

Frequently Asked Questions: Business Productivity Online Suite Risk Management

Table of Contents

Security 1
Compliance 3
Privacy 13
Service Continuity 15

Security

Q: How do customers know their information is secure with Microsoft Online Services?

Businesses must use a combination of technology and processes to help protect their messaging and collaboration environment from internal and external security threats. These threats use an array of attack vectors that require the establishment of multiple layers of protection. The Business Productivity Online Suite services enable customers to extend their own security controls and processes by:

- Managing risk through a comprehensive program that encompasses security, privacy, service continuity, and compliance management
- Using multiple layers of physical and logical security controls and multiple technologies
- Aligning risk management controls and practices with industry recognized standards such as ISO 27001 and SAS 70, and periodically having those controls and practices validated through third-party certification

Q: How many Microsoft staff have administrative rights? In other words how many have potential to access data?

The number of Microsoft staff with administrative access varies based on the individual Microsoft Online Service. Service support and administration access to Microsoft Online Services environments is protected through strong authentication practices that mandate both physical and logical isolation within each service. Within Microsoft Online Services, each staff member is issued an individual account to support maintenance activities. Access to Microsoft Online Services environments is granted based on the individual’s role and business need. Privileges are granted to each account following least privilege and need-to-know principles. Accounts are terminated when an individual’s employment status

changes. Accounts are periodically reconciled to help ensure all access is required and remains consistent with an individual's role.

Q: How does Microsoft prevent administrators from accessing customer data?

While database administrators, by definition, have access to all the resources on a database -- including customer data -- Microsoft strictly prohibits accessing customer data for purposes other than business needs such as performance tuning of databases, migrating customers from one database to another.

All Microsoft Online personnel are accountable for their handling of customer data, meaning access to Microsoft Online services is granted in a manner that is traceable to a unique user. In other words, accountability is enforced through a set of system controls, including the use of unique user names, data access controls and auditing. Unlike generic user names such as "Guest" or "Administrator", unique user names are used to enforce accountability by binding user actions to a specific person. Two factor authentication, such as smart card logins using digital certificates or RSA tokens, are also used to further strengthen this binding.

User Access to data is also limited by user role, for example, system administrators are not provided with database administrative access.

Microsoft applies strict controls over which user roles and users will be granted access to customer data. For example, all employees undergo background screening prior to employment with Microsoft. Screening prevents hiring the wrong person. Users are required to complete a form along with business justification to request access. This must be approved by the manager of the user prior to gaining access. In addition the access levels are reviewed on a periodic basis to ensure that only users who need access have access to the systems. When employees leave Microsoft, they go through an exit process during which their logical and physical access is removed.

In addition Microsoft Online data centers have biometric access controls with the majority of the data centers used to provide Microsoft Online requiring palm prints to gain physical access to the data centers.

Q: How does Microsoft identify, halt, correct, and notify customer about inappropriate access of their data?

Microsoft Online has developed robust processes to facilitate a coordinated response to security incidents including identification, containment, eradication, and recovery.

Identification – System and security alerts are harvested, correlated, and analyzed. Events are investigated by Microsoft Online Operational and Security teams. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists.

Containment – The escalation team evaluates the scope and impact of the incident. The immediate priority of the escalation team is to help ensure the incident is contained and data is safe. The

escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices.

Eradication – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering.

Recovery – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity.

Q: How will Microsoft help customers conduct an investigation of customer employees?

The Microsoft Online Services Security team may operationally assist customers on security matters that they cannot investigate given the available logs and tools from the Microsoft Online system. This activity is performed on a case-by-case basis, based upon the situation and extent Microsoft Online resources are required.

Q: Are customers able to access periodic reports on results from security audits, attempted intrusions, etc?

- SAS70 for facilities and dedicated are available to customers under NDA
- CyberTrust is available from CyberTrust site
- We are in pursuit of SAS 70 for Standard and ISO 27001 for both standard and dedicated – will be available to customers
- Some customers tell us they would rather NOT have all these details – it’s one of the reasons they adopted an online service in the first place. That said, we are looking into the possibility of providing customers with more frequent detailed reports about service health, incidents, etc.

Q: Is the BPOS Dedicated offering more secure than BPOS Standard?

