Microsoft

RESPONSE TO GCIO 105 QUESTIONS - MICROSOFT OFFICE 365 - JULY 2015

Microsoft Office 365

July 2015

MICROSOFT NEW ZEALAND LIMITED

22 Viaduct Harbour Avenue, Auckland

Security Privacy Compliance Transparency

Table of Contents

Executive Summary 2

Disclaimer 2

How to read this document 2

Security and Privacy Considerations 3

3.1 Value, Criticality and Sensitivity of Information 3

3.2 Data Sovereignty 4

3.3 Privacy 9

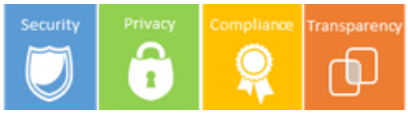
3.4 Governance 12

3.5 Confidentiality 20

3.6 Data Integrity 39

3.7 Availability 42

3.8 Incident Response and Management 49



Summary

In 2014 the NZ Government Chief Information Officer published a due diligence framework for agencies to use in evaluating cloud computing services. This document provides Microsoft's responses to the questions in that framework in relation to Microsoft Office 365.

Disclaimer

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

For the latest version of this document contact Russell Craig, the Microsoft New Zealand National Technology Officer, at Russell.Craig@microsoft.com

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

How to read this document

The document breaks the 105 due diligence questions (the "considerations") into their sub-sections as per the source document, and records Microsoft's understanding of who is responsible for responding to each question. It repeats the text in the source document and then provides the most appropriate and detailed answer possible to each question where Microsoft has sole or joint responsibility to respond. No responses to questions 1-13 are provided, as these are the sole responsibility of agencies to answer.

In some cases where it may be helpful to users of this document, Microsoft has provided a response to questions where it has no responsibility to do so.

Readers should note that, while the document should be helpful to both public and private sector organisations that are considering using Microsoft Office 365, it has been drafted with the needs of public sector organisations being of foremost importance.

Readers should also note that some of the answers are drafted on the assumption that the organisation making use of this document is an "Eligible Agency" under the terms of the Microsoft G2015 all-of-government agreement that is in place with the Department of Internal Affairs with the New Zealand Government.

Security and Privacy Considerations

This section describes the core considerations for any agency planning a deployment of a cloud computing service. Each area is described in some detail followed by a list of key considerations to assist agencies in developing an assessment of their risk position for a proposed service.

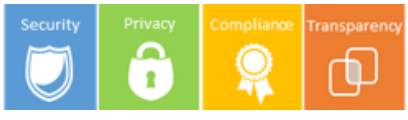
3.1 Value, Criticality and Sensitivity of Information

In order to be able to assess the risks associated with using a cloud service, agencies must recognise the value, criticality and sensitivity of the information they intend to place in the service.

Agencies are required to classify official information in accordance with the guidance published in 'Security in the Government Sector 2002 (SIGS)'. They are also required to protect official information in line with the guidance published in the 'New Zealand Information Security Manual (NZISM)'.

The under-classification of data could result in official information being placed in a cloud service that does not have appropriate security controls in place and therefore cannot provide an adequate level of protection. Conversely, over-classification could lead to unnecessary controls being specified leading to excessive costs resulting in suitable cloud services being rejected. Therefore it is critical that an agency accurately assesses the value, criticality and sensitivity of its data, and correctly classifies it to ensure that it is appropriately protected.

Consideration	Respondent
1. Who is the business owner of the information?	Customer
2. What are the business processes that are supported by the information?	Customer
3. What is the security classification of the information based on the NZ government guidelines for protection of official information?	Customer
4. Are there any specific concerns related to the confidentiality of the information that will be stored or processed by the cloud service?	Customer
5. Does the data include any personal information?	Customer
6. Who are the users of the information?	Customer
7. What permissions do the users require to the information? (i.e. read, write, modify and/or delete)	Customer
8. What legislation applies to the information? (e.g. Privacy Act 1993, Official Information Act 1982, Public Records Act 2005)	Customer
9. What contractual obligations apply to the information? (e.g. Payment Card Industry Data Security Standard (PCI DSS))	Customer
10. What would the impact on the business be if the information was disclosed in an unauthorised manner?	Customer
11. What would the impact on the business be if the integrity of the information was compromised?	Customer
12. Does the agency have incident response and management plans in place to minimise the impact of an unauthorised disclosure?	Customer
13. What would the impact on the business be if the information were unavailable?	
a. What is the maximum amount of data loss that can be tolerated after a disruption has occurred? This is used to define the Recovery Point Objective.	Customer
b. What is the maximum period of time before which the minimum levels of services must be restored after a disruption has occurred? This is used to define the Recovery Time Objective.	Customer
c. What is the maximum period of time before which the full service must be restored to avoid permanently compromising the business objectives? This is used to define the Acceptable Interruption Window.	Customer



3.2 Data Sovereignty

The use of cloud services located outside of New Zealand's jurisdiction, or owned by foreign companies, introduces data sovereignty risks. This means that any data stored, processed or transmitted by the service may be subject to legislation and regulation in those countries through which data is stored, processed and transmitted. Similarly, a foreign owned service provider operating a service within New Zealand may be subject to the laws of the country where its registered head offices are located.

The laws that could be used to access information held by the service provider vary from country to country. In some instances when a service provider is compelled by a foreign law enforcement agency to provide data belonging to their customers, they may be legally prohibited from notifying the customer of the request. Therefore it is critical that an agency identify the legal jurisdictions in which its data will be stored, processed or transmitted. Further, they should also understand how the laws of those countries could impact the confidentiality, integrity, availability and privacy of the information.

If the service provider outsources or sub-contracts any aspect of the delivery of the service to a third-party, agencies must also identify whether this introduces additional data sovereignty risks.

Privacy information that is held in legal jurisdictions outside of New Zealand may be subject to the privacy and data protection laws of the countries where the cloud service is delivered. Privacy and data protection laws can vary considerably from country to country. Therefore it is important that agencies assess how the laws of those countries could affect the privacy of their employees and/or customers' information.

Considerations	Respondent
14. Where is the registered head office of the service provider?	Microsoft
15. Which countries are the cloud services delivered from?	Microsoft
16. In which legal jurisdictions will the agency's data be stored and processed?	Microsoft
17. Does the service provider allow its customers to specify the locations where their data can and cannot be stored and processed?	Microsoft
18. Does the service have any dependency on any third parties (e.g. outsourcers, subcontractors or another service provider) that introduce additional jurisdictional risks? If yes, ask the service provider to provide the following details for each third party involved in the delivery of the service:	Microsoft
18a. The registered head office of the third party;	Microsoft
18b. The country or countries that their services are delivered from; and	Microsoft
18c. The access that they have to client data stored, processed and transmitted by the cloud service.	Microsoft
19. Have the laws of the country or countries where the data will be stored and processed been reviewed to assess how they could affect the security and/or privacy of the information?	Joint
20. Do the laws actually apply to the service provider and/or its customer's information? (e.g. some privacy laws exempt certain types of businesses or do not apply to the personal information of foreigners.)	Customer
21. Do the applicable privacy laws provide an equivalent, or stronger, level of protection than the Privacy Act 1993?	Joint
21a. If no, are customers able to negotiate with the service provider to ensure that the equivalent privacy protections are specified in the contract?	Microsoft
22. How does the service provider deal with requests from government agencies to access customer information?	Microsoft
22a. Do they only disclose information in response to a valid court order?	Microsoft
22b. Do they inform their customers if they have to disclose information in response to such a request?	Microsoft
22c. Are they prevented from informing customers that they have received a court order requesting access to their information?	Microsoft

Once agencies have identified the legal jurisdictions where their data will be held, they should assess whether or not it is appropriate to store their data in the service. This may require them to seek specialist legal and/or security advice. Agencies without access to specialist resources are encouraged to seek advice from the Government Chief Information Officer (GCIO).

Microsoft Responses

14. Where is the registered head office of the service provider?

Microsoft Corporation is headquartered in Redmond, Washington, USA. Microsoft Operations Pte Ltd is the service provider and its registered head office is in Singapore.

15. Which countries are the cloud services delivered from?

Microsoft Office 365 services will be provided to New Zealand Government customers from Microsoft's datacentre facilities located in Australia (Melbourne and Sydney).

16. In which legal jurisdictions will the agency's data be stored and processed?

Microsoft presumes that New Zealand public sector customers will choose to use the Office 365 service delivered from Australia, which will therefore be the jurisdiction in which their data will be stored and processed. However, customers should note that, in order to reliably provide the service, Microsoft does reserve the right to move customer data to other locations if necessary.

Microsoft's privacy commitment associated with this ability, as set out in the Microsoft Online Services Privacy Statement:

"Except as described below, Customer Data that Microsoft processes on your behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities. You appoint Microsoft to perform any such transfer of Customer Data to any such country and to store and process Customer Data in order to provide the Online Services. Microsoft abides by the EU Safe Harbor and the Swiss Safe Harbor frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union, the European Economic Area, and Switzerland. Some Online Services may provide additional commitments around keeping Customer Data in a specified geography. Please visit the Online Services Trust Center(s) or consult your agreement(s) for details."

For data location information specific to Office 365, customers should review the data location information available in the Office 365 Trust Centre.

17. Does the service provider allow its customers to specify the locations where their data can and cannot be stored and processed?

Yes. See answer to question 16 above.

18. Does the service have any dependency on any third parties (e.g. outsourcers, subcontractors or another service provider) that introduce additional jurisdictional risks?

Office 365 uses subcontractors to perform a variety of support services. Microsoft holds our subcontractors to security and privacy standards equivalent to our own. For an overview, see here.

Our subcontractors only handle your data when required to provide or maintain the services. In the interest of transparency, we let you know which subcontractors we use and what they do. An up-to-date list of these subcontractors is available here: http://go.microsoft.com/fwlink/?LinkId=213175&clcid=0x409.

Additionally, you can request that Microsoft share your Office 365 data with Microsoft partners, who are value-added service providers. Office 365 has a broad network of such partners, called delegated administrators or support partners. We provide you with tools to enable, disable, and monitor partner access and you can choose to give them account access so they can assist you in setting up or supporting your service. You can get more information on permissions in Office 365 here. Also, you can find out how to grant or remove partners' permission in Office 365 to access and administer your data here.

Finally, customers should understand that Office 365 services utilize Microsoft Azure platform services. Subcontractors assist with various aspects of Microsoft Azure platform services. A list of these subcontractors is available at any time from the Azure Trust Centre. This document identifies the subcontractors Microsoft uses, the service provided by the subcontractor and the area the subcontractor is from.

18. If yes, ask the service provider to provide the following details for each third party involved in the delivery of the service:

18a. The registered head office of the third party;

Microsoft does not publish information about the registered head offices of its subcontractors.

18b. The country or countries that their services are delivered from; and

Country of operation is set out in the various documents cited in the answer to question 18 above.

18c. The access that they have to client data stored, processed and transmitted by the cloud service.

In the Office 365 Trust Centre Microsoft states:

"Microsoft will only disclose your data to subcontractors so they can deliver the services we have retained them to provide.

Subcontractors are prohibited from using your data for any other purpose, and they are required to maintain the confidentiality of your information. Subcontractors that work in facilities or on equipment controlled by Microsoft must follow our privacy standards. All other subcontractors must follow privacy standards equivalent to our own." (see: http://www.microsoft.com/online/legal/v2/?docid=26&langid=en-us)

In addition, Microsoft's Online Service terms (OST) state:

"**Use of Subcontractors**. Microsoft may hire subcontractors to provide services on its behalf. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations in the OST. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the OST."

In addition, the Privacy section of the Data Processing Terms (DPT) incorporated in the OST states:

"**Subcontractor Transfer**. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Each Online Service has a website that lists subcontractors that are authorized to access Customer Data. At least 14 days before authorizing any new subcontractor to access Customer Data, Microsoft will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval."

19. Have the laws of the country or countries where the data will be stored and processed been reviewed to assess how they could affect the security and/or privacy of the information?

Microsoft presumes NZ Government customers will be using the O365 serviced delivered from Australia. Customers should seek their own legal advice to fully understand the laws of the country where the data will be stored and processed.

20. Do the laws actually apply to the service provider and/or its customer's information? (e.g. some privacy laws exempt certain types of businesses or do not apply to the personal information of foreigners.)

Customers should seek their own legal advice to fully understand the laws of the country where the data will be stored and processed.

21. Do the applicable privacy laws provide an equivalent, or stronger, level of protection than the Privacy Act 1993?

In Microsoft's view, the privacy laws in Australia provide similar protections to New Zealand's privacy laws in instances where they apply. In addition, with respect to law enforcement requests in Australia, in Microsoft's view there are appropriate due process requirements in place so as not to present any substantial risk of arbitrary or improper data disclosure requests by law enforcement or other government officials

21a. If no, are customers able to negotiate with the service provider to ensure that the equivalent privacy protections are specified in the contract?

No. Due to the inherent nature of a multi-tenant public cloud service customers cannot negotiate for specific privacy provisions beyond those that Microsoft provides to all its Office 365 customers.

22. How does the service provider deal with requests from government agencies to access customer information?

Microsoft's Online Service terms (OST) state:

"**Disclosure of Customer Data.** Microsoft will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) with permission from an end user, (3) as described in the OST, or (4) as required by law.

