Assessment Report

Microsoft Corporation
Microsoft Azure

Assessment dates	11/04/2018 to 11/09/2018 (Please refer to Appendix for details)
Assessment Location(s)	Redmond (000)
Report Author	Willibert Fabritius
Assessment Standard(s)	ISO/IEC 27001:2013, ISO IEC 27018

Table of contents

Executive Summary

The audit team recommends that BSI consider the information found in this assessment report as the evidence of the conformity of Microsoft Azure (for public, government and Germany environment including Azure services and physical infrastructure) to the requirements for ISO 27001 and ISO 27018 for extension to scope and continued certification.

The audit was performed at Microsoft Headquarter (HQ), Redmond, the recommendation is to maintain the validity of the existing certificates for Microsoft Azure ISO 27001 (Certificate # IS 577753) and ISO 27018 (certificate # PII 648972) respectively, collectively referred as Microsoft Azure certificate and add the new services into the scope of certification.

The audit objectives have been achieved and the certificate scope remains appropriate. The audit team concludes based on the results of this audit that Microsoft Azure does fulfil the standards and audit criteria identified within the audit report and it is deemed that the management system continues to achieve its intended outcomes.

There were no outstanding nonconformities from previous assessments. No new nonconformities were identified during the assessment. Enhanced detail relating to the overall assessment is contained within subsequent sections of the report.

Changes in the organization since last assessment

There is no significant change of the organization structure and key personnel involved in the audited management system.

The following changes in relation to the certified organization activities, products or services covered by the scope of certification were identified:

New services have been added to the Azure Scope

There was no change to the reference or normative documents which is related to the scope of certification.

NCR summary graphs

There have been no NCRs raised.

Your next steps

NCR close out process

There were no outstanding nonconformities to review from previous assessments.

No new nonconformities were identified during the assessment. Enhanced detail relating to the overall assessment findings is contained within subsequent sections of the report.

Please refer to Assessment Conclusion and Recommendation section for the required submission and the defined timeline.

Assessment objective, scope and criteria

The objective of the assessment was to conduct a certification (extension to scope) assessment to evaluate the level of conformity with the Standard(s) requirements, effectiveness of the management system(s) in continually meeting objectives, and the ability of the management system to ensure the organization meets applicable statutory, regulatory, and contractual requirements and as applicable, to identify areas for potential improvement of the management system(s).

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001 / ISO 27018 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

The visit was conducted as an integrated assessment.

ISO 27001 / ISO 27018
Microsoft Corporation/ Microsoft Azure management system documentation

Assessment Participants

* Names are redacted from the report

Name	Position	Opening Meeting	Closing Meeting	Interviewed (processes)
*	Principal PM Manager	x	x	
*	Senior Program Manager	x	x	x
*	Program Manager 2	x	x	x
*	Senior Engineering Lead			x
*	Senior Software Engineer Manager			x
*	Senior Software Engineer			x
*	Senior Security Program Manager			x
*	Principal Software Dev Lead			x
*	Senior Program Manager			x
*	Senior Program Manager			x
*	Program Manager 2			x
*	Principal Program Manager			x
*	Principal Engineering Manager			x
*	Senior Service Engineer Manager			x
*	Principal Program Manager			x
*	Senior Program Manager			x
*	Senior Program Manager			x
*	Attorney			x
*	Compliance PM			x

Assessment conclusion

BSI assessment team

Name	Position
Willibert Fabritius	Team Leader

Assessment conclusion and recommendation

The audit objectives have been achieved and the certificate scope remains appropriate. The audit team concludes based on the results of this audit that the organization does fulfil the standards and audit criteria identified within the audit report and it is deemed that the management system continues to achieve its intended outcomes.

RECOMMENDED - The audited organization can be recommended for certification / recertification / continued certification to the above listed standards, and has been found in general compliance with the audit criteria as stated in the above-mentioned audit plan.

Use of certification documents, mark / logo or report

The use of the BSI certification documents and mark / logo is effectively controlled.

Findings from this assessment

Organizational overview:

Microsoft Azure is part of Cloud + AI Platform organization. Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers. It provides Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) and supports several different programming languages, tools and frameworks, including both Microsoft-specific, third-party software, as well as solutions based Open-source software.

Microsoft Azure is responsible for the management of the global Microsoft owned as well as 3rd party datacenters. The Microsoft owned datacenters are visited and audited per a sample-based plan. The 3rd party datacenters are not visited, but during the audit at HQ, samples are reviewed to demonstrate that Microsoft has an effective 3rd party vendor management program.

The audit followed two "paths", one was focused on the management of individual controls / processes and the second path was focused on confirming that individual services had followed the required global controls / process.

All services are required to follow the established Azure processes, following new services were sampled for testing/verification. Based on the assessment it was confirmed that all verified services followed the required Azure processes.

None of the 9 new services from scope extenuation were deployed in Azure Germany.

Statement of Applicability
Statement of Applicability
ISO 27001 - Mandatory Clauses, and Information Security Policy (All services):

Clause 4, 5 and 9
Annex Controls A.5 and A.6
Annex Controls A.18.1.1 - A.18.1.3, A.18.1.5, A.18.2 , A.15

The organization has determined interested parties including their needs and expectations. The organization scope was defined and documented. The ISMS has been established.

No changes to the ISMS other than being applied to the new services added to the scope.

The set of policies for information security previous s defined, approved by management, published and communicated to employees and relevant external parties is also applicable to the new services.

Controls surrounding the Context of the Organization are operating effectively.