We have the same risk management methodology and controls for both dedicated and standard versions of BPOS. We believe the two are equally secure and private.

Compliance

Q: Where are the BPOS Data Centers located? Can a customer request a particular data center?

Microsoft has data center locations of various sizes in key locations around the world. We don't talk publicly about the exact number or locations of our data centers, however there are primary and backup datacenters operating the BPOS services in the following regions: Europe, North America, and Asia Pacific.

Q: What security policies does Microsoft follow for Microsoft Online Services?

Microsoft Online Information Security Policy is based on ISO 27002 directives augmented with requirements specific to online services. (In the online space, for example, Microsoft Online requires that all major service releases must undergo web penetration testing; any critical vulnerabilities discovered during such penetration testing must be resolved prior to releasing that service version to the web.) The Microsoft Online Information Security Policy also incorporates additional requirements derived from best in class security practices and mapping of relevant international, national and state/providential requirements.

ISO 27002 is part of the ISO/IEC 27000 family of standards, published jointly by the [International Organization for Standardization](#) (ISO) and the [International Electrotechnical Commission](#) (IEC) and is the renamed, updated ISO17799 standard. The full name of this international standard is, "*Information technology - Security techniques - Code of Practice for Information Security Management*". The ISO27000 standard is intentionally broad in scope, covering privacy, confidentiality and technical security issues and "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization." To that end, the standard outlines hundreds of potential controls and control mechanisms. ISO27000 was developed in the context of the following core principles:

"the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)"¹.

The topical domains addressed by ISO27002 and the Microsoft Online Information Security Policy include:

- Risk assessment
- Security policy - management direction
- Organization of information security - governance of information security
- Asset management - inventory and classification of information assets
- Human resources security - security aspects for employees joining, moving and leaving an organization
- Physical and environmental security - protection of the computer facilities
- Communications and operations management - management of technical security controls in systems and networks

¹ Information Technology—Information security management systems - Requirements, International Standards Organization, ISO/IEC 27001:2005(E)

- Access control - restriction of access rights to networks, systems, applications, functions and data
- Information systems acquisition, development and maintenance - building security into applications
- Information security incident management - anticipating and responding appropriately to information security breaches
- Business continuity management - protecting, maintaining and recovering business-critical processes and systems
- Compliance - ensuring conformance with information security policies, standards, laws and regulations

Q: The Solution Services Agreement – Microsoft’s standard agreement that covers subscriptions to the Microsoft Online Dedicated offering -- states the customer is solely responsible for determining whether the Microsoft Data Security Policy meets the customer’s requirements. How does Microsoft enable the customer to get to a sufficient understanding of Microsoft’s policies?

Microsoft Online information Security Policy is based on ISO 27002 directives augmented with requirements specific to online services. (In the online space, for example, Microsoft Online requires that all major service releases undergo web penetration testing; any critical vulnerabilities discovered during penetration testing must be resolved prior to releasing that service version to the web.)

The ISO 27000 series specifically addresses information security and has become the *de facto* comprehensive information security standard in the IT industry. The ISO 27000 series is being adopted more and more broadly by industry and government. While it is the customer’s responsibility to decide whether Microsoft Online’s policies meet customer’s internal security requirements and risk appetite, Microsoft provides a number of resources to assist customer in making this determination, including the Microsoft Business Productivity Online Suite Security White Paper and Applicable third-party audit reports.

Q: What assurance can Microsoft provide about the security of Microsoft Online Services?

Microsoft Online’s security is based upon some of the most advanced security practices around. Microsoft Online institutes security controls (technical, process, people and physical) from end to end; i.e., product development phase to service launch and operational phases. These security controls are strictly enforced and monitored on a continuous basis for compliance. For detail, see the Microsoft [Business Productivity Online Suite Security White Paper](#)

Dedicated only:

In addition to internal monitoring, the Microsoft Online Dedicated environment goes through a SAS 70 Type II audit by an independent third party on an annual basis. The audit report will be shared under NDA.

Microsoft Online is continually assessing the ongoing evolution of the security space and enhancing its security program as appropriate.

Standard only:

BPOS-S services go through the Cybertrust's Security Management Program (SMP) perimeter certification. The Cybertrust SMP:

- Identifies critical assets and the most vulnerable areas of BPOS-S infrastructure, such as Internet-facing systems,
- Assesses and prioritizes real-world threats to critical information assets,
- Secures those assets through efficient, enterprise-wide controls and mitigation strategies, and
- Manages the maintenance of security posture through robust ongoing support.

