Business Requirements of Access Control		
9.1.1	Access control policy	An access control policy has been implemented and is subject to annual review. Access to Office 365 assets by staff requires business justification and the asset owner's authorisation. In addition: • Access to assets is granted based upon need-to-know and least-privilege principles. • Where feasible, role-based access controls are used to allocate logical access to a specific job function or area of responsibility rather than to an individual. • Physical and logical access control policies are consistent with standards. The Access Control policy requires that access to assets is based on the need-to-know and least-privilege principles. Access is only granted with the asset owners' authorisation. User access privileges are periodically reviewed by the asset owners for appropriateness. Remote access to the Office 365 production environments by Microsoft staff and contractors is strictly controlled. All remote access requires management approval and automated processes remove access upon change in employee status. Additionally: • Terminal Services servers are configured to use the highest encryption setting. • Remote access requires two-factor authentication to a secure terminal server. Microsoft users must have a Microsoft-issued smartcard with a valid certificate and a valid domain account to establish a remote access session. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed.

ISO 27001 Control	Description	Statement and justification of compliance
9.1.2	Access to networks and network service	Microsoft employs the concept of least privilege, authorising access for users (and processes acting on behalf of users) when necessary to accomplish assigned tasks in accordance with business and operational requirements. By default, no one has access to customer content without authorisation. When a problem arises or a customer requests a service ticket, a Microsoft administrator must use a special lockbox tool to request and obtain elevated privileges to enter the data system and fix the problem. The lockbox sits between the administrator and the customer's system. The lockbox tool checks the scope of the administrator's permissions for carrying out certain activities. The tool will approve or deny the request and, if approved, grant access only after management approval has also been obtained. In certain situations, the lockbox may also notify another administrator to assist with situation. Only necessary actions are permitted and access is granted on a time-limited basis. After the permitted entry period has timed out, access privileges are automatically revoked. Every request for elevated privileges is logged.

ISO 27001 Control	Description	Statement and justification of compliance
9.2. User Access Management		
9.2.1	User registration and deregistration	The Microsoft Security Policy requires that access to information, systems and physical access to Microsoft buildings follow the principle of least privilege. The Security Policy prohibits the use of guest/anonymous and temporary accounts. All account requests go through the standard account management process. A record is maintained of personnel authorised to access systems that contain Customer Data. Office 365 has procedures as well as automated and semi-automated systems for granting and revoking access to the servers in the "Managed" domain based on employee status data from Microsoft HR. Automated feeds from HR systems provide this information and account management processes create or delete accounts based on valid HR records. Managers, owners of applications and data are responsible for reviewing who has access on a periodic basis. Regular access review audits occur to validate appropriate access provisioning has occurred.
9.2.2	User access provisioning	The Information Security Policy requires that access to Office 365 assets is based on business justification, with the asset owner's authorization and in accordance with the "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Account changes are managed with automated workflow management tools that allow service teams to track the process through account request, approval, creation, modification, and deletion.
9.2.3	Management of privileged access rights	Authorisation is granted based on the principle of least-privilege. Where feasible, role-based authorisation is used to allocate privileges to a specific job function or area of responsibility rather than to an individual. Microsoft restricts privileged accounts on the system to defined personnel or roles.

ISO 27001 Control	Description	Statement and justification of compliance
9.2.4	Management of secret authentication information of users	Password policies for corporate domain accounts are managed through Microsoft's corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. Temporary passwords are communicated to users using MSIT established processes. At initial login or after a password reset, the employee is required to change their password in compliance with defined complexity requirements. Regular password changes are enforced in compliance with corporate policy.
9.2.5	Review of user access rights	Managers, owners of applications and data are responsible for reviewing who has access on a periodic basis. Regular access review audits occur to validate appropriate access provisioning has occurred.
9.2.6	Removal or adjustment of access rights	Upon termination of employment, information system access is disabled. Microsoft Human Resources (HR) holds the primary responsibility of ensuring personnel termination is handled appropriately. Account changes are managed through automated workflow management tools that allow service teams to track the process through account request, approval, creation, modification, and deletion. When an employee leaves Microsoft employment, the relevant account is removed from the system via a service ticket. Once the transaction has been keyed in and approved, Microsoft Accounts and Security teams are notified and access to the network and buildings is shut off, via the termination transaction process and/or urgent terminations email template. For involuntary terminations, an urgent request for access termination is submitted via email from HR and access is disabled. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis. Regular access review audits occur to confirm that access has been provisioned appropriately. Customers are responsible for managing access to their own Office 365 environments.

ISO 27001 Control	Description	Statement and justification of compliance
9.3. User Responsibilities		
9.3.1	Use of secret authentication information	Microsoft enforces password complexity, expiry and reuse. Passwords are encrypted both in storage and in transmission. Passwords must not be shared or revealed and must be encrypted when stored. Additionally, passwords must be promptly changed if suspected of being compromised. Passwords must not be written down or stored in readable form batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them. All Office 365 employees take part in an appropriate security-training program and are recipients of periodic security awareness updates. Security education within Microsoft is an on-going process and is conducted at minimum annually in order to minimize risks. All O365 Contractor staff are required to take any training determined to be appropriate to the services they are providing and the role they perform.
9.4. System and Application Access Control		
9.4.1	Information access restriction	The Office 365 Access Control policy requires that access to assets is based on the need-to-know and least-privilege principles. Access is only granted with the asset owners' authorisation. User access privileges are periodically reviewed by the asset owners for appropriateness. Critical, back-end servers and storage devices are segregated from the public-facing interfaces. The networks within the Microsoft data centres are designed to have multiple separate network segments. Networks are logically separated wherever necessary according to trust boundaries. Network ACLs and filters are configured to segregate the traffic among the network segments.

ISO 27001 Control	Description	Statement and justification of compliance
9.4.2	Secure log-on procedures	Microsoft Online Services properties uniquely identify and authenticate Microsoft organizational users through the use of multiple Active Directory deployments. Office 365 employs secure login features including CTRL+ALT+DELETE, passwords are not shown in clear text, sensitive information is not displayed during login process, and minimal information is provided as a result of a failed login. Session time-out requirements are part of the technical and procedural controls defined by Microsoft's corporate policies. It is Microsoft's policy that there are no limitations of connection time as staff may require access 24x7.
9.4.3	Password Management System	Password policies for corporate domain accounts are managed through Microsoft's corporate Active Directory which specifies minimum requirements for password length, complexity and expiry. Temporary passwords are communicated to users using MSIT established processes. Password handling requirements include the changing of contractor supplied default passwords prior to introducing the associated service or system into any Microsoft Online Services owned or operated environment. Each Service Team within Microsoft Online has a local administrator password manager to securely maintain and store local administrator passwords for service systems.
9.4.4	Use of privileged utility programs	Access to system utilities is controlled by Active Directory ACLs/ACE's and is limited to authorised personnel only in accordance with Microsoft's Access Control Policy.