Microsoft will not disclose Customer Data to law enforcement unless required by law. Should law enforcement contact Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, then Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third party request for Customer Data (such as requests from Customer's end users), Microsoft will promptly notify Customer unless prohibited by law. If Microsoft is not required by law to disclose the Customer Data, Microsoft will reject the request. If the request is valid and Microsoft could be compelled to disclose the requested information, Microsoft will attempt to redirect the third party to request the Customer Data from Customer.

Except as Customer directs, Microsoft will not provide any third party: (1) direct, indirect, blanket or unfettered access to Customer Data; (2) the platform encryption keys used to secure Customer Data or the ability to break such encryption; or (3) any kind of access to Customer Data if Microsoft is aware that such data is used for purposes other than those stated in the request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party."

22a. Do they only disclose information in response to a valid court order?

Microsoft will only disclose information to law enforcement if required to do so by applicable law. We require a court order or warrant before we will consider releasing content. All our Principles, Policies and Practices regarding how we respond to criminal law enforcement requests and other government legal demands we receive for customer data are published here. We recommend that customers fully acquaint themselves with this information.

See also response to question 22 above.

22b. Do they inform their customers if they have to disclose information in response to such a request?

Yes. As set out in Microsoft's Online Service terms (OST), upon receipt of any other third party request for Customer Data (such as requests from Customer's end users), Microsoft will promptly notify Customer unless prohibited by law. If Microsoft is not required by law to disclose the Customer Data, Microsoft will reject the request. If the request is valid and Microsoft could be compelled to disclose the requested information, Microsoft will attempt to redirect the third party to request the Customer Data from Customer.

See also response to question 22 above.

22c. Are they prevented from informing customers that they have received a court order requesting access to their information?

In some cases, the terms of the court order may prevent Microsoft from informing customers of the court order. While particular orders may not be published, Microsoft does publish a six-monthly Law Enforcement Transparency Report to report on the number of disclosure requests and disclosures made against those requests.

See also response to question 22 above.

3.3 Privacy

Agencies planning to place personal information in a cloud service should perform a Privacy Impact Assessment (PIA) to ensure that they identify any privacy risks associated with the use of the service together with the controls required to effectively manage them.

Cloud services may make it easier for agencies to take advantage of opportunities to share information. For example, sharing personal information with another agency may be achieved by simply creating user accounts with the appropriate permissions within a SaaS solution rather than having to implement a system-to-system interface to exchange information. Although cloud services have the potential to lower the technical barriers to information sharing, agencies must ensure that they appropriately manage access to personal information and comply with the requirements of the Privacy Act 1993.

Service providers typically use privacy policies to define how they will collect and use personal information about the users of a service. US service provider's privacy policies usually distinguish between Personally Identifiable Information (PII) and non-personal information. However, it is important to note that both are considered personal information under the Privacy Act 1993.

Agencies must carefully review and consider the implications of accepting a service provider's privacy policy.

In addition to this, the Office of the Privacy Commissioner (OPC) has published guidance for small to medium organisations that are considering placing personal information in a cloud service. Agencies are encouraged to review and ensure that they understand the guidance.

Considerations	Respondent
23. Does the data that will be stored and processed by the cloud service include personal information as defined in the Privacy Act 19939? If no, skip to question 28.	Customer
24. Has a PIA been completed that identifies the privacy risks associated with the use of the cloud service together with the controls required to effectively manage them?	Customer
25. Is the service provider's use of personal information clearly set out in its privacy policy?	Joint
25a. Is the policy consistent with the agency's business requirements?	Customer
26. Does the service provider notify its customers if their data is accessed by, or disclosed to, an unauthorised party?	Microsoft
26a. Does this include providing sufficient information to support cooperation with an investigation by the Privacy Commissioner?	Customer
27. Who can the agency, its staff and/or customers complain to if there is a privacy breach?	Microsoft

Microsoft Responses

23. Does the data that will be stored and processed by the cloud service include personal information as defined in the Privacy Act 1993? If no, skip to question 28.

This question is for customers to answer.

24. Has a PIA been completed that identifies the privacy risks associated with the use of the cloud service together with the controls required to effectively manage them?

This question is for customers to answer.

25. Is the service provider's use of personal information clearly set out in its privacy policy? Is the policy consistent with the agency's business requirements?

Customers can review the Microsoft Online Services Privacy Statement, which applies to Office 365. The current version of this privacy statement (which is updated from time to time) sets out the following types and uses of information:

Customer Data: used to provide the Services (including troubleshooting, detecting and preventing malware etc.)

Administrator Data: used to complete the customer's requested transactions, administer accounts, improve the Services and detect and prevent fraud.

Payment Data: used to complete customer transactions, as well as for the detection and prevention of fraud.

Support Data: used to provide the support services, resolve your support incident and for training purposes.

Cookies and other information: used for storing users' preferences and settings, for fraud prevention, to authenticate users and to collect operational information about the Services.

In regard to Customer Data, the privacy statement says:

"Customer Data will be used only to provide customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. "Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, you or your end users through use of the Online Service. Customer Data is not Administrator Data, Payment Data or Support Data.

For more information about the features and functionality that enable you and your end users to control Customer Data, please review documentation specific to the service. Microsoft also makes a number of data protection commitments in our customer agreement (see the Online Services Terms or other applicable terms for details)."

Customers may also be interested in reading Microsoft's whitepaper entitled "Protecting Data and Privacy in the Cloud".

25a. Is the service provider's use of personal information clearly set out in its privacy policy?

Yes. Personal Informational falls within the scope of "Customer Data" which is handled in accordance with the arrangements referenced in the answer to question 25 above.

26. Does the service provider notify its customers if their data is accessed by, or disclosed to, an unauthorised party?

As set out in the answer to question 22 above, if Microsoft is legally compelled to disclose customer data to law enforcement it will notify the customer unless legally prohibited from doing so.

Otherwise, in regard to any possible instance of unlawful access to Customer Data, Microsoft's Online Service terms (OST) state:

"**Security Incident Notification.**

If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service."

26a. Does this include providing sufficient information to support cooperation with an investigation by the Privacy Commissioner?

The question of whether the measures outlined in response to question 26 above would provide information that would be sufficient to allow cooperation with an investigation by the Privacy Commissioner can only be answered *ex post* on a case-by-case basis.

27. Who can the agency, its staff and/or customers complain to if there is a privacy breach?

Microsoft's Online Service terms (OST) state:

"**How to Contact Microsoft**

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form. Microsoft's mailing address is:

Microsoft Enterprise Service Privacy
Microsoft Corporation
One Microsoft Way

Also, to report suspected security issues or abuse of Office 365, customers can contact the cert.microsoft.com team, which is available 24x7.

3.4 Governance

3.4.1 Terms of Service

Cloud computing is essentially a form of outsourcing and like all outsourcing arrangements, it introduces governance challenges. However, unlike traditional outsourcing models it may not always be possible for customers to fully negotiate all contract terms with the service provider, especially in the case of public cloud services (e.g. Google Apps, Microsoft Office 365, Amazon Web Services).

The primary governance control available to agencies is the service provider's Terms of Service (or contract), the associated Service Level Agreement (SLA) and Key Performance Indicators and metrics demonstrating the service performance. These must be carefully reviewed to ensure that the service can meet the agency's obligations to protect the confidentiality, integrity and availability of its official information and the privacy of all personally identifiable information it intends to place within it.

To be able to exercise any level of control over the data that is held in the cloud service, agencies must maintain ownership of their data and know how the service provider will use the data when delivering the service. Service providers may use customers' data for their own business purposes (e.g. for generating revenue by presenting targeted advertising to users or collecting and selling statistical data to other organisations). Although the use of customer data is usually limited to consumer rather than enterprise contracts it is important to determine whether the service provider will use the data for any purpose other than the delivery of the service. Therefore, the service provider's Terms of Service must be reviewed to ensure that they clearly define the ownership of data, how it will be used in the delivery of the service and whether the service provider will use it for any purpose other than the delivery of the service.

It is not uncommon for a service provider to rely on components from other service providers. For example, a SaaS service may be hosted on an IaaS offering from a different provider. It is essential to identify any dependencies that the service provider has on third-party services to gain a complete understanding of the risks introduced through the adoption of a service.

Considerations	Respondent
28. Does the service provider negotiate contracts with their customers or must they accept a standard Terms of Service?	Microsoft
29. Does the service provider's Terms of Service and SLA clearly define how the service protects the confidentiality, integrity and availability of official information and the privacy of all personally identifiable information?	Microsoft
30. Does the service provider's Terms of Service specify that the agency will retain ownership of its data?	Microsoft
31. Will the service provider use the data for any purpose other than the delivery of the service?	Microsoft
32. Is the service provider's service dependent on any third-party services?	Microsoft

Microsoft Responses

28. Does the service provider negotiate contracts with their customers or must they accept a standard Terms of Service?

Microsoft and the New Zealand Government (contracting through the New Zealand Department of Internal Affairs) have negotiated and entered into the G2015 Framework Agreement. "Eligible Agencies" under the G2015 Framework Agreement would license Office 365 pursuant to the terms of the G2015 Framework Agreement, which include the Microsoft Online Services Terms.

29. Does the service provider's Terms of Service and SLA clearly define how the service protects the confidentiality, integrity and availability of official information and the privacy of all personally identifiable information?

Yes. The Data Processing Terms incorporated into Microsoft's Online Service terms (OST) detail the various steps taken by Microsoft to protect the confidentiality and integrity of data (including, for example, the appointment of security officers, the various independent certifications and detail of the internal processes to protect and maintain data).

Customers will be pleased to know that the Data Processing Terms also include the "Standard Contractual Clauses," pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the EU Data Protection Directive. Microsoft's implementation of the Standard Contractual Clauses has been endorsed by Data Protection Authorities across the EU as evidenced here: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf

Customers should also be pleased to note that that, as part of its certification of compliance with ISO/IEC 27001:2013, Office 365 complies with the requirements of the new standard ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

In addition, Microsoft recommends that customers review the document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements"

Finally, Microsoft suggests that customers familiarise themselves with the Office 365 Service Description.

30. Does the service provider's Terms of Service specify that the agency will retain ownership of its data?

Yes. Microsoft's Online Service terms (OST) state:

"**Use of Customer Data.** Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer."

31. Will the service provider use the data for any purpose other than the delivery of the service?

No. See answer to question 30 above.

Also, customers should note that as part of its certification of compliance with ISO/IEC 27001:2013, Office 365 complies with the requirements of the new standard ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

In particular, ISO/IEC 27018:2014 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

ISO/IEC 27018:2014 is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

The guidelines in ISO/IEC 27018:2014 might also be relevant to organizations acting as PII controllers; however, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. ISO/IEC 27018:2014 is not intended to cover such additional obligations.

32. Is the service provider's service dependent on any third-party services?

For some components in Office 365 Microsoft makes use of third parties. Customers can download lists of these subcontractors using the links provided in the response to question 18 above. Third party components are included in the audits conducted on the Office 365 service.

3.4.2 Compliance

The NZISM advises agencies to formally assess and certify that their information systems have been deployed with sufficient controls to protect the confidentiality, integrity and availability of the information they store, process and transmit before accrediting them for use.

As discussed, it may not be possible for customers to negotiate the terms of the contract with a service provider. As a result, an agency may not be able to stipulate any specific security controls to protect its data, or to directly verify that the service provider has sufficient controls in place to protect its data. Even if it is possible to directly verify that a service provider has controls, it may not actually be practical to do so if the service is hosted in a data centre outside New Zealand. Therefore customers must typically rely on the service provider commissioning a third-party audit.

Agencies need to consider which certifications are useful and relevant, and whether or not they increase their confidence in the service provider's ability to protect their information. It is essential that an agency understand if certification to an internationally recognised standard or framework provides any assurance that the service provider meets its security requirements. For example, the Statement for Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II allows the service provider to limit the scope of the audit. Similarly, service providers that are certified as being compliant with the requirements defined in ISO/IEC 27001 are able to define the scope of the audit using a Statement of Applicability. Therefore agencies need to check exactly what controls are covered by the audit by asking the service provider for a copy of the latest external auditor's report (including the scope or Statement of Applicability), and the results of all recent internal audits.

Access to information related to audits varies amongst service providers. Some are willing to provide customers (including potential customers) with full audit reports under a non-disclosure and confidentiality agreement. Whereas others will only provide the certificate to demonstrate that they have passed the audit. The more transparent the service provider is, the easier it is for agencies to assess if the provider has suitable security practices and controls in place to meet their requirements.

Another potential source of information relating to the security controls that a service provider has in place is the Cloud Security Alliance's Security, Trust & Assurance Register (CSA STAR). The level of assurance provided depends on the level that the service provider has achieved on the CSA's Open Certification Framework (OCF).

The first level is self-assessment. To achieve this, service providers submit a completed Consensus Assessments Initiative Questionnaire (CAIQ) or Cloud Controls Matrix (CMM) report that asserts their compliance with the CSA cloud security controls. While these reports can provide agencies with an insight into the service provider's security controls and practices, the CSA only verifies authenticity of the submission and performs a basic check of the accuracy of its content before adding it to the registry. The CSA does not guarantee the accuracy of any entries. As a result, the fact that a provider is listed on the CSA STAR Self-Assessment is an indication that the provider has sought to assert some level of diligence with a registration

body but does not actually provide any assurance that they have adequate security practices or controls in place.