The BPOS-S SMP certification includes in its review:

- Onsite physical review of all data centers,
- Internal vulnerability scanning for all service segments,
- External vulnerability scanning against the service at all data centers,
- Process and procedure review (with System Administrators, Network Engineers and other key personnel involved in provision of the service), and
- E-Mail filtering tests.

Microsoft Online is continually assessing the ongoing evolution of the security space and enhancing its security program as appropriate.

Q: Who has administrative rights to Microsoft Online? Are they full-time employees or are they contractors?

Microsoft Online is operated by both full-time employees and contractors. Full-time employees and contractors may have administrative rights to Microsoft Online infrastructure.

Administrative access: Administrative and user access to Microsoft Online's infrastructure is limited and allowed on a need-to-know basis only. Only operations personnel who are responsible for administering the Microsoft Online infrastructure may be granted administrative access.

Access to customer data: Only database administrators and customer support staff have access to customer data. Even though database administrators and support staff have access to customer data, Microsoft strictly prohibits accessing or using customer data for purposes other than business needs (such as database administrative activities or responding to support questions from a customer where such access is necessary).

Access to live Microsoft Online environment: Software development staff does not have access to the Microsoft Online environment.

Support access. Microsoft Online customer support staff does not have administrative rights to Microsoft Online systems. Microsoft strictly prohibits using computing facilities or accessing customer data for purposes other than business needs.

Controls applicable to each access category. Microsoft applies strict controls over access to Microsoft Online Infrastructure and customer data. For example, all Microsoft employees undergo background screening prior to employment with Microsoft. Screening prevents hiring the wrong person. Additionally, Microsoft Online staff is required to complete an application form and provide business justification to request access. Before access will be granted, the individual's manager must review and approve the access request. Access levels are reviewed on a periodic basis to ensure that only users who have an ongoing, validated business need have access to the systems. When employees leave Microsoft, they go through an exit process during which their logical and physical access to Microsoft Online is removed.

Additionally, Microsoft Online requires smart cards (two factor authentication) or RSA tokens to access the infrastructure that is used to host Microsoft Online. Two factor authentication uses two factors to authenticate a user, one of which is a password or pin (i.e., what the user knows) and the second of which is a physical device the user possesses (i.e., smart card or RSA token). This provides a stronger defense to access vulnerabilities such as password hacking (i.e., even if a user's password is hacked, the hacker would also need the physical device to access the system. Similarly, if a user loses the physical device (smart card or RSA token), one would need the user's password to gain access to the system.)

Dedicated only:

Microsoft Online Dedicated undergoes an annual SAS 70 audit, which includes verification of the effectiveness of logical and physical access controls by an independent third-party auditor. Examples of the logical access controls the Dedicated SAS70 tests for are:

- Access requests to Microsoft Online Infrastructure are formally submitted via Infopath form and approved by manager before access is granted;
- Requests to modify domain groups are approved by owners of the groups, such as authorized managers, prior to modification;
- Domain password resets are formally submitted by the users of Microsoft Online Infrastructure and validated by the Microsoft Online Identity & Provisioning team prior to resetting the password; and Accounts with administrative access are reviewed by Microsoft Online on a quarterly basis to ensure access is commensurate with roles and responsibility.

Examples of the physical access controls SAS 70 tests for are:

- Physical access to the Microsoft data centers is controlled by two-tier authentication, including Microsoft Proxy card access readers (card access badge required) and Microsoft Hand Geometry Biometric readers; and
- On a quarterly basis the Microsoft Security Officer sends out reports to the authorized personnel with authority to approve datacenter access listing. The reports contain the listing of persons who currently have access to the data centers. The authorized personnel then audits the list ensuring all persons still require access and have the least privileged access level

necessary to perform their job function. The authorized personnel must reply back to the Microsoft Security Officer with any changes or as a confirmation that no changes were necessary.

Q: How does Microsoft prevent administrators from accessing customer data?

While database administrators, by definition, have access to all the resources on a database -- including customer data -- Microsoft strictly prohibits accessing customer data for purposes other than business needs such as performance tuning of databases, migrating customers from one database to another.