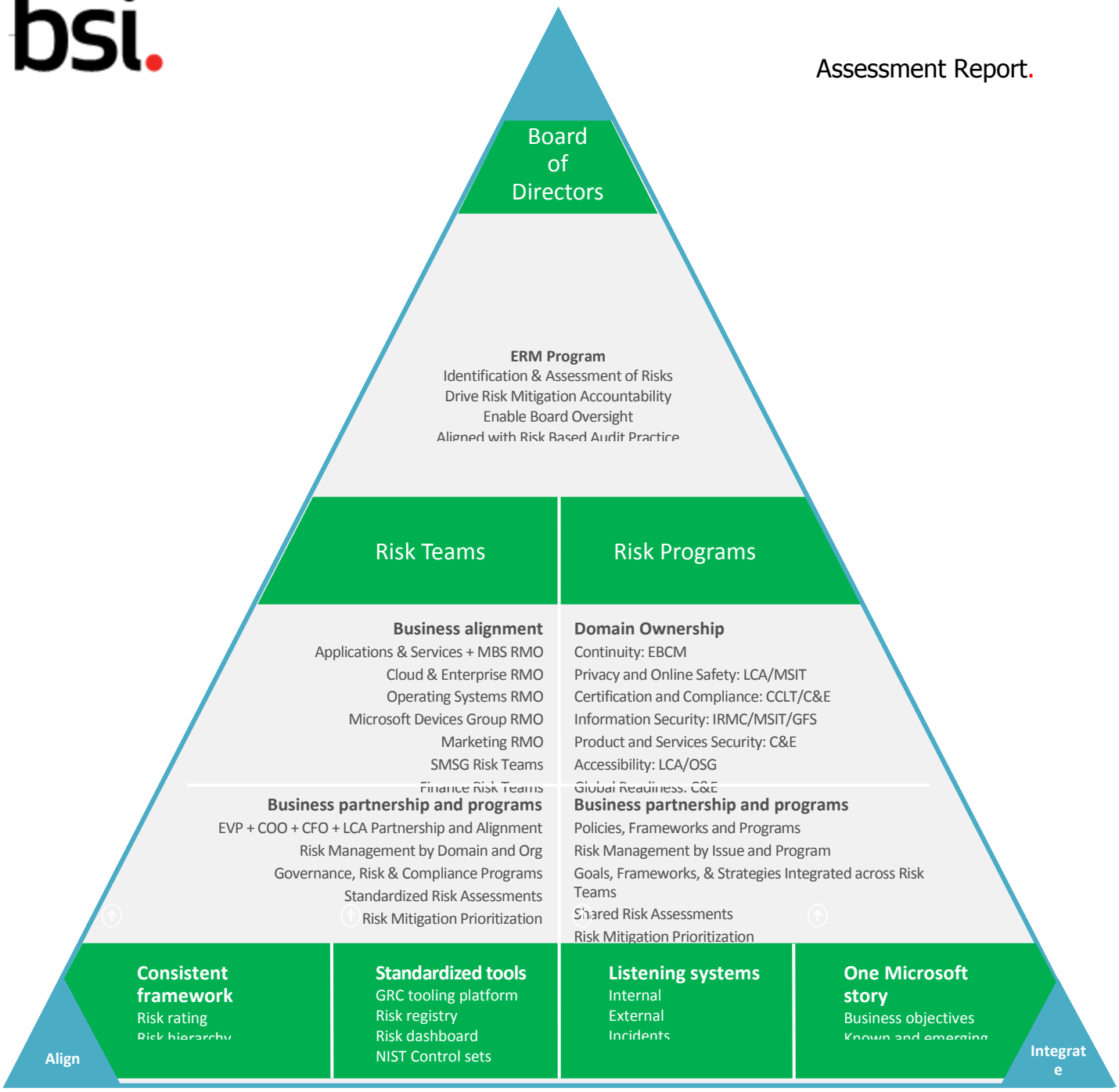
Relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements were already previously identified, documented and kept up to date for each information system and the organization. --- There are no new requirements for the new services being added to the scope. For details concerning privacy please refer to section "Privacy Management - ISO 27018 (All Services) " in this report.

Same for Supplier Relationship --- there are no new suppliers due to addition of the new services, process and controls remain unchanged and unaffected by new services. .

Planning / Operations - Risk Assessment, Analysis and Treatment and Exceptions Management: Clause 6, 8, 10

The organization follows an enterprise risk management process which identifies risk at following levels:

- Strategic
- Legal
- Operational
- Financial



Risk scope is computed based on following formula:
Inherent Risk = Impact* Likelihood
Residual Risk = (Inherent Risk) ((1)- (Control Effectiveness/5)) +((Inherent Risk) /5))
Impact is rated on a scale of 1 to 5 (1 being Mild and 5 being Critical)
Impact Rating Scale:

Impact Rating	Description of Impact				Score (Risk Mgr. Use Only)
	Reputational impact to stakeholders (i.e., customers, shareholders, employees, key partners, Business Groups, subscribers, 3rd Parties)	Legal/ Compliance/ Environmental	Loss of Revenue	Brand Image / Shareholder Value	
Critical	• Critical loss in MSA service, reliant services or internal and external stakeholder groups confidence resulting in legal action, interruption in operations, and/or defection to competition • CPE: Service - Degradation of up to 20% of customers - Loss of approx. 10% of customers • Critical Impact on Employee / workforce - Morale or significant displacement of employees (greater than 25%) - Compensation and/or benefits - Safety of workforce	• Restricted in conducting business in a specific location or line of business - E.g., Windows in Germany, Telecom/Lync • Potential or expected fines or liabilities - E.g., liable for damages, contracts, fines, "can't do this" - Limited ability to provide feedback/influence regulators • Severe impact not meeting legal requirements or contractual obligations or defend against potential or existing lawsuits	Rev. Loss up to 10%	• Major visibility with severe impact to product/service image, brand name or market share • Major traditional and online media attention • Major impact to the public perception of the value of the company	5
Severe	• Severe losses to MSA service, reliant services, and other internal stakeholders • CPE: Service - Degradation of approx. 10% of customers - Loss of approx. less than 5% of customers • Severe impact to overall customer satisfaction	• Restricted in conducting business in a specific location or line of business - E.g., Windows in Germany, Telecom/Lync • Potential or expected fines or liabilities - E.g., liable for damages, contracts, fines, "can't do this" - Limited ability to provide feedback/influence	Rev. Loss up to 5%	• Severe impact to product/service image or brand name • Severe traditional and online media attention • Severe impact to the public perception of the value of the company	4
Serious	• Serious loss to MSA service and reliant services • Service degradation up to 5% of customers • Serious impact to overall long term customer satisfaction	• Potential or expected fines or liabilities - E.g., liable for damages, contracts, fines, "can't do this" - Able to mitigate damages/influence regulators • Serious impact not meeting legal requirements or contractual obligations or defend against potential or existing lawsuits	Rev. Loss up to 3%	• Serious impact to product/service image, brand name or market share • Serious traditional and online media attention • Serious impact to the public perception of the value of the product/service	3
Moderate	• Moderate short-term loss to MSA service	• Potential or expected fines or liabilities - E.g., liable for damages, contracts, fines, "can't do this" • Moderate impact not meeting legal requirements or contractual obligations or defend against potential or existing lawsuits	Rev. Loss up to 2%	• Moderate visibility with little or no impact to product/service image, brand name or market share • Moderate traditional and online media or other inquiries anticipated • Moderate impact to the public perception of the value of the product/service	2
Mild	• Minimal Impact	• Minimal Impact	Rev. Loss up to 1%	• Minimal Impact	1

Likelihood Rating Scale

Likelihood is rated on a scale of 1 to 5 (1 being Slight and 5 being Expected)
Control Effectiveness is rated on a scale of 1 to 5 (1 being Very Low and 5 being Very high)

Likelihood Rating	Consideration	Description of Likelihood		Score
		Probability	Frequency	
Expected	The risk event or circumstance is relatively certain to occur, or has occurred within the past year	90 - 100%	Weekly	5
Highly Likely	The risk event or circumstance is highly likely to occur	70-90%	Monthly	4
Likely	The risk event or circumstance is more likely to occur than not	50-70%	Quarterly	3
Not Likely	The risk event or circumstance occurring is possible	10-50%	Semi-Annually	2
Slight	The risk event or circumstance is only remotely probable	< 10%	Annually	1

