Assessment Report

Microsoft Corporation

Assessment dates	02/24/2025 to 02/28/2025 (Please refer to Appendix for details)
Assessment Location(s)	Redmond (001)
Report Author	Katherine Read
Assessment Standard(s)	ISO/IEC 27701:2019, ISO/IEC 27017:2015, ISO/IEC 27001:2022, ISO/IEC 27018:2019, ISO 22301:2019

Table of contents

Executive Summary

This was an annual surveillance audit to verify continued compliance to multiple standards including ISO 27001:2013, ISO 27701:2021, ISO 27018:2020, ISO 27017:2021, ISO 22301:2019, and ISO 27001:2022.

Microsoft 365 has successfully maintained their management system to high standards.
During the audit, samples of evidence were taken from different service line offerings, and all observed to be of a mature nature with no NC's identified as part of this audit. The management system is part of their daily operating practices, and this was evident from speaking with various staff members as part of the interviews and reviewing objective evidence presented. Industry best practices were observed throughout the audit with staff having a clear understanding of the ISO requirements from all standards as part of their daily tasks.

This audit certifies the processes that govern Microsoft 365 (M365) services and support features, which can be purchased in a variety of combinations by customers. For a detailed list of the services in scope, they are outlined in the Microsoft Product Terms for Online Services.
The certificates for M365 (all ISO/IEC 27001, 27017, 27018, 27701 and 22301) are in accordance with the requirements of the activities within the ISMS, PIMS and BCMS.

The report is issued to the entity/client Microsoft Corporation from the corporate headquarters of One Microsoft Way, Redmond, WA 90852.

Although the M365 services are available worldwide, management of all services included in the scope of M365's ISO Certificates are centralized across a standard set of technology, processes, and requirements. While the ISO Audit takes place at the Microsoft corporate headquarters, because of how the M365 services are maintained, all worldwide locations of M365 are included.
Licenses of M365 sold by certified partners including Microsoft affiliates and subsidiaries outside the USA, are serviced by Microsoft Corporation performing contractual obligations. Those commitments are implemented via the ISMS that is operated by the certified entity.

The ISO standards require an audit, which includes a requirement for vulnerability assessment and remediation of issues by the operators of the ISMS under test in this assessment. Additionally, Microsoft has a published policy for customer performance of vulnerability assessment. Such testing can be used by Customers to further assess vulnerability risk in M365 under the Microsoft Cloud Penetration Testing Rules of Engagement.

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.

No change in relation to the audited organization's activities, however the M365 offering has been expanded to include M365 Copilot as one of the product and services covered by the scope of certification was identified.

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 surveillance assessment and look for positive evidence to ensure that elements of the scope of certification and the requirements of the management standard are effectively addressed by the organization's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organization's 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 and where applicable to identify potential areas for improvement of the management system.

The scope of the assessment was defined in the plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria of the assessment was ISO 27001, 27701, 27017, 27018, and 22301 and Microsoft's management system documentation.

Statutory and regulatory requirements

Top management is responsible for determining applicable statutory and regulatory requirements and ensuring compliance.

Assessment Participants

Name	Position	Opening Meeting	Closing Meeting	Interviewed (processes)
Sarah McCoy	PRINCIPAL PM LEAD M365 Core	X	X	X

Assessment conclusion

BSI assessment team

Name	Position
Vikas Dhanker	Team Leader
Kayode Agboola	Team Leader
Katherine Read	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

Context, Leadership, Planning - Scope, Objectives, Policy, Statement of Applicability (4, 5, 6):

Planned activities have been fully realized. Methods for determining process results:
Interview with leadership team
Overview of Microsoft 365 (M365) presentation
M365 is Subscription-based service: M365 suite of cloud-based service offerings in-scope (not limited to): M365 Copilot, EXO, SPO, Teams, Windows 365, Substrate, RDS, EOP, Viva Engage/Yammer, IC3, SIP, M365 Portal (Suite), ODSP (all of which are supported by Azure AD, (which is not in scope of this certification as a service, Azure AD single sign-on enables use of M365 by the customer; SaaS model for on-demand access to applications):
Evidence/Documentation Reviewed:
- Overview of Microsoft 365 Feb25

-M365 Copilot

-Microsoft AI Substrate Intelligence Platform
- Microsoft's Cloud Environment, PaaS, IaaS
- Supporting Services, Suite, Internal Security Tools, RDS, Substrate, IC3
- SharePoint & OneDrive (ODSP), Teams, 365 Web Apps, Windows 365, Viva Engage
- 4.2 Customer Requirements, Management Requirements, Engineering Requirements
- Email, Rajesh Jha Planning memo reviewed which was broken down into FY25 Priorities were reviewed to ensure alignment with the strategic direction while maintaining and improving the ISMS.
- Email, ISMS & PIMS Manual & SoA Review & Approval 02-19-2025
- Microsoft Recruit, Candidate Evaluation
- Microsoft Connect
- 7.3 Awareness, Standards of Business Conduct
- 7.4 Service Updates, Roadmaps, MSR, All Hands, Policy including internal and external communications.
- Audit Calendar 2025
- Internal Audit Report for Purview June 6, 2024 was reviewed-
- 10.1 Control Design, Control Effectiveness, Monthly Service Reviews, GRC Continuous Monitoring
Scope
The management of Microsoft 365 Service's Information Security Management System (ISMS), development, operations, and protection of personally identifiable information (PII), in accordance with the Statement of Applicability dated February 19, 2025.
Microsoft 365 ISO 27001:2022 Annex A Controls Overview - Feb 2025:
-Statement of Applicability dated February 19, 2025, with A.8.30 - excluded (no outsourced development)
A.5.23 (New) Use of Cloud Services: Compliance Manager screenshot - Compliance offerings certification tracker (27K, SOC 2 Type 2, PCI DSS Lvl 1, FedRamp)
A.8.23 (New) Access to External Websites - automatic browser block: Config_EXO.xml screenshot; Config.stable.wml screenshot
A.8.34 IS audit considerations: Penetration testing Rules of Engagement screenshot
A.5.37 - On call websites with best practices