The second levels are CSA STAR Certification and Attestation. To achieve these levels service providers undergo third party auditing by an approved Certification Body. The CSA STAR Certification is based on ISO/IEC 27001 and the controls specified in the CMM. The maturity of the service provider's Information Security Management System (ISMS) is assessed and given a rating (i.e. Bronze, Silver or Gold) if they are found to have adequate processes in place. Similarly, the CSA STAR Attestation is based on SSAE 16 SOC 2 Type II and is supplemented by the criteria defined in the CMM. The service providers are regularly assessed based on the controls that they assert are in place and their description of the service.

The third level is continuous monitoring and assessment of the cloud service's security properties using the CMM and the CSA's Cloud Trust Protocol (CTP). This is currently in development and is not anticipated to be available until 2015. The goal of CSA STAR Continuous is provide on-going assurance about the effectiveness of the service provider's security management practices and controls.

The Institute of Information Technology Practitioners (IITP) has published the New Zealand Cloud Computing Code of Practice11 that provides a standardised method for New Zealand based service providers to voluntarily disclose information about the security of their service(s). The Cloud Code is designed to ensure that service providers are transparent in the positioning of their services to their clients. However, it does not provide any specific assurance that they have adequate security practices or controls in place. Therefore, an agency should only use the Cloud Code for informational purposes and should not rely on it to replace its own due diligence.

When relying on certification performed by another party (e.g. a third-party auditor or another government agency) it is important for agencies to understand the scope and limitations of the certification and to assess whether they need to perform further assurance activities. For example, agencies deploying services on one of the approved government IaaS platforms must perform a certification and accreditation review of the components they implement as part of their project (e.g. guest operating systems and applications).

Considerations	Respondent
33. Does the service provider's Terms of Service allow the agency to directly audit the implementation and management of the security measures that are in place to protect the service and the data held within it?	Microsoft
33a. If yes, does this include performing vulnerability scans and penetration testing of the service and the supporting infrastructure?	Microsoft
33b. If no, does the service provider undergo formal regular assessment against an internationally recognised information security standard or framework by an independent third-party? (E.g. are they certified as being compliant with ISO/IEC 27001? Have they undergone an ISAE 3402 SOC 2 Type II?)	Microsoft
34. Will the service provider allow the agency to thoroughly review recent audit reports before signing up for service? (E.g. will the service provider provide the Statement of Applicability together with a copy of the full audit reports from their external auditor, and the results of any recent internal audits?)	Microsoft
35. Will the service provider enable potential customers to perform reference checks by providing the contact details of two or more of its current customers?	Microsoft
36. Is there a completed CAIQ or CMM report for the service provider in the CSA STAR?	Microsoft
37. Has the service provider undergone a CSA STAR Certification and/or Attestation?	Microsoft
37a. Have they published the outcome of the audit?	Microsoft
38. Has the service provider published a completed Cloud Computing Code of Practice?	Microsoft
39. What additional assurance activities must be performed to complete the certification and accreditation of the cloud service?	Customer

Microsoft Responses

33. Does the service provider's Terms of Service allow the agency to directly audit the implementation and management of the security measures that are in place to protect the service and the data held within it?

No. For operational and security reasons Microsoft does not permit a customer to directly audit the implementation and management of security measures associated with Office 365. Allowing potentially thousands of customers to audit our services would not be a scalable practice and might compromise security and privacy.

The audits conducted on Office 365 cover all aspects of the service related to the storage, access, and operation of customer data. These aspects align with all 14 ISO domains:

1) General Information
2) Information Security
3) Organization of Information Security;
4) Asset Management
5) Human Resources Security
6) Physical and Environmental Security
7) Communications and Operations Management
8) Access Control
9) Information Systems Acquisition, Development, and Maintenance
10) Information Security Incident Management
11) Business Continuity Management
12) Risk Management
13) Compliance
14) Privacy.

Specific details on the scope of these audit controls are included in the "ISO Statement of Applicability" (available under NDA from the customer's account or support representative), and in the audit reports themselves.

The Microsoft Online Services Bug Bounty (BB) program operates a policy of allowing limited, Customer originated, vulnerability assessments on Office 365 ("Penetration Tests"). These vulnerability assessments can be performed, provided Customer is in full compliance with the rules governing external vulnerability testing of Office 365.

33a. If yes, does this include performing vulnerability scans and penetration testing of the service and the supporting infrastructure?

As noted in question 32 above, the Microsoft Online Services Bug Bounty (BB) program operates a policy of allowing limited, Customer originated, vulnerability assessments on Office 365 ("Penetration Tests"). These vulnerability assessments can be performed, provided Customer is in full compliance with the rules governing external vulnerability testing of Office 365.

Customers may also be interested in reading the document entitled "Microsoft Enterprise Cloud Red Teaming". Finally, Microsoft recommends that customers review the document entitled "Security in Office 365".

33b. If no, does the service provider undergo formal regular assessment against an internationally recognised information security standard or framework by an independent third-party? (E.g. are they certified as being compliant with ISO/IEC 27001? Have they undergone an ISAE 3402 SOC 2 Type II?)

Yes. By providing customers with compliant, independently verified cloud services, Microsoft makes it easier for customers to meet their own compliance obligations. To best understand Microsoft's overall approach to compliance, we suggest that customers also review the document entitled "Microsoft Compliance Framework for Online Services".

Microsoft provides customers with detailed information about our security and compliance programs, including audit reports and compliance packages, to help customers assess our services against their own legal and regulatory requirements. In addition, Microsoft has developed an extensible compliance framework that enables it to design and build services using a single set of controls to speed up and simplify compliance across a diverse set of regulations and rapidly adapt to changes in the regulatory landscape.

ISO/IEC 27001:2013 Audit and Certification

Office 365 is certificated against ISO/IEC 27001:2013, a broad international information security standard. The ISO/IEC 27001:2013 certificate validates that Microsoft has implemented the internationally recognized information security controls defined in this standard, including guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

The certificate issued by the British Standards Institution (BSI) is publically available here.

As part of its certification of compliance with ISO/IEC 27001:2013, Office 365 complies with the requirements of the new standard ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors (see answer to question 31).

SOC 1 SSAE 16/ISAE 3402 Attestation

Office 365 has been audited against the Service Organization Control (SOC) reporting framework for SOC 1 Type 2. The SOC 1 Type 2 audit report attests to the design and operating effectiveness of controls. Audits are conducted in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB).

SOC 2 Type 1 and/or Type 2 Attestation (AT Section 101)

Office 365 has been audited against the Service Organization Control (SOC) reporting framework for SOC21 Type 2. SOC 2 audits are conducted in accordance with AT Section 101 standard established by AICPA and based on trust services principles and criteria. The purpose is to report on controls relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy trust principles. Cloud Service Providers must follow control requirements specified in AT 101, e.g., there is no flexibility in choosing a control set afforded by SOC 1 audit. Some trust principles may not be applicable depending on the nature of the cloud service (IaaS vs. PaaS vs. SaaS). The resulting SOC 2 audit report can be shared with customers under NDA.

European Union Safe Harbour

Microsoft (including, for this purpose, all of our US subsidiaries) is Safe Harbour certified under the US Department of Commerce. The underlying law is the European Commission Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour privacy principles. In addition to the EU Member States, members of the European Economic Area (Iceland, Liechtenstein, and Norway) also recognize organizations certified under the Safe Harbour program as providing adequate privacy protection to justify

trans-border transfers from their countries to the US. Switzerland has a nearly identical agreement ("Swiss-US Safe Harbour") with the US Department of Commerce to legitimize transfers from Switzerland to the US, to which Microsoft has also certified.

The Safe Harbour certification allows for the legal transfer of E.U. personal data outside E.U. to Microsoft for processing. Under the E.U. Data Protection Directive (95/46/EC), which sets a baseline for handling personal data in the EU, Microsoft acts as the data processor, whereas the customer is the data controller with the final ownership of the data and responsibility under the law for making sure that data can be legally transferred to Microsoft. It is important to note that Microsoft will transfer E.U. Customer Data outside the E.U. only under very limited circumstances.

European Union Model Contract Clauses (EUMC)

EU Model Clauses are contractual addendums offered to EU customers requiring additional safeguards for the protection of personal data beyond Safe Harbour Framework. The underlying law is the European Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data under the EU Data Protection Directive (95/46/EC). Model Clauses include additional security and notice requirements that a cloud service provider is willing to contractually commit to in order to support customers. When included in service agreements with data processors, the Model Clauses assure customers that appropriate steps have been taken to help safeguard personal data, even if data is stored in a cloud-based service centre located outside the European Union.

The European Union's data protection authorities have found that Microsoft's enterprise cloud contracts meet the high standards of EU privacy law. This ensures that our customers can use Microsoft services to move data freely through our cloud from Europe to the rest of the world. Via Microsoft's Online Service Terms (OST) we expand these legal protections to benefit all of our enterprise customers around the world.

The EU's 28 data protection authorities have acted through their "Article 29 Working Party" to provide this approval via a joint letter. Importantly, Microsoft is the first – and so far the only – company to receive this approval. This recognition applies to Microsoft's enterprise cloud services – in particular, Microsoft Azure, Office 365, Microsoft Dynamics CRM and Windows Intune.

Additional compliance:

In addition to the above, Office 365 has been audited, accredited, or otherwise meets the requirements of:

- United Kingdom G-Cloud IL2 Accreditation
- Health Information Portability and Accountability Act (HIPAA) Business Associate Agreement (BAA)
- Family Educational Rights and Privacy Act (FERPA)

34. Will the service provider allow the agency to thoroughly review recent audit reports before signing up for service? (E.g. will the service provider provide the Statement of Applicability together with a copy of the full audit reports from their external auditor, and the results of any recent internal audits?)

Customers can contact their account representative to request a copy of the ISO/IEC 27001:2013, SOC 1 Type 2 and SOC 2 Type 2 external audit reports for Office 365. Also, copies of these audit reports have been provided to the NZ Government CIO under NDA. Customers should note that Microsoft does not disclose internal audit results.

35. Will the service provider enable potential customers to perform reference checks by providing the contact details of two or more of its current customers?

Yes. Microsoft provides for reference check opportunities. Please contact your account representative for more information.

36. Is there a completed CAIQ or CMM report for the service provider in the CSA STAR?

Yes. As an "Executive Member" of the CSA Microsoft has published a self-assessment for Office 365 in relation to the CSA CCM. A copy can be downloaded here.

37. Has the service provider undergone a CSA STAR Certification and/or Attestation?

No. This would be redundant given Office 365's SOC attestations, and ISO audits and FISMA audits.

37a. Have they published the outcome of the audit?

Not applicable.

38. Has the service provider published a completed Cloud Computing Code of Practice?

No. As a global provider of public cloud services it is not feasible for Microsoft to become a signatory to the NZ Cloud Computing Code of Practice ("the Code"). Even if it were, due to the existing Privacy, Security and Compliance frameworks Microsoft already adheres to on a global basis, we do not believe becoming a signatory to the Code would add any benefit to its customers.

39. What additional assurance activities must be performed to complete the certification and accreditation of the cloud service?

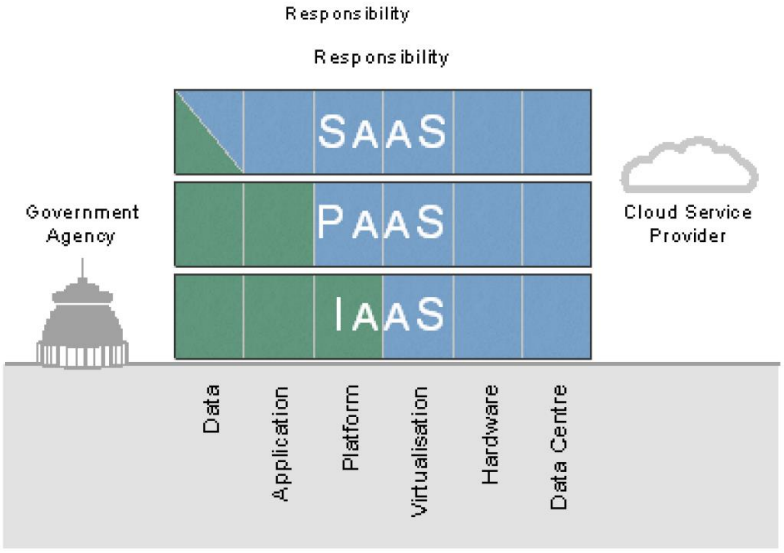
This question is for customers to answer.

3.5 Confidentiality

There are many factors that may lead to unauthorised access to, or the disclosure of, information stored in a cloud service. However, it is important to note that the vast majority of these are not unique to cloud computing.

As highlighted in Figure 1 the cloud service model (i.e. IaaS, PaaS or SaaS) will determine which party is responsible for implementing and managing the controls to protect the confidentiality of the information stored, processed or transmitted by the service. Similarly, the cloud deployment model (i.e. public, private, community or hybrid) will affect a customer's ability to dictate its control requirements.

Figure 1



3.5.1 Authentication and Access Control

An agency may find that as its use of cloud services increases so will the identity management overhead. The adoption of multiple cloud services may place an unacceptable burden on users if the agency does not have an appropriate identity management strategy. For example, each cloud service that is adopted could result in users requiring another username and password. A discussion of the approaches to identity management is beyond the scope of this document. However, agencies are encouraged to develop an approach to identity and access management that supports their adoption of cloud services, by both their employees and customers. This should include consideration of the security implications and risks.