Control Effect Rating Scale

CE Rating	Improvement Opportunities	Control Effectiveness (CE)/ Management Activities	Additional Scoring Criteria	Score
Very High	None Identified	Properly designed and operating as intended.	There are no outstanding High or Medium risk audit issues, no material weaknesses or significant deficiencies.	5
High	Limited	Properly designed and operating, no significant deficiencies.	There are no outstanding High risk audit issues, no material weaknesses or significant deficiencies.	4
Moderate	Moderate	In place, some deficiencies.	There are no outstanding High risk audit issues. There may be some significant deficiencies.	3
Low	Significant	Limited, high level of risk remains, significant deficiencies.	There are outstanding High and/or Medium risk Audit issues or significant deficiencies.	2
Very Low	Critical	Non-existent or has major deficiencies and do not operate as intended.	There are outstanding High risk audit issues or material weakness(es).	1

Risk acceptance criteria is defined as below;
IR > 10 and CS =< 3 Improve (Action Required)
IR > 10 and CS > 3 Monitor
IR=<10 and CS =< 3 Tolerate
IR=<10 and CS > 3 Operate

Risk Treatment Options

Risk Classification	Risk Action	Numerical Values	Definition
Improve	Reduce or Mitigate	IR > 10 CS =< 3.0	Areas of high-risk exposure with a low level of control must be key priority for improvements in management and control activities.
Monitor	Reduce or Mitigate	IR > 10 CS > 3.0	Monitoring areas of high-risk exposure where controls deemed adequate provide ongoing assurance of control effectiveness.
Tolerate	Validate and Monitor	IR =< 10 CS =< 3	The organization accepts that areas of low risk exposure where controls are deemed adequate.
Operate	Validate	IR =< 10 CS > 3	Areas of low risk exposure with a high level of control may generate opportunities to optimize the management and control activities.

Risk acceptance approval matrix defines who has the authority to accept risk depending upon the type of risk.

Exception Management process is established and followed. Exception is granted only for 6 months at maximum. Exceptions are triggered from following sources:
- Secure development lifecycle (SDLC)
- Data Handling requirement
- Internal Audit
- Risk Assessment
- Self reported

Each service has identified a Risk Champion who is responsible for Risk assessment for the service.

Risk Assessment is conducted on annual basis by services (the process is governed centrally by a dedicated team) and is following the enterprise defined framework.

Sampled the risk assessment for "Application Proxy" and noted Risk treatment plans are tracked through tickets in TFS and following were the ratings:

- Improve - 4
- Monitor - 4

- Tolerate - 10
- Operate - 1

Reviewed another sample for "Azure Analysis Service" and noted risk assessment was appropriately conducted on 28 Mar 2018.

Reviewed the following ISMS documents:
- Azure ISMS Manual dated on 04/20/2018 version #2018.01
- Azure ISMS Scope Statement dated on 04/20/2018 version #2018.01
- Azure Statement of Applicability dated 4/16/2018 version #2018.01

Risk Assessment ---- reviewed for all newly added service and confirmed that the required risk assessments have been conducted:

Service	Most recent review	Next review	Comment
Advance Threat Protection	Oct-09-2018	April-09-2019	In Compliance
Azure Stack Bridge	Jun-12-2018	Jan-12-2019	In Compliance
Archive Storage	Jun-17-2018	Jan-17-2019	In Compliance
Power query Online	OCt-19-2018	April-19-2019	In Compliance
D365 Integrator	June-23-2018	Jan-23-2019	In Compliance
Azure 3D Data Preparation	June-12-2018	March-31-2019	In Compliance
Video Indexer	Aug-26-2018	Feb-26-2019	In Compliance
Translator	Oct-18-2018	April-18-2019	In Compliance
xStore	April-05-2018	Oct-05-2018 (Past due)	Assessment was completed within the MSFT corporate requirements. Past due is an in internal flag triggered at 6 months to ensure services stays compliant with the corporate guidelines of annual assessment.

Leadership commitment / Management Responsibility/ Management review / Compliance: 5, 9; A.5, A.6, A.18.1.1, A.18.1.3, A.18.2

During the audit, it was evidenced at every level; top management demonstrates leadership and commitment with respect to the ISMS by:

1. ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
2. ensuring the integration of the ISMS requirements into the organization's processes;
3. ensuring that the resources needed for the ISMS are available;
4. communicating the importance of effective ISMS and of conforming to the ISMS requirements;
5. ensuring that the ISMS achieves its intended outcome(s);
6. directing and supporting persons to contribute to the effectiveness of the ISMS;
7. promoting continual improvement; and
8. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Microsoft Azure Top management is reviewing the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management reviews address:

1. the status of actions from previous management reviews;
2. changes in external and internal issues that are relevant to the information security management system;
3. feedback on the information security performance, including trends in:
    a. nonconformities and corrective actions;
    b. monitoring and measurement results;
    c. audit results;

Leadership Commitment –

Reviewed example of the semester Planning Timeline showing:

- Documented the commitments of the previous semester and performance against those said commitments.

- Defined compliance goals, for instance, 100 % compliance to ISO for ring 0 to ring 2 services (service rings are assigned to service offerings based on predetermined criteria)
- Listed in depth certification coverage for Core Certification programs (ISO / SOC / PCI / FedRAMP)

In addition, relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements have been identified, documented and kept up to date for each information system by Microsoft CELA, which is the legal organization outside of the Azure certification.

Privacy and protection of personally identifiable information is ensured as required in relevant legislation and regulation where applicable. For more detail concerning Privacy please refer to section "**Privacy / ISO 27018 specific control (included in SOA): A.18.1.4, A.19 and A.20, ISO 27018 controls"**

Reviewed the organization's approach to managing information security and assessments conducted independently at planned intervals or when significant changes occur.

Also, reviewed service readiness and onboarding as a part of the ISMS review.

Controls surrounding the Leadership review and commitment are operating effectively.

Internal Audit / Improvement: 9.2 / 10

An internal audit was performed by Ernst & Young (with same qualified audit team as past audits) to review the effective integration of the newly added services to the scope of the ISMS. Reviewed: Scope expansion Internal Audit report dated Nov-06-2018 (original release last week and updated on day of audit).

Internal audit outcome: "Effective Control System, over areas Audited"

Sample size used in internal audit follows the standard sampling methodology (e.g. based on frequency of activity performed).

Capability Strengths mentioned:

- Service that onboard to the ISMS follow common processes and controls
- Azure is following leading practice by consolidating multiple ISO management systems
- Ability to monitor and provide reporting of services availability in real-time, internally within Microsoft as well as external to customers
- High level of engagement and commitment by Microsoft Azure Management to frequently review and improve service delivery

If and when issues are noted they are addressed by suitable actions in a timely manner, these actions are tracked and reviewed by management to ensure effective implementation. During the aforementioned internal audit one issue noted related to the JIT, the root cause analysis/investigation was in progress at the time of audit.

Controls surrounding the Internal Audit and Improvement processes are operating effectively.

Cryptography (All services): A.10

Reviewed cryptography Control SOP version 2018.01 dated Jan 07, 2018

Cryptographic policy is evolved and modified from following triggers:
- Security Exposure
- Outages
- Compliance Violation
- Poor resolution time in case of security incident
- Customer specific requirement on cryptographic control

The apex authority on cryptographic related issues lies with Cryptography board who review and approve the policy.