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately

managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Office 365 Risk Management (8.1-8.3; 6.1):

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed:
- Enterprise Risk Management Program
- M365 Service Teams, M365 Security, M365 Trust, M365 Risk Committee
- Risk Management Process
- Risk Rating Criteria: Inherent Impact
- Management Action and Control Opportunities
- Risk Rating, Critical 100 -125, High 60-99.9, Medium 30-59.9, Low 1-29.9
- Risk Treatment Plan
- Email, Annual Risk Review Final Signoff 9/25/2024
- Annual 2024 Risk Assessment Results Handover to ERO 9/27/2024

Compliance Lifecycle is a federated effort, and this is all done basically as where the M365 is governed by the Overall Enterprise Risk Management (ERM) for Microsoft.

Risk Program Objectives
Identify, Assess, manage, ensure accessibility, and aligns with the ERM, in addition they identify security, privacy and compliance risk.

MS 365 Risk Flow
-Inputs - M365 Teams, Security, Trust, and Risk Committee all feed into the ERM which then reports to Senior Leadership and the BOD. All risks raised by product teams go to risk committees. Risk is identified, assessed, developed treatment plan, report to management, and then are monitored. New risks are added to AZURE Devops to track risks within their ADO.
Risks are identified via pen tests, vulnerability scans, and assessments and controls.

-Risks are assessed via MS 365 committees assess new risk by looking at both a quantitative and qualitative risk criteria that has been developed by the organization ERM.
Impact rating criteria which evaluate trust/reputation, operational, legal/compliance/environmental, and enterprise value. This is done on a scale of 1-5 with 1 being minimal and 5 being critical.
For likelihood, this has is assigned a probability rating ranging from >5%-100% and 1-5, 1 being remote probability and 5 being an expected probability.

-Control opportunities are assessed which lists general, accountability, investment, metrics and monitoring, control validation and financial controls, with a range of 1 being very low to 5 being very high.
Opportunities to increase the effectiveness of management controls actions and controls are evaluated.
Taking all 3 values they look at impact x likelihood x control and assign a rating of either severe, high, medium, or low. Severe is listed at 100-125, high is 60-99.99, medium is 30-59.9, and low is 1-29.99. Each of these is assigned a risk owner, final rank, final score and then the range it falls into.

-Risk treatment plans are developed by the risk committee, whereas the risk option and the owner for the risk are identified. The risk owner is assigned the risk treatment plan.

Risk is assigned as a Parent/Child within ADO (mandatory checklist, tracking regarding the risk trends, due date), all managed by risk owner.

Reporting Status to management
Submission of the proposed risk, both annually and bi-annual assessment done as well as the option to add or review risk any time through the year outside of these to manage the risk appropriately. All risk is elevated to the management committee where it will then go to the ERM Program when necessary.

Monitoring of Ongoing risks
Tracked in ADO AZUREDevOps as work items, status updates going out regularly on plans and treatments, demonstrate competence on the risk management and the drivers of Risk.

Additional Evidence Reviewed:
-Risk Register (Currently no risk identified as severe)
-Efficient controls and timelines demonstrated by the organization for the overall risk management program, process, and procedures

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Performance Evaluation and ISMS Management Review (9, 10):

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed:

- All required elements were reviewed

The following topics were discussed with leadership in the audited period: Leadership Commitment - FY 25 Strategy Memo Contents

Security and Privacy Policies
- Information Security and Privacy Objectives (Management Intent) - Requirements and Guidance, example of security objectives

M365 Security User Stories (Security Requirements and Guidance) - PR -1 Perform Threat Modelling

Planning of Changes and Management Review

Transition to new version Mapping and Testing of Controls
- All controls were mapped, no new requirements to implement
- Everything already

Competence, Resource hiring

Security Incident Response Objective

Competence Evaluations - Connect frequency depends on the rhythm of business, but must happen at least annually
- Connects have areas of discussion with room for employee and manager comments

Internal Audit
- Board of Directors reviews requirements and direct internal audits and direct what should be reviewed - External audits are added in
- Ensures that duplication is avoided
- Control framework maps standards to each other, to ensure that clauses and controls are mapped to at least one of the activities

Remediation and Exception

Objectives
- Business Continuity Process Objectives 13.01
- next layer down determines the measurement

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Human Resources (7) & Supplier Management:

Planned activities have been fully realized. Methods for determining process results:
Evidence/Documentation Reviewed:
- MS 365 ISMS Management Review February 2025
- Background Clearance Checks (Hire Right)
- Background Data Retention 5 Years
- Microsoft Security Policy, Privacy Standard
- 2024 Security Foundations, E+D Privacy Fundamentals
- Business Conduct Policy
- Supplier Security Management Standard
- Subscription Termination

Planned activities have been fully realized. Methods for determining process results:
Background screening
- HRweb Background Screens rules/policy; Only lasts for 5 years (MS policy)
- Vendor Background screening attestations: Microsoft Cloud Background Screen Attestation Letter for Microsoft - Corporation examples - US, Canada, UK, Egypt; Vendor company: HireRight; FISMA Training: policy for required training and T&C of global employees on HRweb; Employee cloud screening tool

Teleworking policy- Azure VPN Manual which is required to do manually.
MSFTVPN Remote Access VPN- Microsoft Guide on HRweb SharePoint site (Zero Trust security model); Rogues Access policy; Tech best practices for VPN (TechWeb)
Standards of business conduct training (SBC 'Trust Code'): acknowledgement signed by employees selected during screening.