ISO 27001 Control	Description	Statement and justification of compliance
9.4.5	Access control to program source code	Access to O365 source code libraries is limited to authorised personnel. Where feasible, source code libraries maintain separate project work spaces for independent projects. Access requests require approval from the relevant project sponsor and access is granted only to those work spaces which are needed for the specific project. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained.
10. Cryptography		
10.1. Cryptographic controls		
10.1.1	Policy on the use of cryptographic controls	Cryptographic controls are designed and implemented, to protect the confidentiality, integrity and availability of Office 365 information. Encryption mechanisms and techniques used by the service team follow the requirements and restrictions outlined in the Microsoft Security Policy. Service data and information are handled in accordance with the requirements and restrictions specified in the Asset Classification and Protection Standards when cryptography is used. Office 365 implements at least the minimum acceptable cryptographic standard specified by internal standards, where cryptography is used. Staff are responsible for giving consideration to state, federal, international, and other controlling regulations and restrictions governing the use of cryptographic techniques. The Office 365 environment uses appropriate security technology as defined by the standards to protect the confidentiality of assets during transmission or storage.
10.1.2	Key management	Appropriate measures defined in key management standards have been taken into account to protect keys from modification, destruction and unauthorized disclosure. The Office 365 internal standards detail effective procedures that have been implemented.

ISO 27001 Control	Description	Statement and justification of compliance
11. Physical and Environmental Security		
11.1.	**Secure Areas**	
11.1.1	Physical security perimeter	The data centre buildings are nondescript and do not advertise that Microsoft services are hosted at that location. Access to the data centre facilities is restricted. Main access to Microsoft data centre facilities is restricted to a single point of entry that is manned 24x7 by security personnel. Emergency exits are alarmed and under video surveillance. The main interior or reception areas have electronic card access control devices on the perimeter doors which restrict access to the interior facilities.
11.1.2	Physical entry controls	Rooms within the Microsoft data centre that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are either restricted through various security mechanisms such as electronic card access control, keyed lock, anti-tailgating and/or biometric devices. Additional physical barriers, such as "locked cabinets" or locked cages erected internal to facility perimeters, may be in place as required for certain assets according to Policy. In addition to the physical entry controls operational procedures have been implemented to restrict physical access to authorized employees, contractors and visitors: • Authorization to grant temporary or permanent access to Microsoft data centres is limited to authorized staff. The requests and corresponding authorization decisions are tracked using a ticketing/access system. • Badges are issued to personnel requiring access after verification of identification. • Visitors are required to be escorted at all times. The escort's access within the data center is logged and if necessary can be correlated to the visitor for future review. • Data centre Management performs a quarterly access list review and take any follow up actions necessary.

ISO 27001 Control	Description	Statement and justification of compliance
11.1.3	Securing offices, rooms and facilities	Access to all Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) and biometrics for entry. Front desk personnel are required to positively identify employees or authorized contractors without ID cards. All guests are required to wear guest badges and be escorted by authorized Microsoft personnel.
11.1.4	Protecting against external and environmental threats	Environmental controls have been implemented to protect the data centres including: • Temperature control; • Heating, Ventilation and Air Conditioning (HVAC); • Fire detection and suppression systems; • Power Management systems;
11.1.5	Working in secure areas	The environment in which the O365 customer's data is stored is physically secured through multiple security checks. Secure physical access is restricted to authorised personnel only. Access is restricted by job function so that only essential personnel are authorised to manage customers' applications and services. Physical access controls are enforced using multiple authentication and security processes: badge and smartcard, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication for physical access to the data centre environment. Physical monitoring, including motion sensors, 24-hour secured access, video camera surveillance, and security breach alarms is in place.
9.1.6	Delivery and loading areas	There are no public access areas in Microsoft's data centres. Loading areas are secured as above.
11.2.	**Equipment**	
11.2.1	Equipment siting and protection	Office 365 equipment is placed in environments which have been engineered to be protective from theft and environmental risks such as fire, smoke, water, dust, vibration, earthquake, and electrical interference.

ISO 27001 Control	Description	Statement and justification of compliance
11.2.2	Supporting utilities	The data centres have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, i.e. generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centres have provisions for emergency fuel delivery. The data centre has a dedicated Facility Operations centre to monitor the following: • Power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment. • The Heating, Ventilation and Air Conditioning (HVAC) system, which controls and monitors space temperature and humidity within the data centres, space pressurization and outside air intake. Fire Detection and Suppression systems exist at all data centres. Additionally, portable fire extinguishers are available at various locations in the data centre. Routine maintenance is performed on facility and environmental protection equipment.
11.2.3	Cabling security	All Data and Power cabling is protected from interception or damage.
11.2.4	Equipment maintenance	Microsoft schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The Critical Environment (CE) team schedules all maintenance activities performed on CE components. Microsoft data centres rely on a computerised maintenance management system (CMMS) to manage maintenance schedules and work order management. Work orders are generated based on OEM guidelines and assigned for completion. All maintenance work performed at a Microsoft data centre must follow approved instructions captured in a Method of Procedure (MOP) document. A MOP must have data centre management approval before work can begin. Completed MOPs are reviewed and receive data centre management sign-off to indicate completion. Details of completed MOPs are stored in CMMS and then the work order closed.

ISO 27001 Control	Description	Statement and justification of compliance
11.2.5	Removal of assets	Microsoft Online Services asset and data protection procedures provide prescriptive guidance around the protection of logical and physical data and include instructions addressing relocation. Removable media and wireless devices are prohibited in Microsoft data centres.
11.2.6	Security of equipment and assets off- premises	The use or storage of Microsoft managed information processing equipment and/or media containing HBI or MBI data (as defined by Microsoft policy) outside a Microsoft managed facility must be approved by the asset owner. Protection afforded to such equipment and storage media is commensurate with the protection it is afforded on-site.
11.2.7	Secure disposal or re-use of equipment	Microsoft employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. NIST 800-88 compliant software is used to erase storage media. Hard drives that cannot be wiped are physically destroyed by shredding or incineration such that the recovery of information is impossible. The appropriate means of disposal is determined by the asset type. Records of the destruction are retained.
11.2.8	Unattended user equipment	All employees take part in a mandatory Office 365 security-training program and receive periodic security awareness updates. Securing unattended user equipment is included in this training. Security education is an on-going process and is conducted at least annually. All contractor staff are required to take any training determined to be appropriate to the services they are providing and the role they perform.
11.2.9	Clear desk and clear screen policy	Microsoft operates a clear-desk policy however this is managed at the Corporate level.
12. Operations Security		
12.1.	**Operational Procedures and Responsibilities**	
12.1.1	Documented operating procedures	Operating procedures are formally documented and approved by O365 management. The standard operating procedures are reviewed at least once per year.