All Microsoft Online personnel are accountable for their handling of customer data, meaning access to Microsoft Online services is granted in a manner that is traceable to a unique user. In other words, accountability is enforced through a set of system controls, including the use of unique user names, data access controls and auditing. Unlike generic user names such as "Guest" or "Administrator", unique user names are used to enforce accountability by binding user actions to a specific person. Two factor authentication, such as smart card logins using digital certificates or RSA tokens, are also used to further strengthen this binding.

User Access to data is also limited by user role, for example, system administrators are not provided with database administrative access.

Microsoft applies strict controls over which user roles and users will be granted access to customer data. For example, all employees undergo background screening prior to employment with Microsoft. Screening prevents hiring the wrong person. Users are required to complete a form along with business justification to request access. This must be approved by the manager of the user prior to gaining access. In addition the access levels are reviewed on a periodic basis to ensure that only users who need access have access to the systems. When employees leave Microsoft, they go through an exit process during which their logical and physical access is removed.

In addition Microsoft Online data centers have biometric access controls with the majority of the data centers used to provide Microsoft Online requiring palm prints to gain physical access to the data centers. For additional information regarding Microsoft Online's approach to customer data, please refer to the [Microsoft Online Privacy policy](#), [Microsoft's Privacy Guidelines For Developing Products and Services](#), and the [Microsoft Business Productivity Online Suite Security White Paper](#).

Dedicated only:

Microsoft maintains several environments relating to a service release; for example, there is a development environment, a test environment, and a preproduction environment apart from the production environment through which Microsoft Online services are delivered to the customers. These separate environments ensure that changes to the service are tested in controlled environments prior to release into production. It is strictly prohibited to move or copy customer data outside of the production environment into any of the other environments. The development, test and stage environments are required to be on private (non-routable) network segments.

In addition, physical access to the data centers used to provide Microsoft Online Services is controlled through a series of technical, people and process controls. Some of the physical security controls are:

- Physical access to the Microsoft data centers is controlled by two tier authentication including Microsoft Proxy card access readers (card access badge required) and Microsoft Hand Geometry Biometric readers.
- On a quarterly basis the Microsoft Security Officer sends out reports to the authorized personnel with authority to approve datacenter access listing. The reports contain the listing of persons who currently have access to the data centers. The authorized personnel then audits the list ensuring all persons still require access and have the least privileged access level necessary to perform their job function. The authorized personnel must reply back to the Microsoft Security Officer with any changes or as a confirmation that no changes were necessary.

Compliance with these controls is audited as part of the SAS 70 audit conducted annually by an independent third party auditor.

Q: What type of background investigation does Microsoft perform on people who are granted administrative rights?

Microsoft has determined that checking a candidate's background irrespective of what access rights to Microsoft Online infrastructure the employee may have is an important part of the selection process. Obtaining comprehensive job-related information assists Microsoft in hiring and maintaining a high-quality workforce. A background check may include information relating to a candidate's education, employment, criminal and credit history. No candidate or employee will begin work or be placed on an assignment until the required background checks have been successfully completed.

Q: Is Microsoft Gramm Leach Bliley Act (GLBA) compliant?

Microsoft Online Services helps customers comply with the security requirements of GLBA by providing technical and organizational safeguards to help customers maintain security and prevent unauthorized usage. Microsoft can provide, on request, a summary report of a third party certification by an independent auditor. Microsoft Office Live Meeting also has notification features that can help customers support GLBA compliance.

Dedicated only:

Microsoft Online Dedicated environment undergoes SAS 70 Type II audit by an independent third party on an annual basis. Our customers often use SAS 70 report which covers IT General Computing Controls for their individual compliance needs such as SOX, Gramm Leach Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA).

For some of the controls covered in Microsoft Online's SAS 70, refer to FAQ "[What is the scope of BPOS-D SAS 70?](#)"

Q: Is Microsoft Online Services HIPAA (Health Insurance Portability and Accountability Act) compliant?

Microsoft Online Services have features that customers can use to support their HIPAA compliance, but we rely on the customer to ensure compliance by integrating our feature-set with their organization's policies and practices. Microsoft Online Services is a conduit of information that includes technical and organizational safeguards to help customers maintain security and prevent unauthorized usage, and Microsoft personnel do not routinely access customer data. For more information about our policies on collection, use and sharing of personal information please read the [Microsoft Online Services privacy statement](#).