Disciplinary policy on HRweb Non-disclosure policy
Located on HRweb (part of the SSBC training): acknowledgement signed by employees selected during screening. E&D Privacy Foundations Course, FISMA
Security training and Privacy training (6.3) - eligibility requirement
Supplier Management - 11.01 Supplier Security Management Standard (5.19-5.22) - Supplier Security Privacy and Assurance (SSPA) program
Roles and responsibilities/management – ISMS Policy

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Change Management (6.3), EXO and Substrate Change Management::

Planned activities have been fully realized. Methods for determining process results:
Evidence/Documentation Reviewed:
- EXO & Substrate Change Management Overview
- Exchange Online (EXO) hosted version of Microsoft's Exchange Server messaging platform
- Substrate Compute, resources for services
- Change Management- Model A/B/B2/D/D2
- Change Management – Deployment Models, Model A/B/B2/D/D2 (Azure & Pilotfish)
- Change Management A/B/B2
- Deployment Config Sample, Build Id 1911049
- Build Id 1911049, Build Evidence, Roslyn test
- PR Code Review in ADO, J.Z. approved May 22nd, 2024
- Code Review Policies
- Model D Workflow, Build Id 19342551
- Build Id 19342551, Build Evidence, Roslyn test
- PR Code Review in ADO, N.D approved Jun 11, 2024
- D2 Deployment Config Sample Build ID 18955805
- Build Id 18955805, Build Evidence, Roslyn test
- PR Code Review in ADO, A.M. approved May 20, 2024
- Model /B/B2, Deployment Process Diagrams, Regular Train, Fast Train, Emergency Patch
- Regular Train 2-3 weeks, Fast Train 1 to 2 days, and Emergency Patch 8-24 hours for Model A.
- Model A, SDFV2 >24, MSIT > 4 days, SIP > 6 Days
- Model D Deployment, On Demand, Normal: 1 to 2 hours
- Model D2 Deployment, On Demand, Normal: 1 to 2 hours
- Regular Train Model A Halt, Incident # 507637858 5-27-2024
- Fast Train Approval Sample, Build #17447203
- Emergency Patch Model A Approval Sample, Build #3243373
- Model B/B2, Regular Train Rollback Approval 02/12/2024
- Safe Configuration Deployment Model B/B2 Approval 06/02/2024
- Model D Deployment, Lockbox Access Request 07/08/2024
- Model D2 Deployment, Lockbox Access Request 07/04/2024
EXO & Substrate Change Management Overview presentation
-Change management for EXO and Substrate is effectively managed and controlled through the

implementation of change deployment modeling. The change delivery approach is based on the severity of the associated incident and/or the urgency of the requested change. Evidence was presented showing the change management workflow process for multiple model-types, including management approval. Controls have been effectively implemented for secure coding.
-EXO - Exchange Online is the hosted version of MS Exchange Server messaging platform, part of M365 suite of products
-Substrate - internal facing platform built from Exchange (provides data storage for emails, offers CPU and Memory) Resources; source code repositories and management platforms; enable usage of Azure and Pilotfish; leverages Azure Managed Components)

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Access Control; Technological Controls – Access:

Planned activities have been fully realized. Methods for determining process results:
Evidence/Documentation Reviewed:
- Engineering Access
- Torus- Account & Identity Management
- LockBox/RBAC Approval Engine
- High Risk Individuals removed every 15 Minutes
- LockBox Access Control Management System
- Customer Lockbox
- Microsoft Security Program Policy
- Access Management Policy Jan 10, 2025

Access Management Presentation - Feb 2025
-Access to the MS 365 production environment is effectively managed and controlled, requiring multi levels of approvals based on eligibility, training, background, and need through an automated system. Changes to access, including termination, is effectively controlled ensuring access is limited or disabled, as needed, without undue delay. Access to the customer's environment is controlled by the org and the client. Physical access to information relevant to this process is controlled by ensuring that employees do not have access to the information (data centers), which are managed and controlled by the DC owners through badge access.
Torus (production environment) access
1. Torus - Account & Identity Management access request - must complete:
Employee profile & Org Hierarchy Background Clearances (HP SAP) Completed Trainings
EUPI attestation Lockbox approver team
2. Eligibility Granted post approvals
3. Toru account - ID Federation: AD and Sovereign Cloud instances
4. File Based RBAC Group Memberships
5. Lockbox/RBAC Approval Engine
OSP Portal request eligibility
-Portal Eligibilities and requirements associated
-Manager approval required (1st level approval): IDM Access Approval Requests portal; elevation approval - Eligibility Owner approval (2nd level): portal process

-Eligibilities portal: my eligibilities (pending, expired, approved)
Torus accounts auto-expire if not used after a certain duration; requires full approval process again to reenable, coding representing disabled account after 35 days of inactivity (Off_Adhoc_RWX)
Lockbox (access control management system; audit logs) approval engine: Elevation Request: Lockbox request sample
Changes to manager - new manager will have to reapprove within 5 days
Termination - IDM disables (Recurring IDSS Feed: periodic sync every 15 minutes) - Urgent termination process
Customer Lockbox - Lockbox plus customer approval for access to the customer's resources (tenant)
Physical control - no access to data centers (Azure controlled only access)
Use of privileged utility programs are controlled through the change management processes and access management processes (Torus, eligibility, lockbox, etc.).