For application secrets related cryptographic controls, following aspects are addressed here:

- Certificate Authentication
- AWS S3/ Azure Storage
- AD Authentication
- Key Management

Process of Cryptography undergoes following steps:

- Discover
- Eliminate
- Centralize
- Automate
- Monitor

Process of encryption of Data at rest was sampled, which is as below:
- Server side encryption can be managed by either MS Azure service or by customer himself

- Customer side encryption are always managed by customer

Access of users or applications to the key vault, is controlled through Azure AD authentication and/or Managed service identity process.

Key rotation schedule is included in the above procedure. Examples;
- Domain password 70 days
- SQL string 90 days
- Self signed certificate 2 Years

During the audit following services were sampled to verify that cryptographic controls are implemented.

Application Proxy Service - noted rotation for following secret type:
- Password
- certificate
- Symmetric Key

Azure Analysis Service reviewed key rotation samples for following secret type:
- Certificate
- Storage Account Keys

The organization has established KPIs for cryptographic controls. KPIs on cryptographic controls are monitored through service 360 tool. For instance KPI for Microsoft Stream included parameters like Expiry, Rotation

Event logs are monitored for the system/servers controlling the cryptographic process. Alerts are generated to remind the target date for rotation of cryptographic key.

Cryptographic algorithms used and required key rotation schedule is defined and adherence is baked into the reporting system.

https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest

https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices

https://www.microsoft.com/en-us/trustcenter/security/encryption

Controls surrounding Cryptography process are operating effectively.

Physical and Environmental Security: A:11

During the visit of the offices in Redmond it was confirmed that Security perimeters were defined and used to protect areas that contain either sensitive or critical information. Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access. All visitors must register with security guard each day and present (upon request) Government issued photo ID.

Physical and environmental controls at each of the visited datacenters were verified.

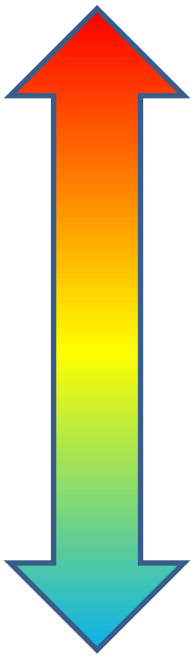
Controls surrounding Physical and Environmental Controls are operating effectively.

Incident Management (All Services): A.16

The organization has established a process to manage information security incidents, which details;
- responsibilities (On call team for all services are identified and communicated to related interested parties)
- appropriate tool to report and track incidents
- Trainings are provided to make employees aware of incidents reporting
- Immediate containment
- Root Cause analysis
- Recording of evidence
- Corrective action

C+AI Incident Management

- Driven by the C+AI Incident Management SOP
- SOP defines both Availability Incidents and Security Incidents/Events
- Security events driven by a specialized team (MSRC)
    - 24x7 Triage team
    - Oncall/Follow the Sun Investigations team
    - Oncall Incident Management
- Defines
    - Phases/Procedures
    - Roles
    - Authority
    - Metrics/Self improvement
- Derived from industry best practices and Microsoft legacy
- Tied to contractual commitments
- Incorporates GDPR requirements

<table>
<tr><td colspan="3">1. Detect</td></tr>
<tr><td colspan="2">Many sources of detection
Detected events / alarms
Customer service / secure@Microsoft.com reports
Service team escalations
http://reportitnow (shown right) →
Cross escalation procedures with partners
Service teams expected to respond to security events 24*7
Cyber Defense Operations Center (cdoc) staffed 24*7</td><td></td></tr>
<tr><td colspan="3">2. Assess</td></tr>
<tr><td>Security engineer has received escalation
Goals
Provide preliminary analysis of risk
Escalate internally if appropriate
Determine if the issue needs to be further diagnosed
Steps by Security
Make the initial determination whether an event impacts system or data security.
Mobilize additional security response and investigation personnel.
Alert Communications, CELA, or additional LiveSite personnel as necessary.
Make a determination in coordination with CELA whether to begin execution of the CRSI Sub-Process.
Determine severity per severity Matrix
Subject to change an investigation progresses</td><td>  </td><td>Severity 0
Severity 1
Severity 2
Severity 3
Severity 4</td></tr>
<tr><td colspan="3">3. Diagnose</td></tr>
<tr><td>Goals
Troubleshoot and diagnose the event.
Move as quickly as possible to Stage 4, Stabilize and Recover.
Reassess severity
Steps by Security
Mobilize additional investigation and forensic personnel
Ensure that evidence is pulled, analyzed, preserved in a</td><td colspan="2">Security events may be classified as:
False positive: An event that meets detection criteria but is found to be part of a normal business practice and may need to be filtered.
Security Event: Incident which increases the risk that a customer data breach may occur but thus far has not, including violations of security policies,</td></tr>
</table>

forensically sound manner Ensure that only individuals with need to know obtain customer or sensitive security data. Appropriately classify the event → (detailed right) Determine the security impact to other Microsoft services Initiate a Microsoft-wide security incident (also known as a SSIRP) if necessary. Customer Reportable Privacy or Security Incident Execution of this process in parallel (if applicable) Detailed later	*acceptable use policies, or standard security practices.* ***Security Incident:*** *Unlawful or unauthorized access to or use of Microsoft's systems, equipment, or facilities resulting in disclosure, modification, or loss of Customer Data.* ***Privacy Incident:*** *A subtype of Security Incident involving Personal Data or PII (Personally Identifiable Information).*
4. Stabilize/Recover	
Goals Identify mitigation and long term repair options Take emergency mitigation or containment steps, if appropriate Verify customer or business impact has been resolved. Steps by Security Determine what migration options are possible Coordinate mitigation actions Ensure that complete mitigation has/will occur Coordinate with communication, CELA, and executives with regard to customer notification and other reporting obligations	**Example Security Mitigations** • Roll impacted credentials • Shut down/isolate impacted systems • Deploy patch/code fix • Roll back to previous version • Rebuild compromised systems
5. Close	

Any customer impacting event that is also an SLA impacting issue should have a Post Incident Response (PIR) Identify technical or communications lapses, procedural failures, manual errors, process flaws Ensure technical lapses are captured in the form of bugs Evaluate response procedures for sufficiency and completeness The Incident Manager is accountable for drafting the postmortem and maintaining an inventory of all repair items The PIR should contain the following: • Customer/Business Impact • Incident Severity • Root Cause Description • Repair items • Timeline • External Public Statement (if necessary)	

Controls surrounding the Incident Management Process are operating effectively.

Business Continuity Management (All services): A.17

Microsoft Azure has several operational global datacenters. Due to the architecture, sufficient redundancy is ensured. Azure has determined its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

Microsoft Azure has also been certified to ISO 22301 - BSI certificate BCMS 659501. Most recent audit for this certificate was 07/24/2017 with the next audit scheduled for 12/05/2018

The Enterprise Business Continuity Management (EBCM) Office provides the governance, oversight, and support for Business Continuity Management (BCM) across Microsoft.