ISO 27001 Control	Description	Statement and justification of compliance
12.1.2	Change management	An operational change control procedure is in place for changes to O365 services and systems. This procedure includes a process for management review and approval. This change control procedure is communicated to all parties who perform system maintenance on, or in, any of the O365 facilities. The operational change control procedure considers the following actions: • The identification and documentation of the planned change; • An assessment process of possible change impact; • Change testing in an approved non-production environment; • Change communication plan; • Change management approval process; • Change abort and recovery plan (when applicable).
12.1.3	Capacity management	Microsoft proactively monitors the performance of key subsystems of the Office 365 platform against established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates an alert so that operations staff can take any necessary action. Microsoft has the following operational processes in place: • proactive capacity management based on defined thresholds or events; • hardware and software subsystem monitoring for acceptable service performance and availability, CPU utilization, service utilization, storage utilization and network latency.

ISO 27001 Control	Description	Statement and justification of compliance
12.1.4	Separation of development, test and operational facilities	Separate environments are maintained for the Non-production and for Production operations of Microsoft Online Services. Movement or copying of Customer data out of the Production environment into a Non-Production environment is expressly prohibited except where customer consent is obtained, or at the directive of LCA. Changes between environments, and within the Production environment, are to be subject to a policy. Access to the production environment is carefully controlled to allow access to Microsoft Online Services Staff and Microsoft Online Services Contractor Staff members who require access and are authorized to perform certain duties. While each environment may have its own standards for operating, a formalized procedure exists for the exchange of Assets between environments. These procedures adhere to all relevant privacy requirements and Services Standards.

ISO 27001 Control	Description	Statement and justification of compliance
12.2.	**Protection from malware**	
12.2.1	Controls against malware	Microsoft Online Services run multiple layers of anti-malware software to ensure protection from common malicious software. For example, servers within the Microsoft Online environment run anti-malware software that scans incoming files for viruses. Additionally, Microsoft Exchange mail servers run additional anti-virus software that focuses on scanning email messages for malware. Additional information may be found in the relevant service descriptions: **Microsoft Online Services Server Operating System** All Microsoft Online environment servers run anti-malware software that scans the operating system for malware. AV agents on servers check for updates to antivirus definitions every 30 minutes. **Forefront for Exchange** Microsoft Forefront Security for Exchange Server integrates multiple scan engines from industry-leading security firms into a comprehensive, layered solution, helping businesses protect their Microsoft Exchange Server messaging environments from malware, worms, spam, and inappropriate content. **Forefront for SharePoint** Microsoft Forefront™ Security for SharePoint provides comprehensive protection for SharePoint Online documents and files uploaded to SharePoint Online environments using multiple scan engines and content controls to help eliminate malicious code. SharePoint Online refreshes virus signatures daily. Antivirus scanning is configured to scan only when files are uploaded to the system. If a file contains a virus, upload will fail with an error message displayed to the user about the virus found in the document. At this time no reporting is provided about antivirus scanning statistics. Microsoft Online Services is an isolated server centric environment which mobile code isn't as applicable as in a desktop environment. In addition, all code is explicitly installed on our servers by Administrators through the change control process.

ISO 27001 Control	Description	Statement and justification of compliance
12.3.	**Back-up**	
12.3.1	Information back-up	Customer content is replicated from a primary data centre to a secondary data centre in a redundant environment. As such, there is not a specific backup schedule as the replication is constant. Multiple levels of data redundancy are implemented including redundant disks to protect against local disk failure and full data replication to a geographically dispersed data centre. Customers can choose to perform their own extractions/backups if necessary. Office 365 performs a validation of backup/recovery procedures annually.
12.4.	**Logging and monitoring**	
12.4.1	Event logging	Office 365 has formal monitoring processes in place and a defined set of user and administrator events are logged and sent to a central log server to protect them from unauthorised access. Microsoft has teams dedicated to real time monitoring of the service at various levels. The teams provide 24/7 security logging, monitoring/correlation, analysis and reporting. All security incidents are investigated. Microsoft also continually re-assesses the threat framework using industry sources and performs 24/7 PAVC (Patching, A/V, Vulnerability and security Configuration) scanning and reporting of the Office 365 service. All faults notified to the Support Centre are logged and followed up to satisfactory completion. With regard to physical security, Microsoft maintains three 24/7 Global Security Operations Centers (GSOC) to monitor, communicate and coordinate responses to security incidents. Each GSOC monitors and responds to signal data and event notifications within its own region. Signal data includes intrusion, duress, environment and fire alarm information from all of the equipment related to physical security access control and monitoring. The GSOCs also facilitate communications and dispatch on-site security in response to events.

ISO 27001 Control	Description	Statement and justification of compliance
12.4.2	Protection of log information	Access to log information is restricted and defined by policy. A delegated management model enables administrators to have only the access they need to perform specific tasks. Logs are stored on a central log server to prevent unauthorised access
12.4.3	Administrator and operator logs	Audit logs record privileged user access and activities, authorised and unauthorised access attempts, system exceptions, and information security events.
12.4.4	Clock Synchronisation	Office 365 servers and components use consistent clock settings. Server clocks are synchronized through the Network Time Protocol to a central time source so that a consistent and accurate time is maintained throughout the environment.

ISO 27001 Control	Description	Statement and justification of compliance
12.5.	**Control of operational software**	
12.5.1	Installation of software on operational systems	The Microsoft Security Policy includes the following requirements regarding the installation of software in the Office 365 environment: • All software (including tools and utilities) installed in the Office 365 production environment must be approved by the appropriate stakeholders. • Software undergoes appropriate testing and staging before being released into the Office 365 production environment to minimize impact to system security, integrity and availability. • Software submitted for approval must have a legitimate business purpose. Production software is deployed according to approved procedures. The capability to release software into production is restricted to a limited number of authorised personnel who are responsible for ensuring that the requirements of Microsoft Online Services Trustworthy Services Lifecycle Standards are met prior to deployment. The integrity of Microsoft Online Services' production software is confirmed on a regular basis. An automated version control system has been implemented to help facilitate this process. Duty segregation is enforced by requiring that during normal operations, only authorized operations personnel have access to production systems. There are processes in place to allow developers and testers to access production systems on a temporary basis.