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

O365 Asset Management O365 Asset Management - Central Admin Overview O365 Continuous Monitoring and Reporting (9.1):

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed:
- Vulnerability Scanning, Patches, Application Vulnerabilities, Limited InSecure Configurations
- Metadata Scanned not customer Data
- High Severity, Medium Severity
- 3rd party Audits ISO, SOC, Fedramp
- Agent Scan (offnode), Remote Network Scan, Container Image Scanning
- Daily Scans from > 2M Assets, Displayed w/in 12 Hours
- Vulnerability Remediation Process
- Remediate Vulnerabilities w/in SLA, High 30 days, Moderate 90 days
- Vulnerability Exceptions, False Positives, No Patch Available (30 days), Risk Adjustment
- TVR Exception Board each Request
- Email, TVR Exception Review Process 1/29/24
- Monthly Security Review, MSR PAVC Trending
- Logical Assets, Physical Assets
- Office 365 Exchange Total 360498, Vulnerability 220, 36 Unique
- Dashboard, KPI Trending, 30 Day Vulnerability Timeline

HW request workflow diagram
-Service Team Inventory - add to their HW inventory application

Asset Ownership - Physical GDCO property field (billing codes)
-Logical inside Azure subscription ID
-Logical outside of Azure tracked by service team
-Asset Handling & Acceptable Use - Confidential Information Policy MSPOLICY-804079558-11

-Information Labeling - Minimum Physical Security for HBI Assets Baseline policy

Exchange/Substrate Asset Management presentation
-Central Admin Inventory Tracking (Management platform)
-Screenshot of various state of machine: Activity and Provisioning states:
-Dashboard M365 Pulse: OSP - displaying the state of machines screenshot

Vulnerability Scanning and Reporting presentation
-Remediation measured against *KPIs: High severity - patch release + 30 days; Med severity - patch release + 90 days

Performance Evaluation: 3rd party auditing (ISO, SOC, FedRAMP)

Vulnerability Management Process 7 Responsibilities: Remediation process workflow diagram

Scan types: Agent Scanner and Remote scanning
-Architecture - Daily scans received from > 2M assets and processed and displayed within 12 hours: Process workflow
-Patch review board meets 1x per week to approve/deny and exception review portal screenshot

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

SIP - Substrate Intelligence Platform:

Planned activities have been fully realized. Methods for determining process results:
Evidence/Documentation Reviewed:
- Static Security Test: Roslyn Results 3 15464304 Dated 10/26/2024.
- PR Code Review and Approval
- SIP D-Z Deployment-
- SIP Retention (formally known as Sweeper Deletion) (SIP D-X Example)
Code and Repository Builds Models -SIP Model Z - deploying (SIP partners) eyes-off environment, partners can use to deploy ML Models
-SIP Model Y - training (SIP partners)
eyes-off environment, partners can use to process data and ML Datasets
-SIP-DataOps - producing (engineers)
-Compute - code is executed
-Orchestration - coordinate code execution Customer Data Storage - data is stored
Access control layers for SIP environments
1 Torus
2 Authorization
3 Configuration
-End-to-end production workflow - offline/online
Change Management -Model Z approach build release and configuration files; Supporting code build tests and results; Security Test (Bandit); Log files; Security Test results; Code review approvals; and approval;

code review policy (Polymer); Lockbox approval and email
-Model Y approach
Components packaged into builds (can be multiple builds deployed to the same environment) creates a pipeline (not deployed to customer-facing production 'offline'): known code repositories approval; AML Policies with eligibility validation; Torus Eligibility (BG check, Trainings, clearances) - Heron description (eligibility requirements) and approval team
Detonation chamber: offers minimum number of code reviewers and static security testing AML Pipeline screenshot.
Engineering Team responsibilities
Manages deployment, code repository, unit tests, security Tests and approving code reviews, deploys builds and executes pipelines
Access Management
Azure-based environments managed through subscriptions and managed by Torus, Customer data Segregation - tenant/user list script code
Retention Platform - data within SIP is deleted based on static retention windows "time-to-live Timer" (TTL Timer): Data movement logs reviewed; SIP Retention Data Deletion; Lineage Data Deletion Logs
ODIN-ML HDI Cluster URI Syntax (default); AML compute – Encryption in transit; Synapse - TLS enabled by default; ADF encryption in transit by default; ADLS encryption at rest
Data is auto-deleted based on the classification of the data by the Data Retention Platform based on the TTL timer. This process is monitored (deleted data) through alerting

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

M365 Copilot:

Planned activities have been fully realized. Methods for determining process results:
M365 Copilot is an AI-powered assistant integrated into Microsoft 365 to enhance productivity by providing intelligent suggestions and automating routine tasks.