The broad network access characteristic of cloud computing amplifies the need for agencies to have strong identity lifecycle management practices. This is because users can typically access the information held in a cloud service from any location, which could present a significant risk as employees or contractors may still be able access the service after they have ceased to be employed. Therefore agencies should maintain a robust process for managing the lifecycle of identities that ensures:

- Permissions are approved at the appropriate level within the organisation.
- Role Based Access Control (RBAC) is sufficiently granular to control permissions.
- Users are only granted the permissions they require to perform their duties.
- Users do not accumulate permissions when they change roles within the organisation.
- User accounts are removed in a timely manner when employment is terminated.

In addition, agencies should regularly audit user accounts and the permissions granted to the accounts within the cloud services they have adopted to ensure that redundant accounts are removed and that users continue to only be granted the permissions they require to perform their duties.

Ubiquitous access also means that users can access the information held in the cloud service from any location using many different devices. Agencies must carefully consider the associated information security implications and assess what controls are required to adequately protect their information. For example, an agency adopting a SaaS based Customer Relationship Management (CRM) solution may determine that it needs to restrict access to specific features and functionality (e.g. downloading customer records or saving reports) when users access the service from outside the agency's premises or using a non-agency owned and managed device.

Another area of concern when adopting cloud services is whether passwords provide a sufficient level of assurance that the person authenticating to the service is the owner of the user account. Agencies must determine whether they require a stronger authentication mechanism (e.g. multifactor authentication) that provides sufficient confidence that the party asserting the identity is the authorised user.

Considerations	Respondent
40. Does the agency have an identity management strategy that supports the adoption of cloud services?	Joint
40a. If yes, does the cloud service support the agency's identity management strategy?	Customer
41. Is there an effective internal process that ensures that identities are managed throughout their lifecycle?	Joint
42. Is there an effective audit process that is actioned at regular intervals to ensure that user accounts are appropriately managed?	Joint
43. Have the controls required to manage the risks associated with the ubiquitous access provided by the cloud been identified?	Joint
44. Does the cloud service meet those control requirements?	Customer
45. Is there a higher level of assurance required that the party asserting an identity is the authorised user of the account when authenticating to the service? (I.e. is multi-factor authentication necessary?)	Joint

Microsoft Responses

40. Does the agency have an identity management strategy that supports the adoption of cloud services? If yes, does the cloud service support the agency's identity management strategy?

This question is for customers to answer.

40a. If yes, does the cloud service support the agency's identity management strategy?

The underlying identity platform for Office 365 is Microsoft Azure Active Directory. Customers should see the link for responses to a range of frequently asked questions regarding Office 365 identity management. This question is for customers to answer.

41. Is there an effective internal process that ensures that identities are managed throughout their lifecycle?

In regard to Microsoft's internal identity management practices, customers are advised to review the document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements". Specifically, customer should note the following responses:

- **SA-02: Security Architecture - User ID Credentials**

"Office 365 uses Active Directory to manage enforcement of our password policy. Office 365 systems are configured to force users to use complex passwords. As appropriate, customers must configure account setup and deletion; password complexity, expiry and history; account lockout; and/or online user IDs.

Password handling requirements include the changing of Contractor supplied default passwords prior to introducing the associated service or system into any Office 365 owned or operated environment.

“User password management and user registration” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 11.2.1 and 11.2.3. For more information review of the publicly available ISO standards we are certified against is suggested.”

- **SA-11: Security Architecture - Shared Networks**

Office 365 has procedures as well as automated and semi-automated systems for granting and revoking access to the servers in the "Managed" domain which contain user’s apps and data as well as servers in the "Management" domain which provides systems management functions (e.g., monitoring, backup, troubleshooting, software and patch mgmt.). The people in the Office 365 "Access and Identity" group manage access via Microsoft Active Directory to the "Managed" and "Management" domains. Authority is granted under the "Least Privilege Access" principle by the Service Managers in each area. Office 365 users of production systems are restricted to only one User ID per system.

Office 365 ensures that access control and credential management systems are designed and operated to comply with Office 365 policies and standards. Office 365’ key controls related to Identity and Access management are formally audited annually through the SSAE-16 audit for Office 365 and GFS. In addition, these controls are internally assessed for compliance with Office 365 policies and standards.

“Network security management and user access management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 10.6 and 11.2. For more information review of the publicly available ISO standards we are certified against is suggested.” In particular, customers should note the following in regard to Microsoft Office 365’s ISO 27001 audit documentation:

- **A.11.02.01 User registration**

The standard asks “Is there a formal user registration and de-registration procedure in place for granting and revoking access to information systems and services?”

Our response states: “The O365 Multi-Tenant (MT) Security Policy contains rules and requirements that must be met in the delivery and operation of O365 MT. More detailed requirements are established within O365 MT Security Procedures and service team-specific standard operating procedures (SOPs). These standards and procedures act as adjuncts to the security policy and provide implementation level details to carry out specific operational tasks.

Office 365 Security Policy prohibits the use of guest/anonymous and temporary accounts. In the case of the built-in guest account that is created by Windows, that account is disabled prior to deployment. All account requests go through the standard account management process.

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.

Terminated users are removed from Corp AD; as the regular AD sync occurs, this also removes them from service team AD. Additionally, service team management is notified of terminations and transfers and removes users as needed.

From a people and process standpoint, presume breach involves zero standing permission for administrators in the service, “Just-In-Time (JIT) access and elevation” (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service. An access approver role reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed."

• A.11.02.02 Privilege management

The standard askes "Is allocation and use of privileges restricted and controlled?"

Our response states: "Service teams require all individuals with administrative privileges to use their assigned accounts for performing business and administrative functions in the production environment. Office 365 Services requires that users of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions. AD uses Role Based Access Control (RBAC) to enforce the separation of privileged and non-privileged roles."

42. Is there an effective audit process that is actioned at regular intervals to ensure that user accounts are appropriately managed?

In regard to those aspects of Office 365 identity management that are the responsibility of Microsoft, yes. See answer to question 41. Customers should also note that they control access by their own users and are responsible for ensuring appropriate review of such access.

43. Have the controls required to manage the risks associated with the ubiquitous access provided by the cloud been identified?

See answers to questions 40.a, 41 and 42 above

44. Does the cloud service meet those control requirements?

This question is for customers to answer.

45. Is there a higher level of assurance required that the party asserting an identity is the authorised user of the account when authenticating to the service? (I.e. is multi-factor authentication necessary?)

Office 365 supports multi-factor authentication. This is enabled through Azure Active Directory which is the underlying authentication platform for Office 365. For more information on multi-factor authentication with Azure Active Directory, please see here. For details of how multi-factor authentication for Office 365 works for customers, see here.

In regard to Microsoft's internal use of multi-factor authentication, the document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements" states:

"**• SA-07: Security Architecture - Remote User Multi-Factor Authentication**

Access to the Office 365 production environments by staff and contractors is tightly controlled.

• Terminal Services servers are configured to use the high encryption setting.

• Microsoft Users have an Office 365 issued smartcard with a valid certificate and a valid domain account to establish a remote access session. The use of digital certificates or RSA tokens further strengthens control.

"Microsoft User authentication for external connections" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.4.2. For more information review of the publicly available ISO standards we are certified against is suggested".

3.5.2 Multi-Tenancy

The resource pooling characteristic of cloud computing means that cloud services typically use some form of multi-tenancy. This enables service providers to deliver services at a lower cost than traditional delivery models by allowing multiple customers (tenants) to share the same compute resources and/or instance of an application. While resource pooling and sharing has obvious benefits in terms of costs it does introduce security risks that must be understood by agencies wishing to leverage the benefits of cloud computing. The risks associated with multi-tenancy are typically related to either infrastructure virtualisation or data commingling.

Virtualisation is a key technology in the delivery of cloud services as it enables information systems to be abstracted from the underlying hardware using a hypervisor (i.e. software that enables a host server to run multiple guest operating systems concurrently). The most often cited area of concern within a virtualised environment is that a malicious party could exploit a vulnerability within the hypervisor to gain access to another customers' information (e.g. by performing a 'guest-to-host' or 'guest-to-guest' attack).

Virtualisation has made it easy to take a snapshot (i.e. a copy of a running server's memory and disk at a point in time for backup and redundancy purposes). If the snapshots are not appropriately protected, a malicious party may be able to gain unauthorised access to the information stored on the virtual machine's local drives and all encryption keys and data stored in memory. As a result, the service provider's architecture, implementation and ongoing management and monitoring of the virtualisation environment together with their patch and vulnerability management practices are key to ensuring the security of information stored and processed within the cloud service.

Another common concern in IaaS and PaaS environments is that the customer with the weakest security practices and controls may determine the security of the entire environment (the lowest common denominator problem). For example, a co-tenant that does not harden its operating systems and applications could define the security of the environment to the lowest common denominator if there are not appropriate controls in place to isolate customer's virtual machines and networks from each other.

SaaS and PaaS services use logical controls within the application or platform and supporting infrastructure to isolate access to each customer's data. However, the data is usually commingled within the application, database and back-up media. This places complete reliance on the quality of the design, implementation and enforcement of access controls within the platforms and applications.

The on-demand self-service characteristic of cloud computing introduces security concerns because the registration processes to become a customer are not always robust in confirming a customer's identity (i.e. web-based self-registration). This weakness can allow a malicious party to register for a service to then use it for malicious or fraudulent activities that may include attempting to subvert the access controls to gain unauthorised access to another customer's data.

An agency must be sufficiently assured that other customers using a cloud service cannot subvert the service provider's controls to gain access to its data. As discussed, this can be difficult as the "as a service" nature of cloud computing often means a lack of transparency regarding the security controls and practices that the service provider has in place to protect their customers' data. Consequently there is again a strong dependency on third-party audit reports and penetration testing.

Considerations	Respondent
46. Will the service provider allow the agency to review a recent third-party audit report (e.g. ISO 27001 or ISAE 3402 SOC 2 Type II) that includes an assessment of the security controls and practices related to virtualisation and separation of customer's data?	Microsoft
47. Will the service provider permit customers to undertake security testing (including penetration tests) to assess the efficacy of the access controls used to enforce separation of customer's data?	Microsoft
48. Does the service provider's customer registration processes provide an appropriate level of assurance in line with the value, criticality and sensitivity of the information to be placed in the cloud service?	Joint

Microsoft Responses

46. Will the service provider allow the agency to review a recent third-party audit report (e.g. ISO 27001 or ISAE 3402 SOC 2 Type II) that includes an assessment of the security controls and practices related to virtualisation and separation of customer's data?

Office 365 is a highly scalable multi-tenant service, which means that your data securely shares the same hardware resources as other customers. We have designed Office 365 to host multiple customers in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through Active Directory and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates your data using security boundaries. This safeguards your data so that the data cannot be accessed or compromised by co-tenants. For more information about how Microsoft secures Office 365 tenants' data, we recommend customers review the white paper entitled "Security and Compliance - Office 365".

In addition, Microsoft also advises customers to review the document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements" which states:

• SA-09: Security Architecture – Segmentation

"The networks within the Office 365 datacenters are designed to create multiple separate network segments. This segmentation helps to provide physical separation of critical, back-end servers and storage devices from the public-facing interfaces. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft datacenter. These connections established between customers and Microsoft datacenters are encrypted using industry-standard Transport Layer Security (TLS) /Secure Sockets Layer (SSL). The use of TLS/SSL effectively establishes a highly secure browser-to-server connection to help provide data confidentiality and integrity between the desktop and the datacenter. Filtering routers at the edge of the Office 3+D7465 network provides security at the packet level for preventing unauthorized connections to Office 365 Services.

Data storage and processing is logically segregated among customers of the same service through Active Directory® structure and capabilities specifically developed to help build, manage, and secure multitenant environments.

The multitenant security architecture ensures that customer data stored in shared Office 365 datacenters is not accessible by or compromised to any other organization. Organizational Units (OUs) in Active Directory control and prevent the unauthorized and unintended information transfer via shared system resources. Tenants are isolated from one another based on security boundaries, or silos, enforced logically through Active Directory.

"Security of network services" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.6.2. For more information review of the publicly available ISO standards we are certified against is suggested."

47. Will the service provider permit customers to undertake security testing (including penetration tests) to assess the efficacy of the access controls used to enforce separation of customer's data?

As of September 23rd 2014 we added the Microsoft Online Services Bug bounty (BB) program to the very exhaustive security toolset in place for Office 365. This program operates a policy of allowing limited, Customer originated, vulnerability assessments on Office 365 ("Penetration Tests"). These vulnerability assessments can be performed, provided Customer is in full compliance with the rules governing external vulnerability testing of Office 365.

48. Does the service provider's customer registration processes provide an appropriate level of assurance in line with the value, criticality and sensitivity of the information to be placed in the cloud service?

This question is for customers to answer. Microsoft recommends that customers review the information regarding secure end-user access contained in the document entitled "Security and Compliance - Office 365".

3.5.3 Standard Operating Environments

Although not unique to cloud computing it is important to acknowledge that one of the biggest causes of information security incidents is poorly configured and managed information systems. While the service provider is entirely responsible for ensuring that their SaaS solution is appropriately configured and managed, the responsibility is shared between the agency and the service provider in the other cloud service models (i.e. IaaS and PaaS). Agencies that do not have defined and documented build and hardening standards for operating systems and applications they are planning to deploy on IaaS or PaaS cloud services may find it difficult to effectively protect their systems against unauthorised access.

Where an agency decides to delegate the build and hardening of the operating systems and applications to the service provider, it must determine whether it is appropriate to accept the provider standards or define its own. Irrespective of the approach that is selected by the agency it is recommended that a penetration test be undertaken to ensure that services are initially deployed in a secure manner.