ISO 27001 Control	Description	Statement and justification of compliance
12.6.	**Technical Vulnerability Management**	
12.6.1	Control of technical vulnerabilities	Office 365 has implemented procedures to scan the environment for vulnerabilities. Any such vulnerabilities identified will be monitored and tracked until remediated. In addition, the RMT performs formal regular vulnerability assessments to determine whether key controls are operating effectively. Any findings are categorised by risk level and modifications to the environment are implemented accordingly The Microsoft Security Response Centre (MSRC) regularly monitors external security vulnerability awareness sites. As part of the routine vulnerability management process, the Office 365 team will evaluate the exposure to these vulnerabilities and will take action to mitigate risks when necessary. The MSRC releases security bulletins on the second Tuesday of every month or as appropriate to mitigate zero-day exploits. In the event that proof-of-concept code is publicly available regarding a possible exploit, or if a new critical security patch is released, the Office 365 team is required to apply these patches to affected systems in accordance with the patching policy. Servers within Microsoft Online are regularly updated with the appropriate security updates for the software that they use. The time when updates are applied is based upon a timeline derived by the criticality, scope, and impact of the security vulnerability associated with each update.
12.6.2	Restrictions on software installations	Microsoft has established policies governing the installation of software by users. The Microsoft Acceptable Use Standard details acceptable and unacceptable use of Microsoft Online Services IT assets, including the use of elevated privileges and communications software. This document details acceptable and unacceptable use of Microsoft information assets including the unauthorised installation of software.

ISO 27001 Control	Description	Statement and justification of compliance
12.7.	**Information systems audit considerations**	
12.7.1	Information systems audit controls	A scope and approach is formally agreed during the planning phase for both internal and external audits. The controls that are to be tested are identified together with the tools and techniques to be used, the required level access or privilege of audit software and the service personnel support/hours required. Coordination between the service/asset owners and management helps to ensure that any potential risks are identified and plans put in place to mitigate them.

ISO 27001 Control	Description	Statement and justification of compliance
13. Communications security		
13.1.	**Network Security Management**	
13.1.1	Network controls	Access to all O365 assets is based upon business requirements and only granted with the asset owner's authorisation. To maintain the confidentiality and integrity of customer data, Microsoft keeps consumer services networks separate from Office 365 networks. Multiple techniques are used to control information flows including but not limited to: • **Physical separation**. Network segments are physically separated by routers configured to restrict traffic. • **Logical separation**. VLANs are used to further segment network traffic. • **Firewalls**. Firewalls and other security enforcement points are used to limit network traffic. • All traffic to and from customers are transmitted over encrypted connections. Microsoft does not employ Port-based Network Access Control in the Office 365 data centre environment. However, it has physical security controls to prevent unauthorised equipment being installed on the network. These include: • Staff are prohibited from taking unauthorised equipment is allowed into the data centres; • New equipment is introduced through a quarantined zone, where it is physically commissioned in racks by one team of engineers. It is then transferred to the appropriate machine rooms by a separate team. Another different team will then connect the equipment onto the network. There is no remote access to the Office 365 production network.

ISO 27001 Control	Description	Statement and justification of compliance
13.1.2	Security of network services	The networks within the Office 365 data centres are designed to create multiple separate network segments within each data centre. This segmentation helps to provide physical separation of critical, back-end servers and storage devices from the public-facing interfaces. Physical access to diagnostic and configuration ports is controlled through data centre physical access controls. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed. The production network is shared by all Office 365 Customers. Within the data centres the network has been segregated into multiple segments. The goal of this segmentation is to provide physical separation of critical, back-end servers and storage devices from the public-facing interfaces. Customer access Office 365 services over the Internet from Customer locations to a Microsoft data centre. These connections are encrypted using industry-standard Transport Layer Security (TLS) /Secure Sockets Layer (SSL) to establish a secure browser-to-server connection. Firewalls at the edge of the Office 365 network provides security at the packet level for preventing unauthorized connections. Data storage and processing is logically segregated among Customers of the same service through Active Directory and other capabilities specifically developed to help build, manage, and secure multitenant environments.
13.1.3	Segregation in networks	The networks within the Office 365 data centres have been designed to create multiple separate network segments. This segmentation provides physical separation of critical, back-end servers and storage devices from the public-facing interfaces.

ISO 27001 Control	Description	Statement and justification of compliance
13.2.	**Information Transfer**	
13.2.1	Information transfer policies and procedures	Microsoft authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements. Microsoft requires all third parties to sign a Microsoft Master Vendor Agreement (MMVA). This requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft confidential information. Microsoft includes provisions in the MMVA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements. To minimize the risks associated with the exchange of Assets between organizations, exchanges between internal or external organizations are completed in the following manner: • The exchange is approved by the Asset Owner/Trustee. • The exchange follows the minimum requirements for Asset protection, by class as detailed in the Microsoft Online Services' Asset Classification and Protections Standards. • The RMT approves certain exchanges with parties outside of Microsoft Online Services. Exchanges of High Business Impact and Medium Business Impact assets with non-Microsoft parties are made only in connection with a formal contract approved by Legal & Corporate Affairs (LCA).

ISO 27001 Control	Description	Statement and justification of compliance
13.2.2	Agreements on information transfer	Microsoft's corporate RMT are required to approve any exchanges of information with external parties. As part of this process, exchanges that involve assets that are of High Business Impact or Medium Business Impact must include a formal contract. Third party contracts include appropriate security requirements. Microsoft has documented, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated. This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. Microsoft requires all third parties (external information system services) who are engaged with Microsoft Online Services to sign a MMVA. z.
13.3.3	Electronic messaging	Formal standards include control requirements for all network communication. The control requirements depend on the asset classification and apply whether internal or external to Microsoft network boundaries. Encryption is provided at the transport layer (between the client and data centre) using SSL.
13.3.4	Confidentiality or non-disclosure agreements	Microsoft Legal department and Human Resources maintain policies and procedures defining the implementation and execution of non- disclosure and confidentiality agreements. Microsoft ensures that access to classified information requiring special protection is granted only to individuals who have read, understood, and signed a nondisclosure agreement. All employees sign a confidentiality agreement.

ISO 27001 Control	Description	Statement and justification of compliance
14. Information Systems Acquision, Development and Maintenance		
14.1.	**Security Requirements for Information Systems**	
14.1.1	Information security requirements analysis and specification	Microsoft's implementation of life cycle support is outlined through its SDL process that is followed by all engineering and development projects. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security review and approval checkpoints are included during the system development life cycle. All members of software development teams receive appropriate training to stay informed about security basics. Microsoft Online Services implements the acquisitions control through enforcement of the Microsoft Security Policy. The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft's online services' information assets or information processing facilities, or (ii) add products or services to Microsoft's online services' information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security standards are addressed in the agreement, to provide a level of protection.