M365 Copilot system flows were tested from Applications as well as UI Chat connections. These flows followed the M365 organization structures for the ISO standards covered in this audit. The Copilot flow allows user tokens to move between several different backend services to achieve the desired response to the customer inquiry. M365 Copilot can be accessed through an M365 product interface (Word, Excel, PowerPoint) using a backend system called Augloop or through a UI chat using a Bizchat Connection.

Evidence Reviewed:

-Bizchat Connection – UI chat connection service

-Augloop Workflow – M365 product connection service

-Enterprise Sydney – Copilot backend orchestrator

-3S/LU – Substrate storage and language understanding

-LLM API – Large Language Model API

Each Copilot system flow follows the same requirements as all M365 services. M365 Copilot achieved the planned results, and the processes are deemed effective.

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Operations Security - MS Teams:

Planned activities have been fully realized. Methods for determining process results:
Evidence/Documentation Reviewed:
- Operational Requirements, Prevention
- Geneva is being used for monitoring
- Reporting, Documentation, & Tracking Progress
- Azure DevOps, Remediation
- 1CS Questionnaire
- ADO Dashboard
- Exception Reporting
- Bi-weekly Report

-Operations Security for MS Teams is managed effectively through the various controls established by MS 365 services. Azure subscriptions are used to manage various environments. Effective controls have been implemented for anti-malware, software installation and development activities.
Documented Operating Procedures are stored on Wiki
-TeamSpace Wiki Processes
-Various processes reviewed with evidence of revision history
Capacity Management - CPU screenshot - monitoring
-In Memory capacity screenshot
-Disk Space screenshot
Production vs. non-production - Teams Graphite Fabric Screenshot Anti-malware Configuration screenshot
Encrypted at rest - data masking screenshot
DLP - encryption in motion HTTP (port 443) screenshot Info Backup - Azure: Geo-Redundant Storage screenshot Logging and monitoring: Geneva screenshot
ICM alerting mechanism screenshot - CPU usage too high ICM Query -output of incidents sample
Log information protection workflow (Vanquish analyses data and alerts) -Vanquish portal is read-only for employees
Time sync: NTP dependency on azure
All servers onboarded to TVR M365 program with Azure doing patching SW on OS - Azure DevOps Release Management (ADO RM) screenshot Restriction on SW Installation - approval process (ADO)
Audits planned for 2025 (audit calendar) tracker

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Windows 365:

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed:

- Intro to Windows 365
- Windows 365 Services, Windows 365 Service Boundary, Azure Virtual Services
- Weekly Service Health Review Meeting notes reviewed
- Windows 365 Microservice Architecture
- Change Management Process- Release Process
- Pull Request Sample: 10904683 started on dev branch on Jun 17
- Connecting INT Release (#1.0.2355.175) Continuous Deployment
- Source Control- Branch Policy for Release Branch
- Roslyn Analyzers Scan
- Release build #1.0.02724.271 - passed tests and component governance prior to branch release
- Only signed binaries are allowed to run
- Merger PR 10942056 - 436 test run - proceed with no failures
- SH Release- Lockbox Approval
- Prod Release- Signoff Process
- Lockbox Request and Approval
- Torus JIT Access Control- CMDCloudPCTeam
- Cosmos DB
- Tenant Data Separation
- Service Resiliency
- Tenant data is stored in Windows 365 Microservices
- Tenant Data Deletion
- AAD Tenant Data Deletion (SoftDelete)

Intro to Windows 365 presentation
-Personalized Windows 365 Cloud PCs across devices is managed effectively through the various controls established by MS 365 services.

-My Workspaces Mycloud_PC_001 screenshot
-Windows 365 Service dataflow

License enforcement; manage service & VM health; provision machines; send notifications.
-Microservice Architecture: Repository spreadsheet
-Management oversight: screenshot of monthly recurring service health recurring meeting' Leadership team members listing; SHR Agenda (overview, experiences, retrospective, end user experiences

Change management - release pipeline work flow
-Code change, Pull Request (PR): reviewed
-Testing/analysis: reviewed
-Deployment (Griffin): deployment to INT01 & INT02 (branches)
-Testing/analysis: reviewed
-Pre-production testing and approvals: Roslyn analyzers scan (Bandit)
-Sign off of feature team: Component Governance for build
-Self-host release branch: Branch release policies; Release build reviewed

Production and Eligibility Approvers
-Self-host release - Lockbox Approval to the pre-release environment; Torus JIT Elevation Eligibilities for access control for MDCloudPCTeam members and expiration policy

Data separation
-Data are stored per tenant in Cosmos Db, Cosmos Db policies screenshot

Encryption: Data in Motion
-HTTPS for incoming/outgoing traffic and internally: HTTPS on with TLS 1.2 JIT process settings screenshot

Data in Motion Internally at Microsoft
-CloudPC Graph Outbound calls are HTTPS: screenshot of Windows 365 connecting to Graph (back-end data service) - CloudPCEnvironemnt.cs
-Data in motion between MS and customer: JIT process screenshot

Encryption at rest
-Azure Cosmos DB / Microsoft Docs

Tenant Data Retention is stored in W65 Microservices, tenant offboarding notification from AD Tenant Data Deletion
-DirectoryChangesProcessHelper.cs - AAD notification that the tenant is set for deletion screenshot; tenant softdelete operation in runtime screenshot; tenant service notification to downstream services (OrganizationService.cs); AAD Tenant deletion 'out of scope' CloudCPEvent screenshot; countdown period TTL 30 days screenshot; fully offboarded query for tenant screenshot - null