Considerations	Respondent
49. Are there appropriate build and hardening standards defined and documented for the service components the agency is responsible for managing?	Customer
50. Can the agency deploy operating systems and applications in accordance with internal build or hardening standards?	Joint
50a. If no, does the service provider have appropriate build and hardening standards that meet the agency's security requirements?	Microsoft
50b. Does the virtual image include a host-based firewall configured to only allow the ingress and egress (inbound and outbound) traffic necessary to support the service?	Microsoft
50c. Does the service provider allow host-based intrusion detection and prevention service (IDS/IDP) agents to be installed within the virtual machines?	Microsoft
51. Does the service provider perform regular tests of its security processes and controls? Will they provide customers with a copy of the associated reports?	Microsoft
52. Can a penetration test of the service be performed to ensure that it has been securely deployed?	Microsoft

Microsoft Responses

49. Are there appropriate build and hardening standards defined and documented for the service components the agency is responsible for managing?

No. This question is not applicable given the nature of the Office 365 service. Microsoft can, however, provide extensive guidance regarding the subject of how customers can secure their use of Office 365. Customers may, for example, find it useful to review the Microsoft document entitled "Customer Controls for Information Protection in Office 365".

Customers may also like to review the white paper entitled "Security and Compliance - Office 365".

50. Can the agency deploy operating systems and applications in accordance with internal build or hardening standards?

N/A. See answer to question 49.

50a. If no, does the service provider have appropriate build and hardening standards that meet the agency's security requirements?

N/A. See answer to question 49.

50b. Does the virtual image include a host-based firewall configured to only allow the ingress and egress (inbound and outbound) traffic necessary to support the service?

N/A. See answer to question 49.

50c. Does the service provider allow host-based intrusion detection and prevention service (IDS/IDP) agents to be installed within the virtual machines?

N/A. See answer to question 49.

51. Does the service provider perform regular tests of its security processes and controls? Will they provide customers with a copy of the associated reports?

Microsoft conducts regular testing of the security process and controls for Office 365, as independently verified in our ISO 27001, SOC 1 Type 2 (SSAE 16/ISAE 3402) and SOC 2 Type 2 (AT 101) attestations for both Office 365 and the underlying datacentre infrastructure on which it runs.

51a. Will they provide customers with a copy of the associated reports?

We do not provide copies of our internal test reports to external parties as doing so could compromise the security the Office 365 service. If our internal testing identifies any weaknesses we provide reports on such to our external auditors.

52. Can a penetration test of the service be performed to ensure that it has been securely deployed?

Yes - see answer to question 47.

3.5.4 Patch and Vulnerability Management

Improved patch and vulnerability management is often cited as one of the main benefits of moving to the cloud. Vulnerabilities present a significant risk to any information system, particularly those that are exposed to the Internet. The ubiquitous access provided by cloud services means that it is very important that agencies ensure that these services are patched in a timely manner.

It is important to identify which party is responsible for patching each component of a cloud service (e.g. the application, operating system, hypervisor software, Application Programming Interface (API) etc.). As discussed, the cloud service model (i.e. SaaS, PaaS or IaaS) usually dictates which party is responsible for the management and maintenance of individual components.

Where the service provider is responsible the agency must ensure that Terms of Service and SLA specify the maximum time period permitted between a patch being released by a vendor and being applied to all affected systems (i.e. the maximum exposure window).

Where the agency is responsible for applying patches it must ensure that it has an effective patch management process and monitors appropriate sources for vulnerability alerts (e.g. the vendor's website and/or mailing list, Common Vulnerabilities and Exposures (CVE) databases and the National Cyber Security Centre (NCSC) website) to ensure patches are identified and deployed in a timely manner.

Considerations	Respondent
53. Is the service provider responsible for patching all components that make up the cloud service?	Joint
53a. If no, has the agency identified which components the service provider is responsible for and which it is responsible for?	Customer
54. Does the service provider's Terms of Service or SLA include service levels for patch and vulnerability management that includes a defined the maximum exposure window?	Microsoft
55. Does the agency currently have an effective patch and vulnerability management process?	Customer
56. Has the agency ensured that all of the components that it is responsible for have been incorporated into its patch and vulnerability management process?	Customer
57. Is the agency subscribed to, or monitoring, appropriate sources for vulnerability and patch alerts for the components that it is are responsible for?	Customer
58. Does the service provider allow its customers to perform regular vulnerability assessments?	Microsoft
59. Do the Terms of Service or SLA include a compensation clause for breaches caused by vulnerabilities in the service?	Joint
59a. If yes, does it provide an adequate level of compensation should a breach occur?	Customer

Microsoft Responses

53. Is the service provider responsible for patching all components that make up the cloud service? If no, has the agency identified which components the service provider is responsible for and which it is responsible for?

Yes. As set out in the document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements", in regard to control requirement **IS-20 Information Security - Vulnerability / Patch Management**, Microsoft states:

"Office 365 implements technologies to scan the environment for vulnerabilities. Additionally, we contract with external penetration testers who also constantly scan the systems. Identified vulnerabilities are tracked, and verified for remediation. In addition, regular vulnerability/penetration assessments to identify vulnerabilities and determine whether key logical controls are operating effectively are performed.

Microsoft's Security Response Center (MSRC) regularly monitors external security vulnerability awareness sites. As part of the routine vulnerability management process, Office 365 evaluates our exposure to these vulnerabilities and leads action across Office 365 to mitigate risks when necessary.

Per best practice, Microsoft has full, robust patch management systems that are audited and tracked regularly by management. Any issues or requested exceptions would require management approval to address. This process is included in our ongoing audit schedule. The MSRC releases security bulletins on the second Tuesday of every month ("Patch Tuesday"), 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, Office 365 is required to apply patches to affected Office 365 systems according to a patching policy to remediate the vulnerability to the customer's hosted environment.

"Control of technical vulnerabilities" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12.6. For more information review of the publicly available ISO standards we are certified against is suggested.""

53a. If no, has the agency identified which components the service provider is responsible for and which it is responsible for?

This question is not applicable, given the nature of the Office 365 service.

54. Does the service provider's Terms of Service or SLA include service levels for patch and vulnerability management that includes a defined the maximum exposure window?

No. While Microsoft has extensive controls in place in regard to patch and vulnerability management, in accord with many of the standards Microsoft complies with, it does not include service levels for patch and vulnerability management in either the Microsoft Online Service Terms (OST) or the Service Level Agreement for Microsoft Online Services.

55. Does the agency currently have an effective patch and vulnerability management process?

This question is for customers to answer.

56. Has the agency ensured that all of the components that it is responsible for have been incorporated into its patch and vulnerability management process?

This question is for customers to answer.

57. Is the agency subscribed to, or monitoring, appropriate sources for vulnerability and patch alerts for the components that it is are responsible for?

This question is for customers to answer.

58. Does the service provider allow its customers to perform regular vulnerability assessments?

See answers to questions 33.a, 47 and 52 above.

59. Do the Terms of Service or SLA include a compensation clause for breaches caused by vulnerabilities in the service?

No. Neither the Online Service Terms nor the SLA for Office 365 contain a compensation clause for breaches caused by vulnerabilities in the service.

59a. If yes, does it provide an adequate level of compensation should a breach occur?

This question is for customers to answer.

3.5.5 Encryption

Encryption is often presented as the solution for addressing confidentiality risks within the cloud. There are, however, a number of important limitations that should be understood and considered by agencies planning adoption of cloud services. Agencies must determine their specific requirements for protecting information using encryption. Careful consideration must be given to:

- What information needs to be encrypted? All information held by the cloud service or only certain data types, or database rows, columns or entities?
- Why does the information need to be encrypted? For example, is encryption required to achieve compliance with a policy or standard?
- How should the information be encrypted? For example, what protocols and algorithms should be used?
- Who will encrypt the information and manage the encryption keys? The agency or the service provider?
- Where should the information be encrypted and decrypted? Within the agency, on the client devices or within the cloud service?
- When does the information need to be encrypted and decrypted? In transit, by the application (message encryption) and/or at rest?

While encryption is an effective control for protecting the confidentiality of data at rest, for data to be processed by a business rule within an information system, generally it must be unencrypted. As a result, it may be impractical or impossible to encrypt data stored within a cloud service that actually processes information (as opposed to simple storage).

Where a cloud service is capable of storing data in an encrypted format it is important to know which party (the agency or the service provider) is responsible for managing the encryption keys. It is important to note that if the service provider has access to, or manages, the encryption keys then they will be able to decrypt and access the information held in the cloud service. This has data sovereignty implications if encryption is used to treat risks related to information being stored outside New Zealand.

The party that manages the encryption keys must have an effective key management plan. Key management is essential to ensure that encryption keys are protected from being compromised, which could result in unauthorised disclosure or the agency no longer being able to access its information. It may also affect an agency's ability to meet its obligations under the Official Information Act 1982 and the Public Records Act 2005. The NZISM specifies the key management practices required to effectively manage cryptographic keys.

The interception of data in transit is an inherent risk whenever sensitive information traverses a network, especially a network not owned or managed by the agency such as the Internet or a service provider's network. Agencies must ensure that the cloud service encrypts all sensitive data in transit (including authentication credentials) using only approved encryption protocols and algorithms. Agencies relying on encryption should consider whether the encryption protocol, algorithm and key length used are appropriate. The NZISM specifies the encryption protocols and algorithms (together with recommended key lengths) that are approved for use by agencies for specific information classifications.

Consideration	Respondent
60. Have requirements for the encryption of the information that will be placed in the cloud service been determined?	Customer
61. Does the cloud service use only approved encryption protocols and algorithms (as defined in the NZISM)?	Joint
62. Which party is responsible for managing the cryptographic keys?	Joint
63. Does the party responsible for managing the cryptographic keys have a key management plan that meets the requirements defined in the NZISM?	Joint

Microsoft Responses

60. Have requirements for the encryption of the information that will be placed in the cloud service been determined?

This question is for customers to answer.

61. Does the cloud service use only approved encryption protocols and algorithms (as defined in the NZISM)?

Office 365 does use NZISM approved encryption protocols and algorithms. However, Microsoft does not widely publicise details for reasons related to the overall security of the service. Detailed information about the encryption applied to various aspects of the Office 365 Service is available under NDA.

For a general overview of Office 365 encryption, Microsoft recommends that customers review the document entitled "Security and Compliance - Office 365", which states:

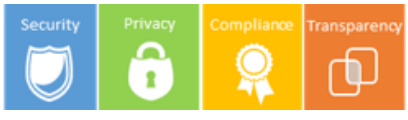
"Our Office 365 services follow industry cryptographic standards such as SSL/TLS (Secure Sockets Layer / Transport Layer Security), AES etc. to protect confidentiality and integrity of data.

All customer-facing servers negotiate a secure session using SSL/TLS (Secure Sockets Layer / Transport Layer Security) with client machines so as to secure the data in transit. This applies to various protocols such as HTTP(S), POP3, etc. that are used by clients such as Lync, Outlook and Outlook Web App (OWA) on any device. Microsoft is working to support and deploy strong encryption using SSLv3.0 support and TLSv1.1/1.2 across all workloads. The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data center.

To further protect your data in the Office 365 service, we use BitLocker as one mechanism to encrypt your data at rest. BitLocker is either deployed with Advanced Encryption Standard (AES) 128bit or AES 256bit encryption on servers that hold all messaging data including emails and IM conversations, content stored in SharePoint Online and OneDrive for Business. BitLocker drive encryption is a data protection feature that is integrated with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers and disks.

In certain other scenarios as appropriate, we use file level encryption. For example, when files and presentations are uploaded by meeting participants, this content is encrypted using 128 bit AES encryption by the Lync Online web conferencing server.

Our latest encryption feature with which content in OneDrive for Business and SharePoint Online will be encrypted at rest is called Per-file encryption. With this, the encryption technology in Office 365 moves beyond a single encryption key per disk to deliver a unique encryption key per file. With this technology, every file stored in SharePoint Online—including OneDrive for Business folders—is encrypted with its own key, and subsequent updates to the file are encrypted with their own unique key as well. Your organization's files will be distributed across multiple Microsoft Azure Storage containers, each with separate credentials, rather than storing them all in a single database. By spreading encrypted files across storage locations,



encrypting the map of file locations itself, and physically separating master encryption keys from both content and the file map, this new encryption storage technology makes OneDrive for Business and SharePoint Online a highly secure environment for your data."

Also, Microsoft recommends that customers review information about Office 365 encryption available online for administrators – see here.

62. Which party is responsible for managing the cryptographic keys?

Microsoft manages keys for the encryption it applies to Office 365. Customers manage keys for any 3rd party encryption they may apply on top of this.

63. Does the party responsible for managing the cryptographic keys have a key management plan that meets the requirements defined in the NZISM?

Yes. Our ISO 27001:2013 certification requires that we demonstrate effective measures for meeting the following Control requirement:

"A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle."

Microsoft has policies, procedures, and mechanisms established for the effective management of cryptographic keys throughout their lifecycle to support encryption of data in storage and in transmission for the key components of the Office 365 service. As TLS is the essential foundation for encrypted communications within and between O365 services, much of the focus of key management practices is on creation, management and monitoring of TLS certificates.

Key management consists of manual and automated processes. Most certificates and keys are managed by automated processes and key management tools that include automatic generation of key pairs, automatic secure storage of the key pair information in a database and automated or on-demand rollover of keys with minimal downtime. Where these are not automated alerts exist to warn on certificates that expire within a configurable number of days to enable manual intervention.