Q: Will Microsoft sign a HIPAA Business Associates Agreement (“BAA”)?

Microsoft Online Services does not sign Business Associate Agreements or any other HIPAA compliance document. Microsoft Online Services merely provide a conduit for the customer's information, as described in HIPAA regulations, and therefore the Services can be used without signing a BAA.

Q: Are Microsoft Online Services Payment Card Industry Data Security Standard (PCI DSS) compliant?

Standard only:

Microsoft Online customers can use credit cards to pay for the service. Microsoft Online handles all credit card information according to the PCI guidelines and systems handling customer credit cards are Level One PCI Compliant.

Dedicated only:

Microsoft Online is designed to provide the customer with a high-level of “customization” by which they can enforce their own internal policies and compliance requirements within the service. Microsoft Online Dedicated service does not handle credit cards and hence PCI compliance is not applicable. However Microsoft Online security policies and controls follow industry best practices such as ISO 27001 and others.

Q: Does Microsoft allow customers to audit Microsoft Online Services?

Microsoft Online conducts internal monitoring and auditing of Microsoft Online on a regular basis to ensure the controls are adequately designed and operationally effective. In addition, Microsoft Online undergoes external, or third-party, auditing to validate Microsoft Online's internal processes and systems. Microsoft Online internal monitoring includes automated compliance monitoring of infrastructure (e.g., vulnerability scans, penetration testing and testing of process and people controls). The Microsoft Online third-party validation program includes independent audits that are conducted on an annual basis to provide verification of Microsoft Online's security posture.

For security reasons, Microsoft Online does not allow our customers to audit our environment.

Dedicated only:

The Microsoft Online Dedicated environment undergoes a SAS 70 Type II audit by an independent third party on an annual basis. The SAS 70 contains valuable information regarding Microsoft Online's

controls and the effectiveness of those controls. Customers receive a detailed description of Microsoft Online's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively during the audit period. Customers may view the independent audit report under NDA.

Q: What type of independent audits and/or certifications does Microsoft Online Services undergo? What is the scope of services covered in each of these certifications and how often are audits conducted?

Service / Third Party Audit	BPOS-D	BPOS-S (excluding. EHS & LM)	FOSE (EHS)	LM
Cybertrust	NO	YES	NO	YES
SAS 70 Type II	SAS 70	FUTURE	NO	NO
ISO 27001	FUTURE	FUTURE	FUTURE	FUTURE

Data Centers / Third Party Audit	BPOS-D	BPOS-S (excluding. EHS & LM)	FOSE (EHS)	LM
Cybertrust	NO	YES	NO	YES
SAS 70 Type II	GFS SAS 70	GFS SAS 70	GFS SAS 70 or 3 rd party data center SAS 70	GFS SAS 70 or 3 rd party data center SAS 70
ISO 27001	GFS ISO 27001	GFS ISO 27001	GFS ISO 27001 except for 3 rd party data centers	GFS ISO 27001 3 rd party data center Cardiff – ISO 27001

Q: Where can I get more information about what SAS 70 is?

SAS 70 is an audit standard set by the American Institute of Certified Public Accountants (AICPA) and is geared towards service organizations. Service organizations are typically entities that provide outsourcing services that impact the control environment of their customers. Examples of service organizations are insurance and medical claims processors, hosted data centers, application service providers (ASPs) and managed security providers. SAS 70 is an independent verification of compliance

to security controls and effectiveness of security controls. SAS 70 audits are conducted by Deloitte & Touche (D&T) for Microsoft. SAS 70 audits are performed once a year. D&T tests the controls which include design of controls, evidence evaluation for a period of time. D&T produces the audit report which also includes opinion of the controls in addition to audit results of controls. More information regarding the standard and types of audits can be found on www.aicpa.org or the auditing firm of the customer.

Q: Is Business Continuity covered in the SAS 70 Audit?

While American Institute of Certified Public Accountants (AICPA) guidelines specifically excludes continuity in the SAS 70 audits, Microsoft has a robust continuity program in place to ensure recovery of a service(s) in a timely manner.

Q: What is the purpose of SAS 70?