Legal, Reg, Compliance obligations for data deletion: Set by commerce team/licensing (SharePoint presentation)
Manual reviews of data deletion: checks within the audit period to make sure the sync/code works (SOC audit)

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Change Management (6.3), EXO and Substrate Change Management:

Planned activities have been fully realized. Methods for determining process results:
Evidence/Documentation Reviewed:

- EXO & SubstrateChange Management Overview
- M365 Copilot
- SIP
- Exchange Online (EXO) hostd version of Microsoft's Exchange Server messaging platform
- Substrate Compute, resources for services
- Change Management- Model A/B/B2/D/D2
- Change Management – Deployment Models, Model A/B/B2/D/D2 (Azure & Pilotfish)
- Change Management A/B/B2
- Deployment Config Sample, Build Id 1911049
- Build Id 1911049, Build Evidence, Roslyn test
- PR Code Review in ADO, J.Z. approved May 22nd, 2024
- Code Review Policies

- Model D Workflow, Build Id 19342551
- Build Id 19342551, Build Evidence, Roslyn test
- PR Code Review in ADO, N.D approved Jun 11, 2024
- D2 Deployment Config Sample Build ID 18955805
- Build Id 18955805, Build Evidence, Roslyn test
- PR Code Review in ADO, A.M. approved May 20, 2024
- Model /B/B2, Deployment Process Diagrams, Regular Train, Fast Train, Emergency Patch
- Regular Train 2-3 weeks, Fast Train 1 to 2 days, and Emergency Patch 8-24 hours for Model A.
- Model A, SDFV2 >24, MSIT > 4 days, SIP > 6 Days
- Model D Deployment, On Demand, Normal: 1 to 2 hours
- Model D2 Deployment, On Demand, Normal: 1 to 2 hours
- Regular Train Model A Halt, Incident # 507637858 5-27-2024
- Fast Train Approval Sample, Build #17447203
- Emergency Patch Model A Approval Sample, Build #3243373
- Model B/B2, Regular Train Rollback Approval 02/12/2024
- Safe Configuration Deployment Model B/B2 Approval 06/02/2024
- Model D Deployment, Lockbox Access Request 07/08/2024
- Model D2 Deployment, Lockbox Access Request 07/04/2024

EXO & Substrate Change Management Overview presentation

-Change management for EXO and Substrate is effectively managed and controlled through the implementation of change deployment modeling. The change delivery approach is based on the severity of the associated incident and/or the urgency of the requested change. Evidence was presented showing the change management workflow process for multiple model-types, including management approval. Controls have been effectively implemented for secure coding.

-EXO - Exchange Online is the hosted version of MS Exchange Server messaging platform, part of M365 suite of products

-Substrate - internal facing platform built from Exchange (provides data storage for emails, offers CPU and Memory) Resources; source code repositories and management platforms; enable usage of Azure and Pilotfish; leverages Azure Managed Components)

M365 Copilot -Change management for M365 Copilot is effectively managed with 3S following the EXO B deployment model and the remaining flows follow the EXO D2 deployment model.

SIP -Change management for SIP is effectively managed as it follows the EXO D2 deployment model.

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

O365 Cryptography - Protocols and Ciphers:

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed:
- Centralized Crypto Policy
- TLS Configuration Standard
- Documents protocols and ciphers that comply with commitments
- Workload compliance is measured by S360 KPI-

- All computers must comply with PCT, SSL, TLS 1.0/1.1 Must be disabled and TLS 1.2 must be enabled and TLS 1.3 should be enabled. Service must disable insecure renegotiation.
- All weak and medium ciphers must be disabled, all cipher suites that use the PC4/DES/3DES encryption must be disable. TLS Certs must use the SHA2
- Reviewed the Cipher Suite
- Insecure Renegotiation
- Key Management- Cert authority key lifetime and requirements.
- Root CA Cert, Subordinate Cert,
- Validated Certificate viewer within outlook

Policy
-Does not allow less than TLS1.2: Powershell 1/28/23 screenshot TLS 1.0/1.1 disabled and 1.2 enabled Only Secure Renegotiation is allowed - M365 security policy; TLS certs must have SHA2 algorithms -Key management policy
-HTTP Strict Transport Security - HSTS required for all web application - M365 policy
-Exception Management Process for M365 TLS Enforcement KPI process; Exception 285937 SMTP Auth TLS 1.0/1.1 - closed

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

M365 SRT (Security Response Team) - Incident Response::

Planned activities have been fully realized. Methods for determining process results:
Evidence/Documentation Reviewed:
- Security Response Team (SRT/IR)
- Security Response Process
- M365 Federated Security Response Model
- SIR SOP v.1.9.14 2/27/24
- Email, Security Response SOP Review 07/2024
- Onboarding New ServicesO365 Security Escalation (Incident & Breach Response)
- Security Escalation in ICM
- ICM Ticket #
- Readiness Checklist
- Incident Response Team Construct
- Security Investigation Flow
- Post Incident/Post Mortem
- M365 Risk Management Semi-Annual Review November 2024

M365/O365 Federated Security Response Model:
Detection & Analysis > Containment Eradication Remediation > Post-Incident Activity
SR Process based on NIST 800-61
-M365 Security Services Security Response SOP (Published Annually) screenshot
-Revision Tracked screenshot: SOP Review: Process and signoff screenshot; review process sop screenshot
-Feedback Review Period email screenshot
-Final published email screenshot