3.5.6 Cloud Service Provider Insider Threat

Unauthorised access to sensitive information by the service provider's employees is a common concern for organisations planning to use cloud services. The controls required to manage this risk are no different from those used to protect against malicious insiders within the agency or a traditional outsource provider.

Agencies should ascertain whether the service provider has appropriate procedures in place to ensure its personnel are reliable, trustworthy and do not pose a security risk to its clients. The level of assurance available to agencies may vary significantly depending on the physical location of the service provider's service and its employees. For example, a New Zealand based service provider will be able to perform a standard Ministry of Justice criminal history check for all employees and require staff that manage system components that store, process or transmit the agency's data to gain New Zealand Security Intelligence Service security clearance (e.g. CONFIDENTIAL, SECRET or TOP SECRET). However, where a service is delivered or supported from another country these New Zealand specific checks will not be possible. In such circumstances agencies must consider whether the alternatives available to the service provider can provide an equivalent level of assurance.

Whilst vetting may prevent a service provider from employing someone that has a history of being untrustworthy, it does have its limitations. For example, vetting that reveals a criminal record may result in a potential employee being rejected. However, candidates that are untrustworthy but have never been caught or haven't been convicted may not be identified. Similarly, a previously trustworthy employee may

become untrustworthy if they become disgruntled or their personal circumstances change. These risks can be effectively managed if the service provider logs and monitors employees' activities and enforces separation of duties so that any malicious activity requires collusion from multiple sources making it less likely.

Logging and monitoring employees' activities is an important control to manage the risks associated with malicious insiders. Logging should cover all relevant activities performed by the service provider's employees that have logical or physical access to equipment or media that contains customer data. The service provider should monitor and review logs to identify any suspicious activity that requires investigation. In addition to this, duties should be separated to ensure that logs are protected from unauthorised modification and deletion (e.g. the administrator of a service component should not be granted modify or delete rights to the Security Information Event Monitoring (SIEM) service).

Consideration	Respondent
64. Does the service provider undertake appropriate pre-employment vetting for all staff that have access to customer data?	Microsoft
64a. Does the service provider perform on-going checks during the period of employment?	Microsoft
65. If the service provider is dependent on a third-party to deliver any part of their service, does the third-party undertake appropriate pre-employment vetting for all staff that have access to customer data?	Microsoft
66. Does the service provider have a SIEM service that logs and monitors all logical access to customer data?	Microsoft
67. Does the service provider enforce separation of duties to ensure that audit logs are protected against unauthorised modification and deletion?	Microsoft
68. Do the Terms of Service or SLA require the service provider to report unauthorised access to customer data by its employees?	Microsoft
68a. If yes, is the service provider required to provide details about the incident to affected customers to enable them to assess and manage the associated impact?	Microsoft

Microsoft Responses

64. Does the service provider undertake appropriate pre-employment vetting for all staff that have access to customer data? Does the service provider perform on-going checks during the period of employment?

Yes. Our ISO 27001:2013 certification requires that we demonstrate effective measures for meeting the following Control requirement:

"Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be processed and the perceived risks."

Microsoft requires full time employees (FTEs) and vendors to undergo a background check as part of the Microsoft HR hiring practice. Background checks are required for both new hires and personnel transferring to positions that involve access to customers' work sites and/or sensitive areas or data. Microsoft standard background check includes but is not limited to review of information relating to education, employment, and criminal history. Typically, the period of the check is 7 years.

Microsoft requires full time employees (FTEs) and vendors to undergo a background check as part of the Microsoft HR hiring practice. Background checks are required for both new hires and personnel transferring to positions that involve access to customers' work sites and/or sensitive areas. Microsoft standard

background check includes but is not limited to review of information relating to education, employment, and criminal history. Typically, the period of the check is 7 years.

64a. Does the service provider perform on-going checks during the period of employment?

Microsoft does not repeat employee background screening within the 7 year period noted in the response to question 64. However, during the time of their employment, all Microsoft and contractor employees are subject to regular processes designed the enable them to understand and comply with their obligations regarding security, compliance and confidentiality.

Additionally, customers should note that information security training and awareness is provided to all Microsoft O365 employees, contractors and third parties on an ongoing bases to educate them on applicable policies, standards and information security practices. Employees receive information security training through different programs such as, new employee orientation, e-learning modules and periodic O365 communications (e.g. compliance program updates). These include training and awareness on Office 365 security, privacy and compliance requirements. Job specific training is provided as appropriate.

Finally, Customers should also note that Microsoft O365 services 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.

65. If the service provider is dependent on a third-party to deliver any part of their service, does the third-party undertake appropriate pre-employment vetting for all staff that have access to customer data?

Yes. See answer to question 64.

66. Does the service provider have a SIEM service that logs and monitors all logical access to customer data?

Yes. The CSA CCM control ID **SA-14 Security Architecture - Audit Logging / Intrusion Detection** requires the following:

"Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel."

As set out in our document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements", in response to this control requirement we state:

"Access to logs is restricted and defined by policy and logs are reviewed on a regular basis. The Office 365 service has features that provide valuable insights into who has accessed which data throughout a customer's service. These features enable customers to directly view a subset of logs to verify who has accessed what data, and what they did with it. While customers cannot access system event logs in real-time, we have mechanisms in place to support access to deal with a security incident and investigation. In the event of a security incident, customers may log a service request for access to historical logs to assist in resolution or troubleshooting. We will provide the requested information if we have it.

"Audit logging" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.10.1. For more information review of the publicly available ISO standards we are certified against is suggested."

67. Does the service provider enforce separation of duties to ensure that audit logs are protected against unauthorised modification and deletion?

Yes. The CSA CCM control ID **IS-15 Information Security - Segregation of Duties** requires the following:

"Policies, process and procedures shall be implemented to enforce and assure proper segregation of duties. In those events where user-role conflict of interest constraint exists, technical controls shall be in place to mitigate any risks arising from unauthorized or unintentional modification or misuse of the organization's information assets."

As set out in our document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements", in response to this control requirement we state:

"Office 365 services can have distinct hosted services development and operations staff to adhere to the principle of segregation of duty. Access to source code, build servers, and the production environment is strictly controlled. For example:

• Access to the Office 365 production environment is restricted to operations personnel. Development and test teams may be granted access to information provided from within the production environment to help troubleshoot issues

• Access to the Office 365 source code control is restricted to engineering personnel; operations personnel cannot change source code

• Data Minimization is used to minimize the actual amount of customer data (Usage Data, Administration account & address book data, Regular and Core customer data) that we manage on our customers' behalf by tiering which internal team (Operations response, Support organization, Engineering and Partners and others within Microsoft marketing and sales) has access to the data.

Microsoft personnel build the servers before they are commissioned for the multi-tenant environment. Once a server build is complete, the build teams have their permissions removed. From the time of server commission, there are limited pathways through which Microsoft personnel may obtain permissions to a system running on the commissioned server. Support staff may obtain access as a direct result of a service ticket requiring access or an update to the system to install software or resolve a problem. In such cases, the audit log would show who logged in and when. The processes Office 365 uses comply with the certifications Microsoft maintains.

Segregation of duties is implemented for sensitive and/or critical functions in Office 365' environments in order to minimize the potential of fraud, misuse, or error.

"Segregation of duties" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.1.3. For more information review of the publicly available ISO standards we are certified against is suggested."

68. Do the Terms of Service or SLA require the service provider to report unauthorised access to customer data by its employees?

Yes. The Microsoft Online Service terms (OST) state:

"**Security Incident Notification**

If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service."

68a. If yes, is the service provider required to provide details about the incident to affected customers to enable them to assess and manage the associated impact?

See answer to question 68.

3.5.7 Data Persistence

It can be difficult to permanently delete data from a multi-tenant cloud service when the organisation scales down or terminates its use of the service. If data is not securely deleted a future compromise of the service may still expose agency information. Similar issues arise if the service provider does not have processes to ensure that ICT equipment and storage media (e.g. hard disk drives, backup tapes etc.) are securely wiped before redeployment or disposal. Therefore it is essential that organisations establish that the service provider has robust and demonstrable data destruction and disposal processes in place.

Considerations	Respondent
69. Does the service provider have an auditable process for the secure sanitisation of storage media before it is made available to another customer?	Microsoft
70. Does the service provider have an auditable process for secure disposal or destruction of ICT equipment and storage media (e.g. hard disk drives, backup tapes etc.) that contain customer data?	Microsoft

Microsoft Responses

69. Does the service provider have an auditable process for the secure sanitisation of storage media before it is made available to another customer?

Yes. The CSA CCM control **ID DG-05 Data Governance - Secure Disposal** requires that:

"*Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means*".

As set out in the document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements", in response to this control requirement we state that:

"Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 (National Institute of Standards & Technology Special Publication 800-88, Guidelines for Media Sanitization) compliant. For hard drives that can't be wiped we use a physical destruction process that destroys them (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained and audited through the ISO process. All Office 365 services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.

"Secure disposal or re-use of equipment and disposal of media" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.2.6 and 10.7.2. For more information review of the publicly available ISO standards we are certified against is suggested."

70. Does the service provider have an auditable process for secure disposal or destruction of ICT equipment and storage media (e.g. hard disk drives, backup tapes etc.) that contain customer data?

Yes. See answer to question 69 that details relevant processes that are covered in our ISO 27001:2013 audit certification.

3.5.8 Physical Security

Physical security controls are vital to ensure that information is physically protected from unauthorised access by both malicious service provider personnel and third parties. Effective information security is dependent on the efficacy of the physical controls implemented to protect the service provider's offices, datacentres and physical assets.

SIGS, the NZISM and the Protective Security Manual (PSM) define the minimum physical security controls that must be in place to adequately protect official information based on its classification.

However, as discussed it may not be possible or practical to directly assess the physical controls that the service provider has implemented to protect its customers data within a cloud service. An agency may be limited to reviewing a third party audit report.

Considerations	Respondent
71. If it is practical to do so (i.e. the datacentre is within New Zealand), can the service provider's physical security controls be directly reviewed or assessed by the agency?	Microsoft
71a. If no, will the service provider allow the agency to review of a recent third party audit report (e.g. ISO 27001 or ISAE 3402 SOC 2 Type II) that includes an assessment of their physical security controls?	Microsoft
72. Do the service provider's physical security controls meet the minimum requirements as defined in the New Zealand government's security guidelines to protect the information stored in the cloud service?	Customer

Microsoft Responses

71. If it is practical to do so (i.e. the datacentre is within New Zealand), can the service provider's physical security controls be directly reviewed or assessed by the agency?

Microsoft can arrange for customers to visit our datacentres. However, such visits do not permit a thorough, audit-style review of our physical security controls.

The document "Microsoft Azure Standard Response to RFI - Security and Privacy" for Microsoft Azure (on top of which Office 365 is deployed) sets out our response to CSA CCM Facilities Security controls ID **FS-01 through FS-08**. The purposes and details of these controls are covered under the ISO 27001 standard, specifically addressed in Annex A, domains 7, 9 & 10 (including sub-domains thereof). For more information it is recommended that customers review the ISO standards we are certified against."

Customers should note that the physical security controls applied by our Microsoft Cloud Infrastructure and Operations organisation (MCIO) team which runs our Global Data Center operations are audited by third parties on an annual basis. Customers can contact their account representative to request a copy of the ISO 27001, SOC 1 Type 2 and SOC 2 Type 2 reports for these datacentres under NDA. Public sector Customers should also note that copies of these reports have been provided to the NZ Government CIO.

We encourage customers to review the document entitled "Windows Azure Security: Technical Insights."

71a. If no, will the service provider allow the agency to review of a recent third party audit report (e.g. ISO 27001 or ISAE 3402 SOC 2 Type II) that includes an assessment of their physical security controls?

Yes - see answer to question 71.

72. Do the service provider's physical security controls meet the minimum requirements as defined in the New Zealand government's security guidelines to protect the information stored in the cloud service?

This question is for customers to answer.

3.6 Data Integrity

Service providers can provide significantly different levels of protection against data loss or corruption. Some providers include data backup services as part of the base service offering, others offer them as an additional cost service and some do not offer them at all (e.g. Google Apps for Business does not provide any back-up services without a subscription to Google Apps Vault at additional cost). As a result, it is important to identify what level of protection the service provider offers and to assess whether or not they meet the agency's business requirements for recovering from data loss and corruption incidents.

It is essential to identify how the service provider protects its customers from data loss or corruption as it can indicate the level of protection provided. If the service provider replicates customer data to another datacentre in near real-time (e.g. every 5 minutes) a corruption could be replicated before it is detected. Similarly, if data is backed-up to tape on a daily basis then a Recovery Point Objective (RPO) of less than 24 hours may not be possible.

Agencies should ascertain the level of granularity offered for data restoration (e.g. can a single file or email be restored or are customers limited to restoring an entire mailbox or database?). In addition to this, they should identify and understand the process for initiating a restore. For example, can a user restore an email or file they have accidentally deleted or will an authorised staff member need to log a call with the service provider?

Data loss or corruption could lead to information being permanently lost. This may mean that agencies are unable to meet their obligations under the Public Records Act 2005 and the Official Information Act 1982. Agencies are advised to assess whether the planned data backup and archiving strategy supports their compliance efforts. Agencies without specialised knowledge in these Acts are encouraged to seek advice from Archives New Zealand and/or the Ministry of Justice to ensure compliance.