SAS 70 is an independent verification of compliance to security controls and effectiveness of security controls. SAS 70 audits are conducted by Deloitte & Touche (D&T) for Microsoft. SAS 70 audits are performed once a year. D&T tests the controls which include design of controls, evidence evaluation for a period of time. D&T produces the audit report which also includes opinion of the controls in addition to audit results of controls.

Q: What is the scope of BPOS-D SAS 70 audit?

Dedicated only:

Microsoft Online Dedicated environment undergoes a SAS 70 Type II audit by Deloitte & Touche on an annual basis.

BPOS-D SAS 70 scope includes the following BPOS-D services

- Exchange Online
- Share point Online
- Desktop Management Systems
- Office Communication Services

The BOPS-D SAS 70 report includes the following controls:

- Logical Access
 - Requests for access are reviewed by Identity and Provisioning team to determine whether the request is for an authorized individual
 - Modifications to domain groups include obtaining approval from group sponsors
 - Service accounts that may require shared access are documented and reviewed periodically
 - Accounts with enterprise administrative access are reviewed quarterly and access is modified based on the results of the reviews

- Change Management
 - All changes to the environment go through a change process
 - Testing is carried out on all changes as appropriate. Users and stakeholders review and approve results of testing prior to implementation
 - The Change Advisor Board reviews and approves changes as required per the change management process
- Security Monitoring
 - Microsoft Online Risk Management Security team monitors potential adverse security events that report to the Intrusion Detection System's console which is reviewed daily by RAID operational and managerial personnel. Live response, investigation, escalation, containment, and eradication procedures are followed if an event is defined as a security incident
 - Each quarter a comprehensive security assessment against prioritized components of the BPOS-D environment to identify host, network, and application vulnerabilities is performed

Other controls included in the BPOS-D SAS 70 are:

- Software Development Life Cycle
- Patch Management
- Backups
- Physical Security

Privacy

Q: What notifications will Microsoft give customers regarding subpoenas Microsoft receives requesting production of customer information?

Microsoft believes that its customers should control their own information. Accordingly, if law enforcement approaches Microsoft directly for information hosted on its systems for its enterprise customers, Microsoft will try, to the extent possible, to redirect legal process to the customer to afford it the opportunity to decide how to respond. While Microsoft may take this position as a matter of policy, it will not always be successful in redirecting the demand as a legal process may be entitled to require Microsoft to produce information in its possession.

When Microsoft is required to comply, it will use commercially reasonable efforts to provide the customer with notice that a demand for its records has been made when providing such notice is permissible. By providing notice, the customer is afforded the opportunity to intervene in order to protect its records. Microsoft may, however, be prohibited by law from providing notice, and where there is no reasonable basis to object to the legal process, it would be required to comply.

Microsoft will only provide customer records where it is legally required to do so and will limit the production to only that information which it is required to disclose. The only exception to this rule

would be disclosures made to law enforcement or others when Microsoft has a good faith belief that an emergency involving the danger of death or physical injury requires disclosure without delay.

Q: How will Microsoft assist customers in responding to a discovery request?

Business Productivity Online Suite customers are in control of their own data, and should be able to respond to most e-discovery requests on their own. Microsoft offers an add-on messaging archive service that may help them in this effort.

Q: A customer has a requirement to keep backups for X years. Does Microsoft support this functionality?

Yes, documents that must be stored can be stored on a SharePoint site as part of our SharePoint Online offering. In addition, e-mail archiving is obtainable through Exchange Hosted Archive, an attached service that can be purchased separately from your Exchange Online service. This archiving solution, when properly configured, will provide a record of all e-mails sent or received from your Exchange Online service, and includes the ability search across mailboxes and other advanced archiving features.

As a matter of ordinary course, Microsoft Online Services retains backups for a limited period of time, in rolling order. Customers should note, however, this is for purposes of service continuity and should not be used in place of an archiving solution. Backup retention is very limited in duration, and backups are normally not retrievable.

Q: Is Microsoft Online Services HIPAA (Health Insurance Portability and Accountability Act) compliant?

Microsoft Online Services have features that customers can use to support their HIPAA compliance, but we rely on the customer to ensure compliance by integrating our feature-set with their organization's policies and practices. Microsoft Online Services is a conduit of information that includes technical and organizational safeguards to help customers maintain security and prevent unauthorized usage, and Microsoft personnel do not routinely access customer data. For more information about our policies on collection, use and sharing of personal information please read the Microsoft Online Services privacy statement at <http://go.microsoft.com/fwlink/?LinkID=104970>.