Onboarding New services:
-SOP - Team Process Screenshot
-Services Guide screenshot New Employee Onboarding:
-SOP Process screenshot
-Checklist screenshot
-Signoff record and mentor (buddy) signoff - ready to join 'on-call' rotation screenshots
Incident Response Team Construct
-Roles and responsibilities and team structure
Security Guidance (Org/Workloads) O365 Security Escalation (Incident & Breach Response) -Instructions - screenshot / Battlecard Site
ICM
-Incident Management tool for MS screenshot of on-call schedule; alert/escalation creation to SIR screenshot
Severity Guidance and SLA screenshot; Sev1 documented in battlecard and SOP
M365 Security Response Process
-Section 7 - Triage > Investigate > Classify > Continuous Improvement Classification - iterative process to analyze, assess impact and scope
Reporting Security Issues:
-Security Analysis and response SOP Section 4.2 - identify and categorize; Section 5 - Roles / Responsibilities
-Section 6 - Security Escalation (Checkpoints for management and communication)

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Remediation & Exception (10.2)::

Planned activities have been fully realized. Methods for determining process results:
Evidence/Documentation Reviewed:
- Operational Requirements, Prevention
- Reporting, Documentation, & Tracking Progress
- Azure DevOps, Remediation
- Remediation Sample Finding
- 1CS Questionnaire
- ADO Dashboard
- 2024 Exception 914087
- Exception Reporting
- Bi-weekly Report

The O365 process for resolution of Nonconformity and Improvement is referred to as Remediation and Exception.
Remediation is the process to provide a remedy to address a finding from an audit
The role of the team is to track, monitor and resolve findings for ISO 27001 (and other compliance standards such as FedRamp and SOC2)
Groupings of findings are Operational Requirements and Prevention
New Findings

Tracked in ADO (Azure Dev Ops)
- Findings are triaged
- Findings are assigned to Service Team and agree on deliverables Active

Remediation Team tracks status and updates ADO
- Service Team provides Evidence
- Remediation Team reviews Evidence Approved
- Remediation Team sends to FedRamp Team for Review and Approval Closed
- Ticket is updated and closed
- Operational Requirements

Remediation Dashboard
- New and Approved Findings
- Changes made by non-Remediation Team
- Recently Closed by Date
- SOC Service Tree Review - Remaining Bugs
- Approved FedRamp ORs by Environment

Delay to resolve findings are the following:
High - 30 days Moderate - 60 days Low - 180 days
Exceptions (findings that take longer than the defined resolution period) are raised as Risks or approved in Management Meetings, example, BCM lasted 3 months for a team to onboard to the program Audit team manages the findings, if audit team states that something needs to be added as a risk
- Management is aware of status of risks Findings are tracked in OneTrust
Remediation Reporting Power BI from data from ADO - verified
Exception Presentation
- Extension of time for teams to get work accomplished, short-term time allotment or extension for teams to resolve noncompliance, KPI or security issues
- Team roles, Collects, gains approval and monitors commitments for E&D teams, while ensuring appropriate awareness for leadership and audit teams
Categories - KPIs, GDPR and Security Issues
New
- Exception categories include S360 Requests, Privacy, BCDR, Security, GDPR, Trust, BCM, Other Service team submits ICS Exception Request
Exception Team reviews the ADO request Active Flow
- Approver evaluates sufficient data
- Approver & Service Team discuss details Approved
- ADO updated with Approval information Exception criteria satisfied
Exception Dashboard
- New Exception Requests by State
- Follow up by Exception Team
Exception Reporting, Power BI dashboard, reviewed
Exception Reporting, Active New Exceptions by Month, reviewed
Grant an exception is required for those that cannot be fixed, Security reviews and approves,

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Compliance:

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed:
- CELA, Field, CXP
- Third Party Content, Third Party Software Governance
- Data Handling Standard
- Independent Review of Information Security
- Pen Testing, Third Party Vulnerability Assessment of M365 + Viva
- M365 Monthly Service Reviewed

Mapping of controls
Compliance with legal and contractual requirements is assured through the MS CELA department

CELA, Field, CXP identify new requirements
The Requirements are triaged by Customer Need, Effort to Implement
New Requirements and New Documents are analyzed
New Requirements are Onboarded and Evaluated
Implementations are Monitored

Intellectual Property is assured in the Data Handling Standard (A.5.10. A.5.12. A.5.33)

A.5.3.4 Privacy and Protection of PII
- Independent Review of Information Security

Compliance with Security Policies and Standards, GRC Reviews
- 2024 Annual M365 Risk Assessment

Management of Technical Vulnerabilities, Qualys, PAVC tool
Penetration Testing
3rd party Penetration
Bug Bounty Program

Supplier Relationships
Suppliers complete a self-attestation to the DPR before work can start
- Yearly process, renewal cycle the supplier has 90 days to complete the review - Requirements are outlined in the DPR, that must be fulfilled

Data Protection Requirements DPR
Master Supplier Services Agreement MSSA
Statement of Work (SOW)

SSPA Enforcement - Reporting
- Reviewed Enforcement Dashboard

SSPA Enforcement Purchasing Tool
- Red they are blocked from the Purchasing
- Usually they turn red because they didn't miss the renewal process - Existing contracts are still honored, but couldn't open up new one

All requirements for the Compliance have been fully and effectively implemented.