It is important to realise that the use of cloud services may not preclude the need for an agency to develop, implement and test its own data backup strategy to ensure that it can sufficiently recover from an incident that results in data loss or corruption.

Considerations	Respondent
73. Does the service provider provide data backup or archiving services as part of their standard service offering to protect against data loss or corruption? If not, do they offer data backup or archiving services as an additional service offering to protect against data loss and corruption?	Microsoft
74. How are data backup and archiving services provided?	Microsoft
75. Does the SLA specify the data backup schedule?	Microsoft
76. Does the data back-up or archiving service ensure that business requirements related to protection against data loss are met? (i.e. does the service support the business Recovery Point Objective?)	Customer
77. What level of granularity does the service provider offer for data restoration?	Joint
78. What is the service provider's process for initiating a restore?	Microsoft
79. Does the service provider regularly perform test restores to ensure that data can be recovered from backup media?	Microsoft
80. Does the agency need to implement a data backup strategy to ensure that it can recover from an incident that leads to data loss or corruption?	Customer
81. Does the proposed data backup and archiving strategy support the agency in meeting its obligations under the Public Records Act and Official Information Act?	Customer

Microsoft Responses

73. Does the service provider provide data backup or archiving services as part of their standard service offering to protect against data loss or corruption? If not, do they offer data backup or archiving services as an additional service offering to protect against data loss and corruption?

Yes. The CSA CCM control ID **DG-04 Data Governance - Retention Policy** requires that:

"Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of disk or tape backups must be implemented at planned intervals."

As set out in the document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements", in response to this control requirement we state that:

"Office 365 provides capabilities for customers to apply data retention policies as defined in the individual service descriptions. Office 365 service does not use datacenters in the traditional sense of one datacenter being active while others are passive. Instead, the service's software manages failover by continuously replicating data among datacenters, in essence keeping them active and current at the same time. Thus, if one datacenter goes down, others can still continue managing customer data with a minimum amount of disruption or loss.

Customer data is stored in a redundant environment with robust backup, restore, and failover capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are implemented, ranging from redundant disks to guard against local disk failure to continuous, full data replication to a geographically dispersed datacenter. Office 365 undergoes an annual validation of backup/recovery practices.

"Information back-up" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.5.1. For more information review of the publicly available ISO standards we are certified against is suggested."

74. How are data backup and archiving services provided?

Microsoft recommends that customers familiarise themselves with the Office 365 Service Descriptions available online.

75. Does the SLA specify the data backup schedule?

No.

76. Does the data back-up or archiving service ensure that business requirements related to protection against data loss are met? (i.e. does the service support the business Recovery Point Objective?)

Details of Microsoft Office 365's approach to service continuity are available online.

Microsoft conducts rigorous testing and measurements of Office 365 to ensure we deliver a reliable service even in times of disaster. The effectiveness of a disaster recovery plan is commonly measured in two ways: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO measures how long before users can access systems in the event of a failure. RPO measures how much of a time gap exists when the data is restored.

The RTO and RPO for Office 365 are based on quarterly verification and what we believe we can deliver in a real disaster. For our service as a whole and each component of our service, we strive to provide minimal

RTO and RPO, in some cases we try to be close to zero. Office 365 is effectively a set of federated services therefore, numbers like RTO/RPO of one component are independent of another which enhances reliability.

We are also continuously improving the service as a whole and each component in the area of failure recovery to provide our customers the service they deserve at all times.

77. What level of granularity does the service provider offer for data restoration?

Please see the Microsoft Office 365 service descriptions. It is possible to recover single items from both Exchange and SharePoint.

78. What is the service provider's process for initiating a restore?

Please see the Microsoft Office 365 service descriptions. Under most circumstances recovery of information can be conducted by the Tenant administrators themselves. In the unlikely case that information needs to be recovered by Microsoft the support process can be used.

79. Does the service provider regularly perform test restores to ensure that data can be recovered from backup media?

Yes. Microsoft regularly performs test restores, as evidenced by our SOC attestations. Also, see answer to question 73.

80. Does the agency need to implement a data backup strategy to ensure that it can recover from an incident that leads to data loss or corruption?

This question is for customers to answer.

81. Does the proposed data backup and archiving strategy support the agency in meeting its obligations under the Public Records Act and Official Information Act?

This question is for customers to answer.

3.7 Availability

3.7.1 Service Level Agreement

The service provider's SLA typically specifies the level of expected availability performance as a percentage. It is important for agencies to understand exactly what the defined percentage means and to assess whether or not these levels meet the requirements for availability (e.g. 99.9% up time over a year allows for up to 9 hours of unscheduled outages without breaching the SLA).

The SLA should include the details of any scheduled outage windows. This will ensure that the service provider cannot schedule long outages (including emergency outages) with little or no notification without breaching the SLA.

Where scheduled outage windows are defined in the SLA they should be reviewed to ensure that they will not have an adverse impact on business operations. For example, if an SLA includes a 3 hour scheduled outage on the first Tuesday of each month between 17:00 and 20:00 Eastern Daylight Time, the outage would occur between 10:00 and 13:00 on Wednesday in New Zealand.

Some service providers use technologies to enable them to perform maintenance activities without the need for an outage, however, agencies should not assume that this is the case simply because scheduled outages are not defined in the SLA.

Another important consideration is the adequacy of the compensation provided if the SLA is breached and the method for calculating penalties over a service period. Typically an SLA for cloud services will specify minimal compensation such as service credits or discounted invoices. Agencies should review any compensation clauses taking into account the impact on the business if the service was unavailable to determine if the level of reparation is sufficient.

Considerations	Respondent
82. Does the SLA include an expected and minimum availability performance percentage over a clearly defined period?	Joint
82a. If yes, are the business requirements for availability met? (I.e. does the service support the business's Recovery Time Objective and Acceptable Interruption Window?)	Customer
83. Does the SLA include defined, scheduled outage windows?	Microsoft
83a. If yes, do the specified outage windows affect New Zealand business operations?	Customer
83b. If no, has the service provider implemented technologies that enable them to perform maintenance activities without the need for an outage?	Microsoft
84. Does the SLA include a compensation clause for a breach of the guaranteed availability percentages?	Joint
84a. If yes, does this provide an adequate level of compensation should the service provider breach the SLA?	Customer

Microsoft Responses

82. Does the SLA include an expected and minimum availability performance percentage over a clearly defined period?

Yes. The SLA for Microsoft Online Services specifies a "minimum Monthly Uptime Percentage".

82a. If yes, are the business requirements for availability met? (I.e. does the service support the business's Recovery Time Objective and Acceptable Interruption Window?)

This question is for customers to answer.

83. Does the SLA include defined, scheduled outage windows?

No.

83a. If yes, do the specified outage windows affect New Zealand business operations?

Not applicable.

83b. If no, has the service provider implemented technologies that enable them to perform maintenance activities without the need for an outage?

Yes. The scheduled maintenance window used for Office 365 is allocated to occur every two weeks. This does not necessarily mean that we have any scheduled downtime during these windows, but is a defined period during which work could be conducted. On an exception basis critical security fixes may be deployed outside the maintenance window. The impact of the maintenance is described in the notification shared with our customers five days in advance from within the service health dashboard. Major changes and infrastructure updates are communicated via the message centre twelve months in advance.

The following information is provided for awareness. For latest details please see the Office 365 service description, message centre and Microsoft Online Services SLA.

- **Exchange Online, Exchange Online Archiving (EOA), and Exchange Online Protection (EOP)**: there is no scheduled downtime for these services. Please see the SLA for the latest information.
- **Lync Online**: Lync is built in a server pool configuration, which means that as code is updated on one server in the pool the connections are moved to other servers within the pool. This results in no planned downtime. Keep in mind that this is not defined in the SLA.
- **SharePoint Online**: SharePoint online may be in a read only state for a short while during maintenance, typically this is just a few minutes when updating the content farm. Notifications may provide for a longer window of read only state (for example 1hr) to cater for any failures, rollbacks or retries needed. The goal is that scheduled downtime should have a minimal impact on customers using SharePoint Online. Organizations should always be able to read their data during upgrades.

Extended details

- **Content Farm Upgrade:** during upgrade of the SharePoint content database a copy of database differential is taken from the original to the new database, this necessitates the database being placed in read only to allow rollback. This typically takes a few minutes per database and only one database is upgraded at the time leaving the other databases fully operational.
- **Service Farm Upgrade (Federated Farm Upgrade):** when we upgrade the services farms including Indexing, User Profiles and other SharePoint services the content farm will remain in read/write mode, allowing documents to be updated or uploaded during the scheduled downtime.

84. Does the SLA include a compensation clause for a breach of the guaranteed availability percentages?

Yes. If the SLA commitment regarding minimum Monthly Uptime Percentage is breached, there is a sliding scale of service credits that customers may submit a claim for.

84a. If yes, does this provide an adequate level of compensation should the service provider breach the SLA?

This question is for customers to answer.

3.7.2 Denial of Service Attacks

Denial of Service (DoS) attacks are an inherent risk for all Internet facing services. The use of cloud services may increase the risk of such an attack eventuating as the aggregation of multiple agencies onto a single service may present a more attractive target for attackers. Similarly, an agency may suffer associated or collateral damage in an attack against a service provider or a cotenant. A DoS attack may be launched against the service provider or the agency itself.

Typically it is difficult to protect against traffic based DoS attacks as they are intended to consume all the available resources and effective defences rely on blocking the source of the attack as close to the attackers location as possible. However, the use of cloud services may lessen the impact of some forms of DoS attacks as service providers have spare network bandwidth and computing capacity. In addition to this some service providers use protocols and technologies (e.g. Anycast, Application Delivery Networks and Content Delivery Networks) together with geographically dispersed datacentres to distribute network traffic and computer processing around the world.

The elastic nature of cloud services may also cause financial impacts. A successful DoS attack may force a service to scale exponentially resulting in abnormally high charges for resource use. This is usually referred to as Economic Denial of Service (EDoS) or bill shock. Agencies using cloud services that scale to meet demand can effectively reduce the risk of unexpected charges by ensuring that they set boundaries to limit the resources that can be consumed to those required to meet their anticipated peak usage.

Considerations	Respondent
85. Does the service provider utilise protocols and technologies that can protect against DDoS attacks? If yes, does enabling the service provider's DDoS protection services affect the answer to questions 15, 16 and 17?	Microsoft
85a. If yes, does enabling the service provider's DDoS protection services affect the answer to questions 15, 16 and 17?	Microsoft
86. Can the agency specify or configure resource usage limits to protect against EDoS/bill shock?	Microsoft

Microsoft Responses

85. Does the service provider utilise protocols and technologies that can protect against DDoS attacks?

Yes. At the interface with the public network, Microsoft uses special-purpose security devices for firewall, NAT, and IP filtering functions. Functions at this layer include denial of service (DOS) blocking, intrusion detection systems (IDS), SSL, and initial access/certificate validation. The edge of the service network houses those servers and services that provide first level authentication and load balancing.

Overall, Microsoft's strategy for defending against DDoS is somewhat unique due to our scale and global footprint. Microsoft is able to do things that many other providers cannot do, and that most if not all on-premises organizations are unable to do. If customers wish, they can request to review a copy of the document entitled "Defending Office 365 against Distributed Denial-of-Service attacks" under NDA.

85a. If yes, does enabling the service provider's DDoS protection services affect the answer to questions 15, 16 and 17?

No.

86. Can the agency specify or configure resource usage limits to protect against EDoS/bill shock?

Customers should actively monitor their utilisation of Office 365 services. In Microsoft's view this is the best the form of protection from EDoS/bill shock. Customers interested to learn more about Office 365 billing should see the information provided here.

3.7.3 Network Availability and Performance

The availability and performance of cloud services are heavily dependent on the supporting network infrastructure. The available bandwidth, latency, reliability and resiliency of local and international network connections could have a significant impact on user experience.

Agencies should evaluate the network connectivity between their users and the cloud service to ensure availability and performance requirements are met. This may be difficult if public networks (such as the Internet) are utilised in the delivery of the service, however, agencies should confirm that the network services they directly manage, or subscribe to, provide an adequate level of availability and bandwidth, together with sufficiently low latency and packet loss to meet the needs of the business.

Considerations	Respondent
87. Do the network services directly managed, or subscribed to by the agency provide an adequate level of availability?	Customer
88. Do the network services directly managed, or subscribed to by the agency provide an adequate level of redundancy/fault tolerance?	Customer
89. Do the network services directly managed, or subscribed to by the agency provide an adequate level of bandwidth (network throughput)?	Customer
90. Is the latency between the agency network(s) and the service provider's service at levels acceptable to achieve the desired user experience?	Customer
90a. If no, is the latency occurring on the network services directly managed, or subscribed to by the agency? Can the issue be resolved either by the network service provider or the agency?	Customer
90b. If no, is the latency occurring on the network services directly managed, or subscribed to by the agency? Can the issue be resolved either by the network service provider or the agency?	Customer
91. Is the packet loss between the agency network(s) and the service provider's service at levels acceptable to achieve the desired user experience? Can the issue be resolved either by the network service provider or the agency?	Customer
91a. If no, is the packet loss occurring on a network services directly managed, or subscribed to by the agency?	Customer
91b. If no, is the packet loss occurring on a network services directly managed, or subscribed to by the agency?	Customer

3.7.4 Business Continuity and Disaster Recovery

The use of cloud services introduces a reliance on the service provider's business continuity and disaster recovery plans. Therefore it is important to confirm that the service provider has adequate plans in place and to understand the level of continuity and recovery provided by them. It is also important to realise that the use of cloud services does not preclude the need for an agency to develop, implement and test its own business continuity and disaster recovery plans to ensure that it can continue to operate during a service outage.