ISO 27001 Control	Description	Statement and justification of compliance
14.1.2	Securing application services on public networks	Microsoft implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical safeguards. Office 365 implements boundary protection through the use of controlled devices at the network boundary and at key points within the network. Office 365 ordering, billing, and payment systems that handle credit card data are Level One Payment Card Industry (PCI) Compliant; this is confirmed by independent audit. Publically available information relating to Office 365 is hosted on secure web servers which are protected from unauthorised access. Only authorised Microsoft staff are allowed access to modify such information. Office 365 is not an e-commerce solution and is not suitable for processing, transmitting, or storing PCI-governed data.
14.1.3	Protecting application services transactions	Office 365 is compliant with the requirements of the PCI-DSS standard with regard to billing and payment for its service. Office 365 is not suitable for processing, transmitting, or storing PCI-governed data.

ISO 27001 Control	Description	Statement and justification of compliance
14.2.	**Security in development and support services**	
14.2.1	Secure development policy	Microsoft manages the information system using a system development life cycle that incorporates information security considerations. Microsoft's implementation of life cycle support is defined in its SDL process that is followed by all engineering and development projects. This is a software development model that includes specific security considerations. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security review and approval checkpoints are included during the system development life cycle. All major milestones go through a SDL review captured via an internal tool called QE.
14.2.2	Change control procedures	A formal change control procedure is followed when making changes to any production Office 365 system. This procedure includes a review and approval process. This change control procedure is communicated to all staff, contractors and third parties who perform system maintenance. The procedure includes: • The identification and documentation of the planned change; • Assessment of the change impact; • Change testing in an appropriate non-production environment; • Change Communication plan; • Change management approval process; • Change abort and recovery plan. Where possible, the system version and change control procedure are integrated with the operational change control procedure.

ISO 27001 Control	Description	Statement and justification of compliance
14.2.3	Technical review of applications after operating system changes	Changes to the underlying operating systems within the Office 365 environment are reviewed and tested for their quality, performance, impact on other systems, recovery objectives and security features before they are deployed into production. The service team follows the SDL process, which involves testing within a segregated environment, code review and documentation of changes within change management tool. Technical reviews of significant Microsoft Online Services system changes are performed and approved by Change Advisory Boards.
14.2.4	Restrictions on changes to software packages	Modifications to software packages are not made unless explicitly approved by Office 365 management and under the control of version and change management procedures. Changes to source code requires write access to the source code trees. Requests for this level of access require the approval of the project sponsor.
14.2.5	Secure system engineering principles	Microsoft has established the Secure Development Lifecycle (SDL) process and procedures which it uses for all development processes. The SDL defines acceptable standards to ensure that data inputs to application systems are accurate and within the expected range of values. Where appropriate, data inputs are sanitised or otherwise rendered safe before being input to an application system. Internal processing controls are implemented within the Office 365 application in order to limit the risks of processing errors. Internal processing controls exist in applications, as well as in the processing environment. Examples of internal processing controls include, but are not limited to, the use of hash totals, and checksums etc. Data output by application systems is validated prior to being stored or passed on to subsequent systems for further processing. Microsoft's SDL specifies tools for testing including output data validation and testing is conducted as part of the security review for new or existing applications or services. This review is carried out by an independent advisor from Microsoft's Trustworthy Computing group.

ISO 27001 Control	Description	Statement and justification of compliance
14.2.6	Secure development environment	The SDL provides guidance to Office 365 personnel on how to meet requirements in accordance with applicable Microsoft, industry, regulatory and best practices for compliance. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security review and approval checkpoints are included during the system development life cycle. All major milestones go through a SDL review captured via an internal tool known as QE. All responsibilities, roles and configurations are defined for each development team. The development, build, staging and production environments are also segregated.
14.2.7	Outsourced development	The MMVA requires third parties to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft confidential information. Microsoft includes provisions in the MMVA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. The risk associated with outsourced software development is mitigated through: • Pre-contract security assessments against Office 365 security policy and standards; • Requests and review of independent audits or certifications reports; • Internal code reviews. Prior to release to production, all third party software undergoes integrated system testing and approval by the change management board.

ISO 27001 Control	Description	Statement and justification of compliance
14.2.8	System security testing	System security testing is included in the SDL. Reviewing attack surface upon code completion helps ensure that any design or implementation changes to an application or system have been taken into account, and that any new attack vectors created as a result of the changes have been reviewed and mitigated including threat models. The Final Security Review (FSR) usually includes examining threat models, tools outputs, and performance against the quality gates and bug bars defined during the Requirements Phase.
14.2.9	System acceptance testing	Microsoft requires the developer of the production, system component, or production service to perform testing/evaluation during development. The service team is responsible for ensuring that all system development and maintenance activities are performed in accordance with the Microsoft SDL process. System acceptance is included in the change management process. This process requires formal acceptance and management review and approval. The change management procedure is communicated to all parties (staff, contractors and third parties).
14.3.	**Test data**	
14.3.1	Protection of system test data	The movement or copying of Customer data from the production environment to a test or development server is expressly prohibited except where Customer consent is obtained to troubleshoot the service or at the directive of Microsoft's legal or investigative department.

ISO 27001 Control	Description	Statement and justification of compliance
15. Supplier relationships		
15.1.	**Information security in supplier relationships**	
15.1.1	Information security policy for supplier relationships	Microsoft contractually requires third party service providers to Microsoft to maintain and meet requirements set forth in the Information Security Policy. In all contracts, Microsoft includes provisions to ensure that third-party providers meet or exceed the personnel security requirements mandated by Microsoft. This includes the ability to successfully pass the Microsoft background check, or equivalent, as well as obtain and maintain a clearance if the specific project requires it. Third-party providers are subject to the same personnel screening requirements as Microsoft employees working on the O365 MT system for Federal customers. Third-party providers are required to sign a Non-Disclosure Agreement prior to accessing Microsoft information systems or resident information.
15.1.2	Addressing security within supplier agreements	Office 365 contractually requires third-party service providers to maintain and meet requirements set forth in the Microsoft Information Security Policy. In addition, these third parties are required to undergo an independent, annual audit or arrange to be included in Microsoft's annual third-party audit. All third parties engaged with Office 365 musty sign a MMVA.
15.1.3	Information and communication technology supply chain	In all contracts, Microsoft includes provisions to ensure that third-party providers meet or exceed the personnel security requirements mandated by Microsoft. Security requirements are included in the third party contracts as per the Procurement Process. Security requirements based on the risk analysis for third party vendors with access to customer information or production access must be identified and included in the contracts with third party vendors.
15.2.	**Supplier service delivery management**	
15.2.1	Monitoring and review of supplier services	Microsoft contractually requires all third party service providers to undergo an independent annual audit or arrange to be included in the Office 365 annual audit.