The Mission is defined as:

To strengthen continuity and resiliency through:
- Collaborating with our global business partners
- Delivering clear and consistent communications
- Providing a consistent, flexible, and streamlined BCM framework
- Embedding continuity concepts and awareness within of services and business processes
- Offering consultative services as appropriate

The Objectives are defined as:

- Ensure the existence of effective, reliable, well-tested plans, systems, and processes
- Integrate enterprise risk-based focus to allow for informed business decisions on risk tolerance, avoidance, and mitigation
- Implement methods to assist business areas to resume business operations quickly, cost-effectively, and with minimal impact on customers

The overall program is managed by the following set of documents that outline from the top down how BCDR is handled:

BCMS – Business Continuity Management System - Manual which documents the Microsoft Azure Platform and Azure based services Business Continuity Management program into the format of an ISO 22301 compliant Business Continuity Management System (BCMS).

Documentation applicable to the development, operation, maintenance and certification of the BSMS includes the documents:

- BCMS Manual – Defines every aspect of the program
- BCMS Risks and Opportunities Document
- Risk Management SOP
- Security Policy
- Business Continuity Management SOP
- Enterprise Business Continuity Management (EBCM) methodology
- Training & Awareness Program SOP
- Document & Record Management SOP
- Third Party Management SOP
- Legal and Regulatory SOP
- Incident Management SOP
- Microsoft Azure Business Continuity Plan – Defines the procedures for people and process recovery
- Microsoft Azure Disaster Recovery Procedures – defines the technology recovery steps for every service
- Other process level Standard Operating Procedure (SOP) documents containing the common control process descriptions along with any service level unique controls' implementation procedures relevant to business continuity

Service Health & Compliance Reporting score card reviewed (Q3FT18 EBCM Executive Scorecard)

Azure Regions – Alternate Processing
Azure is architected to provide resiliency for the most common occurring failures (hard drives, server (service healing, fault domains) automatically – Regional High Availability. Regions are partitioned to contain failures and provide service resiliency.

The BCDR program addresses region loss and alternate region recovery through its program of planning and testing. BCDR addresses the rare widespread catastrophic events that require cross-region recovery due to loss of an entire Azure region. Regions (alternate processing sites) are in separate fault zones (not susceptible to the same regional hazards) & and are physically and logically isolated.

Azure Storage

All data stored has continuous replication in-region, geo-replication & validation (alternate region) which meets the requirement for backup integrity testing. Data replication uses multiple copies - 3 copies within each region and 3 copies where the data is geo-replicated (cross region backup). PITR (Point in time restore) is available via backups that the customer can choose for archival and data retrieval purposes

Azure Security

All services recovered to alternate regions have "like for like" security controls ensuring no vulnerability exposure in the recovery of services

Resource management

Users can distribute compute instances across regions by creating a separate cloud service in each target region, and then publishing the deployment package to each cloud service. However, note that distributing traffic across cloud services in different regions must be implemented by the application developer or with a traffic management service.

Load Balancing – Locally and Cross Region

To load balance traffic across regions requires a traffic management solution. Azure provides Azure Traffic Manager. You can also take advantage of third-party services that provide similar traffic management capabilities.

Strategies

Many alternative strategies are available for implementing distributed compute across regions. These must be tailored to the specific business requirements and circumstances of the application. At a high level, the approaches can be divided into the following categories:

Redeploy on disaster: In this approach the application is redeployed from scratch at the time of disaster. This is appropriate for non-critical applications that don't require a guaranteed recovery time.

Warm Spare (Active/Passive): A secondary hosted service is created in an alternate region, and roles are deployed to guarantee minimal capacity; however, the roles don't receive production traffic. This approach is useful for applications that have not been designed to distribute traffic across regions.

Hot Spare (Active/Active): The application is designed to receive production load in multiple regions. The cloud services in each region might be configured for higher capacity than required for disaster recovery purposes. Alternatively, the cloud services might scale out as necessary at the time of a disaster and failover. This approach requires substantial investment in application design, but it has significant benefits. These include low and guaranteed recovery time, continuous testing of all recovery locations, and efficient usage of capacity.

Recovery by using Geo-Redundant Storage of blob, table, queue and VM disk storage

In Azure, blobs, tables, queues, and VM disks are all geo-replicated by default. This is referred to as Geo-Redundant Storage (GRS). GRS replicates storage data to a paired datacenter hundreds of miles apart within a specific geographic region. GRS is designed to provide additional durability in case there is a major

datacenter disaster.

A complete discussion of distributed design is outside the scope of this document. For further information, see Disaster Recovery and High Availability for Azure Applications.

Controls surrounding the Business Continuity Management Process are operating effectively.

Privacy Management - ISO 27018 (All Services): A.18.1.4, A.19 and A.20, ISO 27018 controls

All reviewed services had their privacy reviews in order to be on-boarded.

There were no material changes related to the Privacy Management Program.

Reviewed the Microsoft Online Service Terms (OST) – which is a customer-facing and Microsoft-wide (not just azure specific) document containing the Data Processing Terms which define additional commitments to privacy and security for certain online services.

The OST is publicly available via the following URL: https://azure.microsoft.com/en-us/support/legal/ Online Services Terms (OST) includes the Data Processing Terms (DPT). Document is available as a download only

The OST is publicly available via the following URL: https://azure.microsoft.com/en-us/support/legal/
The OST was reviewed against the following controls:

- A.1 Consent and Choice
  - A.1.1, Obligation to co-operate regarding PII principals' rights
- A.2 – Purpose, legitimacy and specification
  - A.2.1, Public Cloud PII controller's purpose
  - A.2.2, Public Cloud PII processor's commercial use
- A.4.1, Secure erasure of temporary files
- A.5 Use, retention and disclosure limitation
  - A.5.1, PII Disclosure Notification
  - A.5.2, Recording of PII Disclosures
- A.7.1, Disclosure of Sub-Contracted PII processing
- A.9.1, Notification of a data breach involving PII
- A.9.3, PII Return, transfer and disposal
- A.10.1, Confidentiality or non-disclosure agreements
- A.10.2, Restriction of creation of hard copy material
- A.10.3, Control and logging of data restoration
- A.10.4, Protecting data on storage media leaving the premises

- A.10.5, Use of unencrypted storage media
- A.10.6, Encryption of PII transmitted over public networks
- A.10.7, Secure disposal of hardcopy materials
- A.10.8, Unique use of identifiers
- A.10.9, Records of authorized users
- A.10.10, Identifier Management
- A.10.11, Contract Measures
- A.10.12, Sub-Contracted PII Processing

Additionally, it was also reviewed for the Microsoft defined controls.

Controls surrounding Privacy and ISO 27018 standard are operating effectively.

Azure Service and process overview:

Microsoft Azure is a growing collection of integrated cloud services that developers and IT professionals use to build, deploy, and manage applications through our global network of datacenters.

Microsoft Azure provides a public facing website at https://azure.microsoft.com/en-us/status/ displaying the real time the service availability. Below is the assessment on the sampled services from expansion audit scope.