As the cloud computing market is relatively immature, agencies should consider how they would recover business operations should a service provider go out of business or withdraw a service. They should ensure that the service provider uses common or de facto data format standards and provides a method to extract data in a format usable by the agency.

Considerations	Respondent
92. Does the service provider have business continuity and disaster recovery plans?	Microsoft
93. Will the service provider permit the agency to review of its business continuity and disaster recovery plans?	Microsoft
94. Do the service provider's plans cover the recovery of the agency data or only the restoration of the service?	Microsoft
95. If the service provider's plans cover the restoration of agency data, is the recovery of customer data prioritised?	Microsoft
95a. If so, how? Are customers prioritised based on size and contract value?	
96. Does the service provider formally test its business continuity and disaster recovery plans on a regular basis?	Microsoft
96a. If yes, how regularly are such tests performed?	Microsoft
96a. Will they provide customers with a copy of the associated reports?	Microsoft
97. Does the agency have its own business continuity and disaster recovery plan in place to ensure that it can recover from a service outage, the service provider going out of business or withdrawing the service?	Customer
98. Does the agency require its own data backup strategy to ensure that it can recover from a service outage, the service provider going out of business or withdrawing the service?	Customer
99. Are the backups (whether performed by the service provider or the agency) encrypted using an approved encryption algorithm and appropriate key length?	Joint

Microsoft Responses

92. Does the service provider have business continuity and disaster recovery plans?

Yes. The CSA CCM control ID **RS-01 Resiliency - Management Program** requires the following:

"Policy, process and procedures defining business continuity and disaster recovery shall be put in place to minimize the impact of a realized risk event on the organization to an acceptable level and facilitate recovery of information assets (which may be the result of. For example, natural disasters, accidents, equipment failures, and deliberate actions) through a combination of preventive and recovery controls, in accordance with regulatory, statutory, contractual, and business requirements and consistent with industry standards. This Resiliency management program shall be communicated to all organizational participants with a need to know basis prior to adoption and shall also be published, hosted, stored, recorded and disseminated to multiple facilities which must be accessible in the event of an incident."

As set out in our document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements", in response to this control requirement we state:

"A process for the development and maintenance of a Services Continuity Management (SCM) is in place for the Office 365 environment. The process contains a strategy for the recovery of Office 365 assets and the resumption of key Office 365 business processes. The continuity solution reflects security, compliance and privacy requirements of the service production environment at the alternate site.

We financially back our guarantee of 99.9% uptime. Additionally, we have redundancy at the physical, data, and functional layers, providing high availability and our disaster recovery capabilities keep customers up and running.

"Information security aspects of business continuity management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 14.1. For more information review of the publicly available ISO standards we are certified against is suggested"

Also, the CSA CCM control ID **RS-03 Resiliency - Business Continuity Planning** requires that:

"A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing and maintenance and information security requirements. Requirements for business continuity plans include the following:

- *Defined purpose and scope, aligned with relevant dependencies*
- *Accessible to and understood by those who will use them*
- *Owned by a named person(s) who is responsible for their review, update and approval*
- *Defined lines of communication, roles and responsibilities*
- *Detailed recovery procedures, manual work-around and reference information*
- *Method for plan invocation"*

In response, we state:

"Office 365 maintains a framework that is consistent with industry and Microsoft best practices that drives the continuity program at all levels.

The Office 365 framework includes:

- Assignment of key resource responsibilities
- Notification, escalation and declaration processes
- Continuity plans with documented procedures
- Training program for preparing all appropriate parties to execute the Continuity Plan
- A testing, maintenance, and revision process
- Microsoft Office 365 builds and operates availability at the application layer, which negates the suitability of publishing RPO and RTO values as a measure for system recoverability

By building in the intelligence to handle failure at the application layer (within our own software) instead of at the datacenter layer (relying on third-party hardware), Office 365 is able to deliver significantly high availability and reliability.

"Information security aspects of business continuity management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 14.1. For more information review of the publicly available ISO standards we are certified against is suggested.""

93. Will the service provider permit the agency to review of its business continuity and disaster recovery plans?

No. Other than to our auditors, Microsoft does not disclose our DR/BC plans to external organisations.

94. Do the service provider's plans cover the recovery of the agency data or only the restoration of the service?

The Office 365 DR/BC plan includes recovery of customer data.

95. If the service provider's plans cover the restoration of agency data, is the recovery of customer data prioritised?

Yes.

95a. If so, how? Are customers prioritised based on size and contract value?

Office 365 is a multi-tenant service so no priority is given based on size and contractual value.

96. Does the service provider formally test its business continuity and disaster recovery plans on a regular basis?

Yes. See answer to question 92. Customers should also note that they remain responsible for any service availability and performance issues that sit within their own span of control.

96a. If yes, how regularly are such tests performed?

As attested to by our SOC audits, failover exercises are conducted on a regular basis to test applications and related data to verify the accessibility at a secondary disaster recovery location. The frequency of conducting failover exercises, and the recovery time objectives (RTOs) for each application and support service, are based on the nature and criticality of the systems. Some services conduct monthly tests, while others are quarterly tests.

96b. Will they provide customers with a copy of the associated reports?

This is included in our Office 365 SOC attestation reports. If appropriate testing were not conducted it would be reflected in the reports, which are available under NDA.

97. Does the agency have its own business continuity and disaster recovery plan in place to ensure that it can recover from a service outage, the service provider going out of business or withdrawing the service?

This question is for customers to answer. As a matter of good practice, Microsoft advises customers to develop their own DR/BC plans for those aspects of Office 365 that are under their control.

98. Does the agency require its own data backup strategy to ensure that it can recover from a service outage, the service provider going out of business or withdrawing the service?

This question is for customers to answer.

99. Are the backups (whether performed by the service provider or the agency) encrypted using an approved encryption algorithm and appropriate key length?

Microsoft Office 365 backup tapes use AES 256-bit encryption, which is NZISM approved.

3.8 Incident Response and Management

The level of visibility and control of security incidents is likely to vary considerably across the cloud service models. The service provider is typically responsible for all incident management activities involving a SaaS solution, however, when an incident relates to a system located on an IaaS solution the customer is usually responsible for the incident management activities related to the platform, application and data and the service provider is only responsible for the activities directly related to the infrastructure components they manage. Similarly, the cloud deployment model (i.e. public, private, community or hybrid) adopted by the agency could significantly affect its visibility and control over the incident management activities. For example, customers of public cloud services normally have less visibility and control over incident management activities than those that have implemented a private cloud.

It is not reasonable to expect service providers to implement a separate incident response and management plan for each of their customers, therefore agencies need to gain an appropriate level of assurance that a service provider is capable of effectively and efficiently responding to an information security incident, as even the most meticulously planned, implemented and managed preventative controls can fail to stop a risk from eventuating. As a result, agencies need to review the service provider's Terms of Service and SLA to identify what, if any, support they provide to their customers during an information security incident.

Regardless of the service or deployment model, the use of cloud services does not preclude the need for an agency to have its own incident response and management process and plans. In fact, these plans are essential as they define how the agency will handle the tasks it is responsible for including roles and responsibilities, key contacts, incident definitions and notification criteria, escalation channels, evidence collection and preservation and post incident activities.

Considerations	Respondent
100. Does the service provider have a formal incident response and management process and plans that clearly define how they detect and respond to information security incidents?	Microsoft
100a. If yes, will they provide the agency with a copy of their process and plans to enable it to determine if they are sufficient?	Microsoft
101. Does the service provider test and refine its incident response and management process and plans on a regular basis?	Microsoft
102. Does the service provider engage its customers when testing its incident response and management processes and plans?	Microsoft
103. Does the service provider provide its staff with appropriate training on incident response and management processes and plans to ensure that they respond to incidents in an effective and efficient manner?	Microsoft
104. Does the service provider's Terms of Service or SLA clearly define the support they will provide to the agency should an information security incident arise? For example, does the service provider:	Microsoft
a. Notify customers when an incident that may affect the security of their information or interconnected systems is detected or reported?	Microsoft
b. Specify a point of contact and channel for customers to report suspected information security incidents?	Microsoft
c. Define the roles and responsibilities of each party during an information security incident?	Microsoft
d. Provide customers with access to evidence (e.g. time stamped audit logs and/or forensic snapshots of virtual machines etc.) to enable them to perform their own investigation of the incident?	Microsoft
e. Provide sufficient information to enable the agency to cooperate effectively with an investigation by a regulatory body, such as the Privacy Commissioner or the Payment Card Industry Security Standards Council (PCI SSC)?	Microsoft

f. Define which party is responsible for the recovery of data and services after an information security incident has occurred?	Microsoft
g. Share post incident reports with affected customers to enable them to understand the cause of the incident and make an informed decision about whether to continue using the cloud service?	Microsoft
h. Specify in the contract limits and provisions for insurance, liability and indemnity for information security incidents? (Note: it is recommended that agencies carefully review liability and indemnity clauses for exclusions.)	Microsoft
105. Does the service providers incident response and management procedures map to (or fit with) the agency internal policy and procedures; that does not hinder or delay the agency's ability to manage incidents in a timely and effective manner?	Customer

Microsoft Responses

100. Does the service provider have a formal incident response and management process and plans that clearly define how they detect and respond to information security incidents?

Yes. The document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements" sets out various measures that Microsoft has put in place in relation to Office 365 security incident response and management processes and plans.

In particular, customers should note Microsoft's responses to CSC CCM controls **IS-22 Information Security - Incident Management**, **IS-23 Information Security - Incident Reporting**, **IS-24 Information Security - Incident Response Legal Preparation** and **IS-25 Information Security - Incident Response Metrics**. Certification of the existence and efficacy of these controls is included in our ISO 27001:2013 audit report.

100a. If yes, will they provide the agency with a copy of their process and plans to enable it to determine if they are sufficient?

Microsoft will not share details of its security incident plans and processes with customers, as doing so could compromise the security of Office 365. Microsoft does recommend that customers review the online information we provide entitled "Securing the Cloud Infrastructure".

101. Does the service provider test and refine its incident response and management process and plans on a regular basis?

Yes. See answer to question 100. Customers may also be interested in reading the document entitled "Microsoft Enterprise Cloud Red Teaming".

102. Does the service provider engage its customers when testing its incident response and management processes and plans?

Microsoft approaches the testing of incident response plans with the aim of avoiding customer impact. If impact on a customer is anticipated, then normal support and communication processes would be engaged.

103. Does the service provider provide its staff with appropriate training on incident response and management processes and plans to ensure that they respond to incidents in an effective and efficient manner?

Yes. Customers are advised to refer to the information about training and awareness that is included in the document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements".

104. Does the service provider's Terms of Service or SLA clearly define the support they will provide to the agency should an information security incident arise?

Yes - see answer to question 26 above.

For example, does the service provider:

104a. Notify customers when an incident that may affect the security of their information or interconnected systems is detected or reported?

Yes - see answer to question 26 above.

104b. Specify a point of contact and channel for customers to report suspected information security incidents?

To report security issues 24X7, customers can contact Microsoft Online Services Security Incident and Abuse Reporting

104c. Define the roles and responsibilities of each party during an information security incident?

See answer to question 26 above. In addition, with regard to the role of customers the Microsoft Online Service terms (OST) states:

"Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service."

104d. Provide customers with access to evidence (e.g. time stamped audit logs and/or forensic snapshots of virtual machines etc.) to enable them to perform their own investigation of the incident?

See answer to question 26. In addition, customers should note that the CSA CCM control ID **IS-24 Information Security - Incident Response Legal Preparation** requires the following:

"In the event a follow-up action concerning a person or organization after an information security incident requires legal action proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction."

As set out in our document entitled "Office 365 Mapping of CSA Security, Compliance and Privacy Requirements", in response to this control requirement we state:

"As part of the containment step in our Security Incident Response Process, 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.

"Security incident response plans and collection of evidence" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 13.2. For more information, we suggest a review of the publicly available ISO standards for which we are certified."

104e. Provide sufficient information to enable the agency to cooperate effectively with an investigation by a regulatory body, such as the Privacy Commissioner or the Payment Card Industry Security Standards Council (PCI SSC)?

See answer to question 26. Customers should note that this question could only be answered definitively *ex post* on a case-by-case basis.

104f. Define which party is responsible for the recovery of data and services after an information security incident has occurred?

These responsibilities will vary depending on the nature of the security incident in question. In all instances, Microsoft will be responsible for restoration of access to the Office 365 service. If relevant, data restoration responsibilities will be affected by prior actions the customer may have taken in regard to their data e.g. whether they have applied some form of encryption to it.

104g. Share post incident reports with affected customers to enable them to understand the cause of the incident and make an informed decision about whether to continue using the cloud service?

See answer to questions 26 and 104d.

104h. Specify in the contract limits and provisions for insurance, liability and indemnity for information security incidents? (Note: it is recommended that agencies carefully review liability and indemnity clauses for exclusions.)?

Yes, Microsoft contracts specify the contract limits and provisions for insurance, liability and indemnity. Currently these terms are provided in the whole of government agreement (G2015).

105. Does the service providers incident response and management procedures map to (or fit with) the agency internal policy and procedures; that does not hinder or delay the agency's ability to manage incidents in a timely and effective manner?

This question is for customers to answer.