ISO 27001 Control	Description	Statement and justification of compliance
15.2.2	Managing changes to supplier services	Microsoft Office 365 regularly reviews and engages with third parties to plan for future changes or modifications that may affect the service.
16. Information security incident management		
16.1.	**Management of information security incidents and improvements**	
16.2.1	Responsibilities and procedures	Office 365 has developed processes to facilitate a coordinated response to incidents should one occur. Responsibilities and procedures are defined and documented. Incident handling, management roles and responsibilities have been defined for the Incident Engineer, Incident Manager, Communication Manager and the Feature teams. O365 Operations Managers are responsible for overseeing investigation and resolution of security and privacy incidents with support from other functions. Processes for escalating and engaging other functions for investigating and analysing incidents have been established. These include Privacy, Legal or Executive Management in the event of a security incident.
16.2.2	Reporting information security events	Staff and contractors are required to report all Office 365 security incidents, weaknesses, and failures. The procedures for the reporting and handling of these events have been defined. Processes and procedures are in place to facilitate a coordinated response to incidents if one was to occur. Forensic techniques will be used when necessary. A security event may include, among other things unlawful access to Customer data stored on our equipment and facilities and unauthorized access resulting in loss, disclosure or alteration of Customer data. Contractual obligations in the Data Processing Terms of the OST require Microsoft to notify customers promptly in the event of an incident affecting their data. Security notifications are, by nature, extremely rare, sensitive, and unique. Therefore, a formal process has been developed to tailor notification to the specific incident on a case-by-case basis. Notifications could be via email, phone, broad communication, or by direct engagement, depending on the issue and impact.

ISO 27001 Control	Description	Statement and justification of compliance
16.2.3	Reporting information security weaknesses	Microsoft employees and contractors are required to report any observed or suspected information security weaknesses in systems or services. The reporting and handling of these events follow prescribed procedures pursuant to defined and implemented policy.
16.1.4	Assessment of and decision on information security incidents	During the Identification phase of Microsoft's Incident Management process (see below), system and security alerts will be harvested, correlated, and analysed. Events are investigated by Microsoft operational and security organizations. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. The severity rating of an incident may change as additional information is revealed in an investigation. It is the responsibility of Security Incident Management personnel to update the rating and communicate changes to all stakeholders. Severity categories for Security Incidents include: **Critical**—typically an incident will first have a medium or high rating and then escalated to the critical level following standard escalation paths. Rating an incident as critical results in notification of Senior Management. **High**—incidents that must be addressed immediately. The Incident Management team will have on-call personnel available 24 hours to respond to incidents rated as "high." Typically these incidents would result in a severe degradation of online services, and/or a significant disruption of the Confidentiality, Integrity or Availability (CIA) of Microsoft Online Services assets. **Medium**—incidents that need to be addressed within 24 hours or the next business day. Examples include suspicious alerts, public vulnerabilities that our networks are supposedly immune too, and any other event that doesn't require immediate mitigation. **Low**—incidents that need to be addressed with 48 hours or longer.

ISO 27001 Control	Description	Statement and justification of compliance
16.1.5	Response to information security incidents	Office 365 has a defined process to facilitate a coordinated response to incidents if one was to occur. The process follows the following phases: • **Identification** – System and security alerts may be harvested, correlated, and analysed. Events are investigated by Microsoft Online operational and security organizations. . If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. • **Containment** – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. • **Eradication** – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering. • **Recovery** – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. • **Lessons Learned** – Each security incident is analysed to ensure the appropriate mitigations applied to protect against future reoccurrence. If Office 365 personnel determine that a customer's data was breached or otherwise subject to unauthorized access, the customer will be notified.
16.1.6	Learning from information security incidents	The Lessons Learned phase of the Security Incident Response process ensures that each security incident is analysed and that appropriate controls are applied to protect against future re-occurrence.

ISO 27001 Control	Description	Statement and justification of compliance
16.1.7	Collection of evidence	In the context of forensic information; Microsoft will work with a Customer on a case-by-case basis. However as this is a multi-tenant solution, it cannot provide full and unrestricted access to log file data of the servers and network as that data may include other Customers' information. Revealing such to a third party would be a breach of its contract with these customers. Microsoft will work with a customer to support them through a security incident.
17. Information security aspects of business continuity management		
17.1. Information security continuity		
17.1.1	Planning information security continuity	Business Continuity Plans are developed in line with industry best practices and to reflect the security controls of the production environment. Microsoft's Enterprise Business Continuity Management (EBCM) is based on the Disaster Recovery Institute International (DRII) Professional Practice Statements and the Business Continuity Institute (BCI) Good Practice Guidelines. A business impact analysis is completed at appropriate intervals but at least annually. The analysis includes: • The identification of threats relevant to the Microsoft Online Services business environment and process; • An assessment of the identified threats including potential impact and expected damage; • A management endorsed strategy for the mitigation of significant threats identified, and for the recovery of critical business processes. Office 365 maintains a framework that is consistent with industry to drive the continuity program at all levels. The framework includes: • Assignment of key resource responsibilities; • Notification, escalation and declaration processes; • Recovery Time Objectives and Recovery Point Objectives; • Continuity plans with documented procedures ; • Training program for preparing all appropriate parties to execute the Continuity Plan; • A testing, maintenance, and revision process.

ISO 27001 Control	Description	Statement and justification of compliance
17.1.2	Implementing information security continuity	The business continuity management solution reflects security, compliance and privacy requirements of the production Office 365 service environment at the alternate site. An Enterprise Business Continuity Management (EBCM) framework has been established for Microsoft and applied to individual business units including the Server and Tools Business (STB) under which Office 365 falls. The designated STB Business Continuity Program Office (BCPO) works with Office 365 management to identify critical processes and assess risks. The STB BCPO provides guidance to the Office 365 teams on EBCM framework and BCM roadmap, which includes the following components: • Governance; • Impact Tolerance; • Business Impact Analysis; • Dependencies Analysis (Non-Technical and Technical); • Strategies; • Planning; • Testing; and • Training and Awareness.
17.1.3	Verify, review and evaluate information security continuity	Recovery exercises are performed on a regular basis simulating disaster recovery scenarios.