Archive Storage:

Service Overview:
Archive storage is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Process Overview

Service Architecture	Architecture diagram reviewed
Access Management	Verified that Service has been onboarded to Access Management
Cryptography	confirmed that "standard" Microsoft technology and processes are used. The following secret types were reviewed and confirmed to be managed:

	- Certificates (Azure KeyVault) - Certificate (DSMS) - Storage Account (DSMS) - Storage Account (SecretStore)
Change management	Examples Change ticket: 12990380 - Release to Operations – VEName Confirmed that submitter and approvers where different - separation of duties Azure Security Pack is installed to ensure that security event are logged and monitored and subsequently suitable actions are initiated (via ICM ticket for alerting)
Audit Logging and Monitoring	Verified example IcM ticket raised due tape not in right slot. Sev 3 level Incident with resolution duration 23h57miniutes. Incident ticket #85714433
Secure Development Lifecycle	Team completed their SDL on Sept-13-2018 recorded via SDL ticket # 2450276
BC/DR	Onboarded to BC/DR within Azure assessment report dated April-12-2018
Incident management	Reviewed Incident ticket # 8571443
Privacy	Privacy review # 2450247 dated Oct-04-2018

Microsoft Translator:
Service Overview:

Provides services for text and speech translator - Machine translator

Process Overview

Service Architecture	Reviewed Service Overview Diagram; Available within several Microsoft Solutions as well as available as API so 3rd party can use the Azure service. Authentication services is utilized to ensure that only authorized requested are processed
Access Management	Access Management: User access review (about 45) confirming that the team has been on boarded into the Azure environment.
Cryptography	Contains only Certificate secrets.
Change management	Change deployment ticket# 95335 dated Oct-03-2018 Confirmed in ticket that different individuals were involved (separation of duties).
Audit Logging and Monitoring	Azure Security Pack installed.
Secure Development Lifecycle	SDL review sept-25-2018 Ticket 2824793
Incident management	Sample of Incident management Sev 4 e.g. "bad" translations 79523609 dated Aug-07-2018
BD/DR	Azure utilized by service. Test record reviewed 10/26/2018
Privacy	Privacy review / Assessment dated: 12/5/2017 ticket# 1725212

Azure Advanced Threat Protection:

Service Overview:

Is an enterprise cyber-security cloud services which allows to:

- Detect and investigate advanced attacks on-premises and in the cloud
- Identify suspicious user and device activity with both known-technique detection and behavioral analytics
- Analyze threat intelligence from the cloud and on-premises
- Protect user identities and credentials stored in Active Directory
- View clear attack information on a simple timeline for fast triage
- Monitor multiple entry points through integration with Windows Defender Advanced Threat Protection

Process Overview

Access Management	Access management – User Access Reviews
Cryptography	Service only uses certificate secrets
Change management	Change management: Ticket 1054281 Make Scaling Configurable --- also verified in the life system.
Audit Logging and Monitoring	Confirmed that the Security Pack was used / deployed.
Secure Development Lifecycle	Confirmed SDL is used by the team … ticket# 2982208 Security of Azure ATP SDL 2019 H1 of Azure Advanced Threat Protection
BC/DR:	Confirmed report 3/29/2018 report dated: 4/13/2018 and confirmed service conforms to the Microsoft standard process.
Incident management	Incident # Sev 4 87934791 closed within 19H ---- configuration to limit the number of agents of domain controller. Incident management: on call list
Privacy	Privacy report / review Feb-14-2018 ticket 1510388 AATP Compliance review

Power Query Online:
Service Overview:

Power Query is a data connection technology that enables users to discover, connect, combine, and refine data sources to meet your analysis needs. ---- it is the web equivalent of the Power Query Desktop Component

Process Overview

Access Management	Access Management – User Access Reviews --- quarterly done
Cryptography	Service uses only certificates stored at AzureKeyVault
Change management	Change management Ticket 124964 - bug raised due to with compatibility of a particular browse
Audit Logging and Monitoring	Azure Secure Pack Installed
Secure Development Lifecycle	SDL review performed on Aug-30-2018 Ticket number 104141 Security for PQO SDL renewal 07/2018
Incident management	Incident managed sample ticket # 82606138 sev 2 --- impact duration 20m Oncall list confirmed for 24X7 support
BC/DR	review / assessment March-08-2018 next due march-08-2019
Privacy	Privacy review and sign off ticket 79480 dated 10/17/2018

Not sampled this time:

Video Indexer
Microsoft Azure 3D Data Preparation

Next visit objectives, scope and criteria

The objective of the assessment is to conduct a surveillance assessment and look for positive evidence to ensure the elements of the scope of certification and the requirements of the management standard are effectively addressed by the organisation's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organisations specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan.

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001 / ISO 27018 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

ISO 27001 / ISO 27018
Microsoft Corporation/ Microsoft Azure management system documentation

Please note that BSI reserves the right to apply a charge equivalent to the full daily rate for cancellation of the visit by the organization within 30 days of an agreed visit date. It is a condition of Registration that a deputy management representative be nominated. It is expected that the deputy would stand in should the management representative find themselves unavailable to attend an agreed visit within 30 days of its conduct.

Next Visit Plan

Date	Auditor	Time	Area/Process	Clause
Date: TBD Datacenter Visit: Boydton (BN1/3/4/6)				
TBD	8:30	WF	Arriving / check-in process	
	9:00		Opening meeting	
	9:30		Site overview	
			High Level Information	
			Onsite Vendors	
			DC Access Management	
			Electrical, Mechanical and Fire Management	
	12:00		Working Lunch / Logistics Overview	
	12:30		Facility Tour / Asset management	
	13:00		SOC / NOC (as applicable to site)	
	14:30		Report Preparation	
	16:00		Daily-sync	
	16:30		Leaving site	
Date: TBD Datacenter Visit: Humacao				
TBD	8:30	WF	Arriving / check-in process	
	9:00		Opening meeting	
	9:30		Site overview	
			High Level Information	
			Onsite Vendors	
			DC Access Management	
			Electrical, Mechanical and Fire Management	
	12:00		Working Lunch / Logistics Overview	

	12:30		Facility Tour / Asset management	
	13:00		SOC / NOC (as applicable to site)	
	14:30		Report Preparation	
	16:00		Daily-sync	
	16:30		Leaving site	
Date: TBD Datacenter Visit: Dublin				
TBD	8:30	WF	Arriving / check-in process	
	9:00		Opening meeting	
	9:30		Site overview	
			High Level Information	
			Onsite Vendors	
			DC Access Management	
			Electrical, Mechanical and Fire Management	
	12:00		Working Lunch / Logistics Overview	
	12:30		Facility Tour / Asset management	
	13:00		SOC / NOC (as applicable to site)	
	14:30		Report Preparation	
	16:00		Daily-sync	
	16:30		Leaving site	
Date: TBD Datacenter Visit: Amsterdam 3				
TBD	8:30	WF	Arriving / check-in process	
	9:00		Opening meeting	
	9:30		Site overview	
			High Level Information	
			Onsite Vendors	
			DC Access Management	