Q: Will Microsoft sign a HIPAA Business Associates Agreement ("BAA")?

Microsoft Online Services does not sign Business Associate Agreements or any other HIPAA compliance document. Microsoft Online Services merely provide a conduit for the customer's information, as described in HIPAA regulations, and therefore the Services can be used without signing a BAA.

Q: Is Microsoft GLBA (Gramm Leach Bliley Act) Compliant?

Microsoft Online Services helps customers comply with the security requirements of GLBA by providing technical and organizational safeguards to help customers maintain security and prevent unauthorized usage. Microsoft can provide, on request, a summary report of a third party certification by an

independent auditor. Microsoft Office Live Meeting also has notification features that can help customers support GLBA compliance.

Q: Can Canadian customers use this service? Are Canadian customers allowed to have their data transferred from Canada to the U.S.?

The Personal Information Protection and Electronic Documents Act, or PIPEDA, as it is abbreviated (Canada's federal data protection law), allows for transfer of personal information to other countries, provided that the companies to which the data is transferred provide a level of privacy protection comparable to that required in Canada. Our corporate data handling policies provide a level of protection comparable to that required by PIPEDA. Thus, generally, Canadian customers can transfer personal data to Microsoft in the U.S.

However, in some provinces (including British Columbia), public bodies and their service providers are prohibited by statute from transferring data outside Canada. Those customers should work with their legal counsel to determine whether they are able to use Microsoft's online services.

Service Continuity

Q: What are the redundancy or resiliency features included in BPOS? Is data replicated, backed up?

All services are configured from pairs of data centers with replication between them. Additionally there are multiple copies of data in each data center. In the event of major outage Microsoft offers service continuity by failing over to the alternate data center.

Q: Does Microsoft have a formalized Continuity Program in place?

Microsoft Online has a robust service continuity program in place based on industry best practices and provides the ability to recover subscribed services in a timely manner.

Q: Does each service have the ability to recover from a disasterous event?

Yes, all sevices have redundancy and resiliency to ensure that any significant or major outage is minimized.

Q: What is a Recovery Time Objective (RTO)?

The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTO's are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

Q: What is a Recovery Point Objective (RPO)?

The maximum amount of data loss an organization can sustain during an event.

Q: What type of exercises does Microsoft Online conduct?

- **Tabletop Exercise** - Participants review and discuss the processes, procedures, and tasks they would take without actually performing the actions. In this setting, the users can project how the recovery solution would be validated and ensure their plan content is inclusive and complete.
- **Alternate Site Exercise** - Participants perform the processes and tasks as they would at time of disaster in a controlled environment setting. For this type of exercise, the solution is validated in the alternate recovery site and the service brought online and is functioning as intended.
- **Geo-diverse Exercise** - Participants perform the processes and tasks for a cloud or multiple site recovery solution. The review and validation process is same as above but with a higher degree of complexity and interaction as it relates to manual intervention solutions. Automated geo-diversity solutions are easier to validate and maintain and as labor intensive.

Q: Describe how the recovery solution is exercised.

All services go through a three phase process defined as Pre-exercise, Exercise and Post-exercise to ensure scoping and scenario are defined, the event is conducted, and any issues identified and quickly resolved with updates to the documentation and solution as necessary.

Standard Only:

Internal validations take place on a regular basis to ensure the services are functioning as intended. This will include verifying data transfer from primary to secondary or geo-diverse sites, system and service functionality, and the solution is reflective of the current subscribed capabilities.

Dedicated Only:

Dedicated customers and Microsoft Online coordinate the event through the three phases mentioned above upon completion of the migration process to validate the subscribed service continuity solution. Customers will also be given the opportunity to run through the crisis management process to sync on how the two organizations interact at time of disaster. Once the initial migration is complete, exercises will be coordinated on an annual basis per industry best practices.

Q: For BPOS Dedicated services, will the customer have the opportunity to participate in the exercise?

Yes. The customer will be engaged in the entire exercise process mentioned above.

Q: For BPOS Standard, will the customer have the opportunity to participate in the exercise?