ISO 27001 Control	Description	Statement and justification of compliance
17.2.	**Redundancies**	
17.2.1	Availability of information processing facilities	Microsoft has designed Office 365 to be a fully resilient service with redundancy built into every layer • Physical redundancy (via multiple disk/cards, servers, geographical sites, and data centres); • Data redundancy (constant replication across data centres); • Functional redundancy (the ability for customers to work offline when there is no network connectivity). The O365 Service is hosted in Microsoft data centres in Dublin and Amsterdam for UK Government customers and guarantees a 99.9% uptime. Customers are responsible for deploying their applications in multiple locations for geo-redundancy.
18. Compliance		
18.1.	**Compliance with legal and contractual requirements**	
18.1.1	Identification of applicable legislation	Microsoft has a global presence with Customers worldwide operating in different regulatory frameworks. As a provider of global cloud facilities, Microsoft runs its services with common operational practices and features across multiple jurisdictions. Microsoft has built its services with common privacy and security requirements in mind. All identified security, contractual, and regulatory requirements have been addressed through a formal regime of testing prior to sale of services and on an ongoing basis thereafter. Office 365 complies with all data protection and privacy laws generally applicable to Microsoft's provision of the service. Customers are responsible for compliance with laws and regulations specific to their industry or particular use of Office 365.

ISO 27001 Control	Description	Statement and justification of compliance
18.1.2	Intellectual property rights (IPR)	Risks associated with the violations of Intellectual Property Rights (IPR) are factored into the technical and procedural controls that govern the Office 365 service offerings. However, the vast majority of software used to deliver services is Microsoft product. All employees and contingent staff are required to follow applicable intellectual property laws and Microsoft maintains responsibility for use of proprietary software within the legislative jurisdictions and contractual constraints governing the organization. Microsoft will acquire no rights in Customer Data and will not use or disclose Customer Data for any purpose other than to provide the Office 365 service. With Customer consent, this may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). Microsoft will not disclose Customer Data to a third party (including law enforcement, other government entity, or civil litigant; excluding our subcontractors) except as Customer directs or unless required by law. Should a third party contact Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the third party to request it directly from Customer. As part of that, Microsoft may provide Customer's basic contact information to the third party. If compelled to disclose Customer Data to a third party, Microsoft will use commercially reasonable efforts to notify Customer in advance of a disclosure unless legally prohibited.

ISO 27001 Control	Description	Statement and justification of compliance
18.1.3	Protection of records	Office 365 provides a service which Customers can use to manage and control their own data. In order to create a secure environment for this data, Microsoft has adopted the following approach: • Software and services are developed with the objective of ensuring the confidentiality of data. Microsoft aims to comply with global privacy laws and its privacy practices are derived, in part, from these privacy laws. • Technical and organisational security measures are employed to ensure appropriate handling of Customer data. • Microsoft aims to be open and accountable, whenever possible, about its information handling procedures through publications available in the Office 365 Trust Centre. Microsoft Online Services owned assets are retained as appropriate based on retention requirements set by Corporate Records Management and an asset's classification, or based on contractual requirements. Microsoft guarantees retention of tenant data for 30 days after termination and all information is permanently deleted 90 days after termination of service.

ISO 27001 Control	Description	Statement and justification of compliance
18.1.4	Data protection and privacy of personal information	Microsoft does not have oversight or knowledge of the data stored by Customers in the Office 365 service. It provides a secure environment in which Customers manage and control their own data. The Information Commissioner has stated that cloud service providers, Microsoft in this case, are Data Processors within the meaning of the Data Protection Act and process data on behalf of the service consumer. The service consumer remains the Data Controllers and retains responsibility for ensuring their processing complies with the Act. In consequence it is the Customer, and not Microsoft, who must remain responsible for any personal information stored in Office 365 and for conducting a Privacy Impact Assessment should such an assessment be necessary. Microsoft is a member of the U.S. Safe Harbour program as agreed by the EU and the US Department of Commerce. This requires Microsoft to comply with the EU Data Protection Directive and allows it to transfer data outside of the EU to the US in order to provide Microsoft Online Services. Microsoft is also willing to sign the standard contractual clauses created by the European Union (called the "EU Model Clauses") with all customers. EU Model Clauses address international transfer of data to areas outside the EU. In addition, Office 365 has achieved certification against the ISO 27018 standard – the Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
18.1.5	Regulation of cryptographic controls	Microsoft Online Services provides information about statutes and regulations it adheres to through its contract and service description, including by jurisdiction. Microsoft Online Services has an established process for identifying and implementing changes to services in response to changes in applicable statutes and regulations.

ISO 27001 Control	Description	Statement and justification of compliance
18.2.	**Information security reviews**	
18.2.1	Independent review of information security	Office 365 controls are formally audited annually to the SSAE 16/ISAE 3402 standard by independent external auditors. To maintain its ISO 27001 certification, the service must be audited annually to ensure on-going compliance with the standard.
18.2.2	Compliance with security policies and standards	Microsoft regularly reviews and updates the current audit and accountability procedures. The Microsoft Security Policy contains rules and requirements that must be met in the delivery and operation of Microsoft Online Services. More detailed requirements are established within Microsoft Online Services Security Procedures and service team-specific standard operating procedures (SOPs). The Microsoft Security Policy contains rules and requirements that must be met in the delivery and operation of Microsoft Online Services. More detailed requirements are established within Microsoft Online Services Security Procedures and service team-specific standard operating procedures (SOPs). Microsoft Service Online asset owners ensure procedures within their area of responsibility are carried out correctly to achieve compliance with the Information Security Policy. As such, asset owners regularly review their compliance with the appropriate security policies, standards, and any other security standards. Appropriate actions are taken if any non-compliance is found as a result of the review.

ISO 27001 Control	Description	Statement and justification of compliance
18.2.3	Technical compliance review	Information systems are regularly checked for compliance with security implementation standards either manually or with the assistance of automated tools in coordination with the Risk Management Team. In addition to independent compliance assessments, the Risk Management Team performs the following compliance operational checks including: • Post-patch deployment compliance assessments, • AV agent and signature file assessment, • Routine compliance assessments of changes introduced to the Microsoft Online Services environment as part of Change Management process, • On-going cycle testing of key general computer controls.

Appendix C: Cloud Security Principles

The following table lists the UK Governments 14 Cloud Security Principles and Microsoft O365 level of compliance. For further information, refer to https://www.gov.uk/government/publications/implementing-the-cloud-security-principles/implementing-the-cloud-security-principles.

Cloud Security Principle	Implementation	Gaps / Comments
1. Data in transit protection	Firewalls are installed on the network boundaries and at key points within the network. These firewalls are configured to allow only those connections and services that are necessary for operational purposes. Customer connections to Microsoft O365 over the Internet can be encrypted using industry-standard Transport Layer Security (TLS) v1.2. All communication between data centres take place over Microsoft internal private networks using IPsec encryption.	None identified however, if the customer end user devices do not support TLS v1.2, O365 will fall back to an earlier version or unencrypted communication to attempt connectivity. It is the Customer's responsibility to ensure that end user devices support appropriate levels of encryption.
2. Asset protection and resilience	O365 relies on MCIO to provide datacentre security and infrastructure services (HVAC). MCIO has separate ISO 27001 certification. The data centres used to provide the service to UK organisations are located in the EU (Amsterdam and Dublin). The buildings are nondescript and do not advertise that Microsoft services are being hosted. Access to the facilities is restricted. The main interior or reception areas have electronic card access control devices on perimeter doors which restrict access to the interior facilities. Access to rooms within datacentres that contain servers etc. is restricted through various security mechanisms such as electronic card access control, keyed lock, anti-tailgating and/or biometric devices.	None identified. Independent validation is provided by the MCIO and O365 ISO 27001 certification.