			Electrical, Mechanical and Fire Management	
	12:00		Working Lunch / Logistics Overview	
	12:30		Facility Tour / Asset management	
	13:00		SOC / NOC (as applicable to site)	
	14:30		Report Preparation	
	16:00		Daily-sync	
	16:30		Leaving site	
Date: TBD **Datacenter Visit: Amsterdam 5**				
TBD	8:30	WF	Arriving / check-in process	
	9:00		Opening meeting	
	9:30		Site overview	
			High Level Information	
			Onsite Vendors	
			DC Access Management	
			Electrical, Mechanical and Fire Management	
	12:00		Working Lunch / Logistics Overview	
	12:30		Facility Tour / Asset management	
	13:00		SOC / NOC (as applicable to site)	
	14:30		Report Preparation	
	16:00		Daily-sync	
	16:30		Leaving site	
Date	**Auditor**	**Time**	**Area/Process**	**Clause**
July-08, 2019				
7/8	WF + 2nd auditor	8:30	Opening Meeting	
			Scope and Policy	
			Organizational context	
			Leadership and Commitment	

		12:00	Lunch break	
		12:30	Management System Support	
			Planning and Resources	
			Objectives / Performance Monitoring & Measurement / Management Review	
		16:00	Auditor's caucus	
		16:30	Daly close out meeting	
		17:00	Leaving	
July-09, 2019				
7/9	WF + 2nd auditor	8:30	Follow-up open items	
			Control of Documents and Records	
			Internal Audits	
			Actions / Non-Conformity / Incidents / Complaints / Improvement	
		12:00	Lunch break	
			Risk Management / Prevention	
			A.5 Information security policies	
			A.6 Organization of information security	
		16:00	Auditor's caucus	
		16:30	Daly close out meeting	
		17:00	Leaving	
July-10, 2019				
7/10	Both auditors	8:30	Follow-up open items	
	Willy		A.7 Human resource security	
			A.8 Asset management	
			A.9 Access control	
	2nd auditor		A.10 Cryptography	
			A.11 Physical and environmental security	
		12:00	Lunch break	

	Both auditors		27018 specific areas	
		16:00	Auditor's caucus	
		16:30	Daly close out meeting	
		17:00	Leaving	
July-11, 2019				
7/11	Both auditors	8:30	Follow-up open items	
	Willy		A.15 Supplier relationships (incl. 3rd datacenters)	
	2nd auditor		STAR specific areas	
		12:00	Lunch break	
	Both auditors		Continuation from morning	
		16:00	Auditor's caucus	
		16:30	Daly close out meeting	
		17:00	Leaving	
July-12, 2019				
7/12		8:30	Follow-up open items	
		12:00	close out meeting	
		12:30	Leaving	

Appendix: Your certification structure & ongoing assessment programme

Scope of Certification

IS 577753 (ISO/IEC 27001:2013)

Information Security Management System (ISMS) includes management of information security, privacy and compliance in the areas: infrastructure, development, security and engineering services/systems, operations and support for the following Azure Services deployed in the Azure, Azure Government and Azure Germany environments as documented in the ISMS Statement of Applicability version 2018.02 dated 10/4/2018:

Services in Scope by Environment:

(newly added services are marked as *)

Product Category	Offering / Service	Public	Fairfax	Blackforest
Microsoft Datacenters				
Microsoft Datacenter and Operations Service		✓	✓	✓
Azure				
Compute	App Service	✓	✓	✓
	Batch	✓	✓	✓
	Cloud Services	✓	✓	✓
	Functions	✓	✓	✓
	Service Fabric	✓	✓	✓
	Virtual Machines (including SQL VM)	✓	✓	✓
	Virtual Machines Scale Sets	✓	✓	✓

Networking	Application Gateway	✓	✓	✓
	Azure DDOS Protection	✓	✓	✓
	Azure DNS	✓	✓	✓
	Content Delivery Network	✓	-	-
	ExpressRoute	✓	✓	✓
	Load Balancer	✓	✓	✓
	Network Watcher	✓	✓	✓
	Traffic Manager	✓	✓	✓
	Virtual Network	✓	✓	✓
	VPN Gateway	✓	✓	✓
Storage	Backup	✓	✓	✓
	Archive Storage*	✓	-	-
	Cool Storage	✓	✓	✓
	Import/Export	✓	-	-
	Premium Storage	✓	✓	✓
	Site Recovery	✓	✓	✓
	Storage (Blobs (including Azure Data Lake Storage Gen 2), Disks, Files, Queues, Tables)	✓	✓	✓
	StorSimple	✓	✓	-
Web + Mobile	App Service: API Apps	✓	✓	✓
	App Service: Mobile Apps	✓	✓	✓

	App Service: Web Apps	✓	✓	✓
	Azure Search	✓	-	-
	Media Services	✓	✓	✓
	Notification Hubs	✓	✓	✓
Containers	Azure Container Service (ACS)	✓	-	-
	Azure Kubernetes Service (AKS)	✓	-	-
	Container Instances	✓	-	-
	Container Registry	✓	-	-
Databases	Azure Cosmos DB	✓	✓	✓
	Azure Database for MySQL	✓	✓	-
	Azure Database for PostgreSQL	✓	✓	-
	Azure Database Migration Service	✓	-	-
	Azure SQL Database	✓	✓	✓
	Redis Cache	✓	✓	✓
	SQL Data Warehouse	✓	✓	✓
	SQL Server Stretch DB	✓	✓	✓
Analytics	Azure Analysis Services	✓	✓	✓
	Data Catalog	✓	-	-
	Data Factory	✓	-	-
	Data Lake Analytics	✓	-	-
	Data Lake Storage Gen 1	✓	-	-

	HDInsight	✓	✓	✓
	Stream Analytics	✓	-	✓
AI + Machine Learning	Azure Bot Service	✓	-	-
	Speech Services (formerly Custom Speech Service and Bing Speech)	✓	-	-
	Cognitive Services: Computer Vision API	✓	-	-
	Cognitive Services: Content Moderator	✓	-	-
	Cognitive Services: Custom Decision Service	✓	-	-
	Cognitive Services: Custom Vision Service	✓	-	-
	Cognitive Services: Emotion API	-	-	-
	Cognitive Services: Face API	✓	✓	-
	Cognitive Services: Language Understanding Intelligent Service (LUIS)	✓	-	-
	Cognitive Services: Text Analytics API	✓	✓	-
	Machine Learning Services	✓	-	-
	Machine Learning Studio	✓	-	✓
	Microsoft Translator*	✓	✓	-
	QnAMaker Service	✓	-	-
	Video Indexer*	✓	-	-
	Microsoft Genomics	✓	-	-
Internet of Things	Azure Maps	✓	-	-
	Event Grid	✓	-	-

	Event Hubs	✓	✓	✓
	IoT Hub	✓	✓	✓
	Microsoft IoT Central	✓	-	-
	Time Series Insights	✓	-	-
Integration	Logic Apps	✓	✓	-
	Service Bus	✓	✓	✓
Security + Identity	Azure Active Directory (Free, Basic, Premium)	✓	✓	✓
	Azure Active Directory (AAD) Domain Services	✓	-	-
	Azure Active Directory B2C	✓	-	-
	Azure Advanced Threat Protection*	✓	-	-
	Azure Information Protection	✓	-	-
	Key Vault	✓	✓	✓
	Microsoft Accounts	✓	-	-
	Multi-Factor Authentication	✓	✓	✓
	Security Center	✓	✓	-
Developer Tools	Application Insights	✓	-	-
	API Management	✓	✓	-
	Azure DevTest Labs	✓	✓	-
Monitoring + Management	Automation	✓	✓	-
	Azure Advisor	✓	✓	-
	Cloud Shell	✓	-	-