No, due to the nature of the production and recovery environment, it is not feasible to run customer based exercises.

Q: How are deficiencies remediated found during service continuity exercise?

After every validation for all services, a post-exercise phase is conducted that identifies any and all issues from the actual event. Resolutions and timeframes are defined, owners are identified and the Service Continuity Management Team manages the closure of these issues. This may include updates to the continuity plan documentation, training or modifications to the solution itself.

Q: Are plans in place to support the solution? Please provide an example of the plan.

Yes, every solution has a recovery plan in place and is updated as releases or significant changes take place.

Q: Does the RTO and RPO service levels vary from customer to customer?

No. All RTO's and RPO's are pre-determined for each service and kept consistent across the customer base to ensure consistency in methodology, solution architecture, and scalability.

Q: Describe the procedure for declaring a disaster for a dedicated service.

The detection of an event which could result in a disaster affecting service continuity is the responsibility of BPOS and Global Foundation Services (GFS) once it receives information about an emergency situation developing in one of the functional areas.

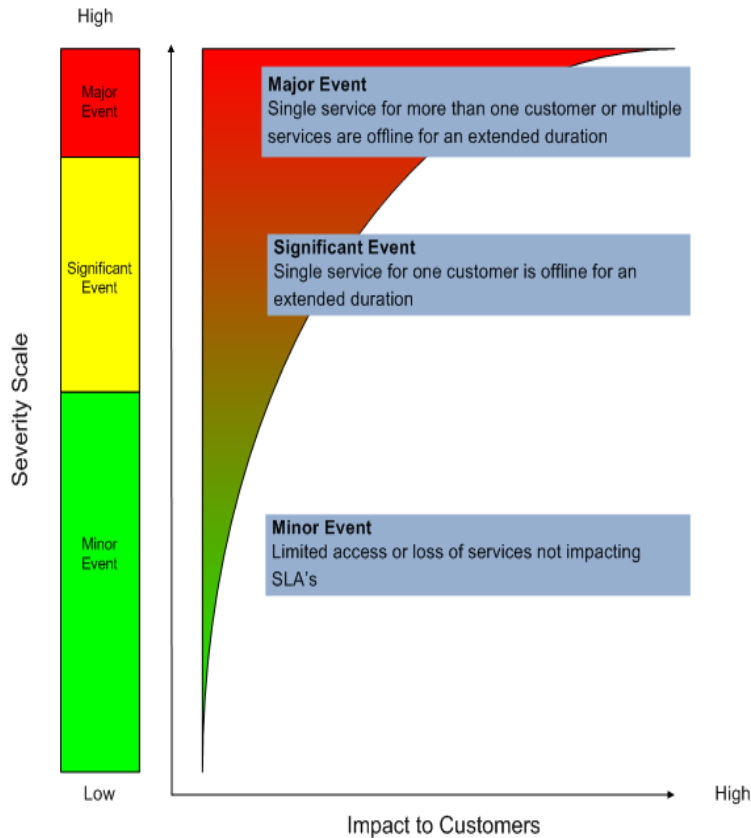
Scripts for gathering data to determine whether this playbook should be implemented, include, but are not limited to the following sample discovery questions:

- What service(s) are down?
- What is the estimated recovery time? What is the comfort level of vendor to meet this recovery estimate and why?
- What is the recommendation from vendor on failover and why?
- What are the details of the situation that caused the outage (i.e., flood, fire, and etc)?
- Is it operationally recoverable (recoverable in primary site)? If yes, how and by when?
- What if anything has been done to rectify the issue? What is planned on being done within the next hour? Next two hours?

Q: What is the difference between a significant event and major event in BPOS-Dedicated?

A significant event is when a single service for one customer is down for an undetermined amount of time.

A major event is when a single service or multiple services are down for one or more customers for an undetermined amount of time.



Q: Is the recovery site on a different power and network grid from the primary site?

Yes. All alternate sites are out of region to ensure any outages localized to the primary site are non-impactful to the secondary.

Q: What type of updates are provided to keep the customer apprised of the status of the continuity solution?

Dedicated only:

Customers will be notified of any updates to the continuity solution as it relates to contract terms and agreements with the intent to update clauses as appropriate. Additionally, customers will have the opportunity to validate new solutions as it falls into the annual validation cycle.