Cloud Security Principle	Implementation	Gaps / Comments
	Microsoft uses NIST 800-88 compliant software to erase hard drives. Removable media and wireless devices are prohibited in Microsoft data centres.	
3. Separation between consumers	The service has been designed and developed using Microsoft's Secure Development Lifecycle process (see Principle 7 below) to help identify and counter risks inherent in a multitenant environment. Data storage and processing is logically segregated among O365 Customers using Active Directory and functionality specifically developed for multitenant services which aims to ensure that Customer data stored in shared datacentres is not accessible by another organisation.	None identified. Independent validation is provided by annual penetration tests carried out by a CREST registered provider.
4. Governance framework	O365 has a defined and documented security governance framework in place which has been certified against the ISO 27001 standard.	None identified. Independent validation is provided by the Microsoft O365 ISO 27001 certification.
5. Operational security	The O365 service has documented processes and procedures in place that comply with the requirements of its ISO 27001 certification. These processes include: Configuration and change management; Vulnerability management; Protective monitoring; Incident management.	None identified. Independent validation is provided by the Microsoft O365 ISO 27001 certification.
6. Personnel security	Customer data can only be accessed by O365 Engineering and Operation (Tier 3) support staff in the US. Such staff are subject to the following pre-employment and on-going background checks: Education history (not carried out on existing staff);	No background checks are carried out on Tier 1 and Tier 2 support staff. However these employees only have access to sanitised log files which do not contain private Customer data. The background checks carried out on Tier 3 staff are broadly in line with the requirements of the UK Government's

Cloud Security Principle	Implementation	Gaps / Comments
	Employment History (not carried out on existing staff); Social Security; Criminal Convictions; Office of Foreign Asset Control list; Bureau of Industry and Security list; Office of Defence Trade Controls debarred list (DDTC). No candidate or employee will begin work or be placed on an assignment until the required background checks have been successfully completed. Contractors etc. who may have access to Customer authored data are also subject to these checks. In addition to background checks, all O365 personnel are required to complete annual security training classes.	BPSS / BS7858. They do not specifically include a formal identity check however it can be assumed that the sum of the other checks carried out effectively fulfils this role.
7. Secure development	Microsoft has defined and implemented the Security Development Lifecycle (SDL). The SDL is a software development process which aims to assist with the build of secure software and address compliance requirements. MS SDL conforms to the international standard for application security, ISO/IEC 27034-1:2011 and has been reviewed by CESG.	None identified. Independent validation is provided by the Microsoft O365 ISO 27001 certification.
8. Supply chain security	Microsoft requires all third parties suppliers involved with O365 to sign a Microsoft Master Vendor Agreement (MMVA). The MMVA contractually requires third parties to comply with Microsoft's Information Security Policy. Microsoft also requires that these third parties undergo an annual independent audit or arrange to be included in the O365 annual third party audit. All services provided by any third parties are included in the O365 risk assessment.	None identified. Independent validation is provided by the Microsoft O365 ISO 27001 certification.

Cloud Security Principle	Implementation	Gaps / Comments
9. Secure consumer management	Customer Administrators of O365 administer their service through the O365 Admin web page. Customers can choose between either of the following authentication methods: • **On-line identities**: Each user of the online Office 365 service can use an MS Online ID; • **Federation**: A customer's AD can be synchronised with MSODS to provide single sign-on.	None identified.
10. Identity and authentication	Users are authenticated using the Microsoft Azure Active Directory (AAD) as the authentication platform. This can be achieved in several ways: An on-premises AD Federation Service (AD FS) server can be linked with the O365 service to provide single sign-on (SSO). In this case, users' credentials never leave the domain network. Windows O365 uses an AD FS token to authenticate. The Microsoft Online Services Directory Synchronization Tool (DirSync) can be used to synchronise Customer AD with the O365 AD service. The DirSync tool and O365 AD mutually authenticate by using certificates and communicate using SSL. Alternatively, Customer administrators can create a Online ID account for users and enable multifactor authentication . This process takes place over an SSL encrypted connection. Microsoft support staff log on to the production service using two factor authentication over internal networks.	If the Online ID option is used, there is with no capability for enforcing the use of strong password selection. This also has the disadvantage of requiring the customer to maintain two authentication databases with the administrative overhead that this will involve.

Cloud Security Principle	Implementation	Gaps / Comments
11. External interface protection	Firewalls are installed on the external interface of the O365 network. See principle 10 regarding identification and authentication. An annual penetration test is carried out on the external network boundaries by a CREST registered provider.	None identified. Independent validation is provided by the annual penetration test.
12. Secure service administration	O365 uses a role-based authentication system to ensure that Customers' users have access on a need to know basis. With regard to administrative access by Microsoft support staff, a delegated management model provides administrators with only the access they need to perform specific tasks. All actions are logged. Access to the O365 production environment is restricted to operations personnel and is strictly controlled. Support staff may obtain access as a direct result of a service ticket to resolve a problem or to install software or patches. Development and test teams may be granted access by exception to production data to help troubleshoot issues. Access to Customer data is minimised and internal support teams only have the level of access necessary to perform their role. In all cases, an audit log is maintained.	None identified. Independent validation is provided by the O365 ISO 27001 certification.

Cloud Security Principle	Implementation	Gaps / Comments
13. Audit information provision to consumers	Audit logs record privileged user access and activities, authorised and unauthorised access attempts, system exceptions, and information security events.	Microsoft has said that as this is a multi-tenant solution, it cannot provide full and unrestricted access to log file data of the servers and network as that data may include other Customers' information. Revealing such to a third party would be a breach of its contract with these Customers. In the event of a security incident, Microsoft will work with its Customers on a case by case basis to ensure an appropriate outcome.
14. Secure use of the service by the consumer	This Security Principle is a Customer responsibility.	Not applicable.

Appendix D: Document Control

Version	Description	Author	Issued Date
0.1	Initial draft.	Richard Ellis	18th June 2012
0.2	Update to reflect RMARD v1.3	Richard Ellis	20th August 2012
0.3	Updated content	Pete Satchwell	10th September
1.0	Final	Pete Satchwell	12th September
2.0	Updated for GCloud 6	Richard Ellis	16th April 2015

Table 4: Version control