	Azure Migrate	✓	-	-
	Azure Monitor	✓	✓	✓
	Azure Policy	✓	✓	✓
	Azure Resource Manager	✓	✓	✓
	Azure Service Health	✓	✓	✓
	Log Analytics	✓	✓	-
	Microsoft Azure Portal	✓	✓	✓
	Scheduler	✓	✓	✓
Azure Supporting Infrastructure Services				
Microsoft Online Services				
Microsoft Graph		✓	-	-
Microsoft Power BI (including Power BI Embedded)		✓	✓	✓
Microsoft Cloud App Security		✓	-	-
Microsoft Flow		✓	-	-
Microsoft Healthcare Bot		✓	-	-
Microsoft Intune		✓	✓	-
Microsoft PowerApps		✓	-	-
Microsoft Stream		✓	-	-
Microsoft Service Map		✓	-	-
Power Query Online*		✓	-	-
Microsoft Azure 3D Data Preparation*		✓	-	-

Azure Supporting Infrastructure and Platform Services

The ISMS for Microsoft's Cloud Infrastructure and Operations encompasses the datacenters listed and functional teams responsible for managing the edge network infrastructure, core servers providing critical shared services and management tools, and the access network infrastructure that supports these critical core services, as well as the remote management of services hosted by third party data centers in accordance with the Microsoft Cloud Infrastructure and Operations ISMS Statement of Applicability version 2018.02 dated 10/04/2018.

Assessed location(s)

The audit has been performed at Central Office.

Redmond / IS 577753 (ISO/IEC 27001:2013)

Location reference	0047306283-000
Address	Microsoft Corporation Microsoft Azure One Microsoft Way Redmond Washington 98052 USA
Visit type	Extension to Scope
Assessment reference	9669407
Assessment dates	11/05/2018
Deviation from Audit Plan	No
Total number of Employees	510
Total persons doing work at this site	510
Scope of activities at the site	Certificate scope applies.
Assessment duration	1 Day(s)

Redmond / PII 665842 (ISO IEC 27018)

Location reference	0047306283-000
Address	Microsoft Corporation Microsoft Azure One Microsoft Way Redmond Washington 98052 USA
Visit type	Extension to Scope

Assessment reference	9669408
Assessment dates	11/07/2018
Deviation from Audit Plan	No
Total number of Employees	510
Effective number of Employees	510
Scope of activities at the site	Certificate scope applies.
Assessment duration	1 Day(s)

Certification assessment program

Certificate Number - IS 577753
Location reference - 0047306283-000

		Audit					
		1	**2**	**3**	**4**	**5**	**6**
Business area/Location	**Date (mm/yy):**	4/17	11/17	6/18	11/18	6/19	4/20
	Duration (days):		1	5	1	5	10
Scope and Policy		X	X	X	X	X	X
Organizational context		X		X	X	X	X
Leadership and Commitment		X		X	X	X	X
Management System Support		X		X	X	X	X
Planning and Resources		X		X		X	X
Human Resource Management		X	X				X
Control of Documents and Records		X		X			X
Objectives / Performance Monitoring & Measurement		X		X		X	X
Management Review		X	X	X	X	X	X
Internal Audits		X	X	X	X		X
Actions / Non-Conformity / Incidents / Complaints		X	X	X	X		X
Risk Management / Prevention		X	X	X	X		X
Improvement		X		X		X	X
A.5 Information security policies		X		X			X
A.6 Organization of information security		X		X			X
A.7 Human resource security		X		X			X
A.8 Asset management		X		X			X
A.9 Access control		X		X		X	X
A.10 Cryptography		X		X			X

A.11 Physical and environmental security	X		X		X	X
A.12 Operations security	X				X	X
A.13 Communications security	X		X			X
A.14 System acquisition, development and maintenance	X				X	X
A.15 Supplier relationships (incl. 3rd datacenters)	X		X			X
A.16 Information security incident management	X				X	X
A.17 Information security aspects of business continuity management	X			X		X
A.18 Compliance	X				X	X
Integration of new services		X		X		

Certificate Number - PII 665842
Location reference - 0047306283-000

		Audit					
		1	**2**	**3**	**4**	**5**	**6**
Business area/Location	**Duration (days):**	4/17	11/17	6/18	11/18	6/19	4/20
	Duration (days):	0.5	0.5	1.5	1	1.5	1.5
Integration audit with Azure		X					
27018 specific controls			X	X	X	X	X

Definitions of findings:

Nonconformity:
Non-fulfilment of a requirement.

Major nonconformity:
Nonconformity that affects the capability of the management system to achieve the intended results. Nonconformities could be classified as major in the following circumstances:

- If there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
- A number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

Minor nonconformity:
Nonconformity that does not affect the capability of the management system to achieve the intended results.

Opportunity for improvement:
It is a statement of fact made by an assessor during an assessment, and substantiated by objective evidence, referring to a weakness or potential deficiency in a management system which if not improved may lead to nonconformity in the future. We may provide generic information about industrial best practices but no specific solution shall be provided as a part of an opportunity for improvement.

Observation:
It is ONLY applicable for those schemes which prohibit the certification body to issue an opportunity for improvement.
It is a statement of fact made by the assessor referring to a weakness or potential deficiency in a management system which, if not improved, may lead to a nonconformity in the future.

How to contact BSI

'Just for Customers' is the website that we are pleased to offer our clients following successful registration, designed to support you in maximizing the benefits of your BSI registration - please go to www.bsigroup.com/j4c to register. When registering for the first time you will need your client reference number and your certificate number

Should you wish to speak with BSI in relation to your registration, please contact our Operations Support Team:

BSI Management Systems
12950 Worldgate Drive
Suite 800
Herndon
VA
20170
Tel: +1 (800) 862 4977 Fax: +1 (703) 437 9001

Notes

This report and related documents are prepared for and only for BSI's client and for no other purpose. As such, BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in

connection with any other purpose for which the Report may be used, or to any other person to whom the Report is shown or in to whose hands it may come, and no other persons shall be entitled to rely on the Report. If you wish to distribute copies of this report external to your organization, then all pages must be included.

BSI, its staff and agents shall keep confidential all information relating to your organization and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. BSI staff, agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

This audit was conducted on-site through document reviews, interviews and observation of activities. The audit method used was based on sampling the organization's activities and it was aimed to evaluate the fulfilment of the audited requirements of the relevant management system standard or other normative document and confirm the conformity and effectiveness of the management system and its continued relevance and applicability for the scope of certification.

As this audit was based on a sample of the organization's activities, the findings reported do not imply to include all issues within the system.

Regulatory compliance

BSI conditions of contract for this visit require that BSI be informed of all relevant regulatory non-compliance or incidents that require notification to any regulatory authority. Acceptance of this report by the client signifies that all such issues have been disclosed as part of the assessment process and agreement that any such non-compliance or incidents occurring after this visit will be notified to the BSI client manager as soon as practical after the event.