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

M365 Viva Engage (Formerly Yammer):

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed
- Security, Privacy & Compliance Overview
- Engage Services Branch Policies screen shot
- Remove unnecessary logs 01/31/2025
- Deleting LDAP Accounts 02/20/2024
- Viva Engage overview presentation
- Viva Engage Security Policies and Procedures: SOPs stored in Azure: Screenshot of Viva Engage security policies and SOPs - master files contents; source code and revisions history of Viva Engage access control policy

Access Control
- Viva Engage-specific access control for Engineering team/production resources (Yubikey) Secure Access Workstation required (SAW); Viva Engage VPN - no access to MS networks; Viva Engage LDAP group account required (70 day password reset)
- Privilege Management: LDAP account creation lifecycle diagram; production access requires additional background checks/security approvals
- Removal/adjustment of Access Rights - process maintained by HR team (automated sign-out - official notification)
- Use of Secret Auth Information: screenshot of PW change in Homie 3 for LDAP through JIT tool
- Info access restriction - screenshot of access request through Homie 3;
- Request to production resources access lifecycle diagram through Homie 3: Access request logs screenshot

Change Management
- Access control to program source code - no 3rd parties; 3 levels of access Read/contribute, Admin/mgmt or read-only to Viva Engage org only

- Viva Engage Azure DevOps access and permissions process
- Viva Engage Base Imagine & Viva Engage Service Image containers diagram

- Process overview for changes and SW releases within Viva Engage environment:

Pull request and approvals: PR 39463 portal with description and approvals, branch policies, test results, deployment status, Dev actions, and change status checks. Build and release definition are based on Templates, scheduled automation (every 2 hours) overrides potential manual modifications through Azure DevOps UI: Viva Engage Azure Mappings file (template system) source code and pipelines screenshot.

- Master branch policies: Viva Engage Service branch policies screenshots with reviewers and approvals Release will build service docker image

Code to production overview
- Build > Release > Deploy workflow diagram (from review/approval, docker imagine process to creation of new service container)

Restrictions on SW installation
- Docker base images and service base imagines

Separation
- Viva Engage uses separate pre-production (staging and dev environments with dedicated virtual servers. No connectively to any staging or production env.
- Sample: Services-fileville-release-1630 - Pipelines screenshot; Release env for service (production/PRO services) pipeline screenshot

Vulnerability scanning
- Vulnerability feed is updated daily using 1ES Component Governance and Anchor-Engine open source tools:
All OS packages from Docker base are being upgraded on every release.
All updates on Services Dockerfiles on top of base images are being updated on every release
- Vulnerabilities are tracked/managed using M3654 Security Bugs policy (SLA, exception, responsibilities, etc.)
- Security Supply Chain Analysis (auto-injected by policy) screenshot for Docker Images
- Component Governance policy and (detection) pipeline screenshots
- Open-Source Security - Status and Active security log screenshots
- Tech Vulnerability management: New and archived Audit Reports - SOC Reports screenshot (SOC 2 bridge letter January 2025)

Operations/Network
Capacity Management
- Monthly capacity planning meeting: MSR PowerPoint presentations for monthly review repository for 2024; All Incidents slide for Feb 2025 presentation

Controls against malware
- Service deployed in containers in read-only mode with write-allowed folders (logs. tmp, etc.) monitored; Open source tool Sysdig Falco - monitors sus behavior from SW and users; User training in malware detection and removal
- Intrusion detection - rules currently enabled
- Intrusion detection system - yammsec Falco coverage per region (PROD only) screenshot (95 - 100% coverage)
- Security Events dashboard - Lens Explorer Viva Engage MesosLand - Falco events

Backups
- Backup process:
Azure snapshot of a virtual hard disk
backups and verification jobs scheduled thru Azure DevOps
Logs in Pipelines - Pipelines (azure.com)
Monitoring metrics with point in time status to monitor time elapsed between backups

Event Logging
- Viva Engage Kusto
- OS and Security Logs retention = 365 days
- Service Logs retention = 30 days
- Service metrics (for capacity purposes are sent to Wavefront Viva Engage account
- Viva Engage Kusto dashboard (IDWeb)
- Admin & Operators Logs - monitor and all activity and admin actions with Falco ev: Falco log for 02/2024 (365 days)

Use of privileged Utility Program
- Falco log for February 2025 with login activity

Data-at-rest encryption
- MS Azure default encryption for disks screenshot Encryption in transit:
- General settings for O365: Default Route Data - redirect to HTPS

User devices
- SAW - Secure Access Workstation for Infrastructure team
- MS provided devices with MS Intune - Eng and Services Team

Customer data deletion
- Subscription retention policy; agreed in customer contract/SLAs; Viva Engage Deleter - data deletion service Business Continuity
- Follows M365 BCDR program requirements
- Annual exercise (take containers down and see how system reacts with full system restoration) - last exercise April 2024; next scheduled for April 2025

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

27017::

Planned activities have been fully realized. Methods for determining process results:

This Audit covered the cloud aspects considered the Microsoft 365 product. The presentation was focused on the compliance with the system needs and the controls.

Evidenced the cloud service customer's information security policy that is part of the ISMS policy. This

policy describes the information can be stored and maintained in the cloud computing environment, and the business processes can be operated in the cloud computing environment. The information security policy for providing cloud services deals with the cloud service customers' information and business processes.

Evidenced that Microsoft is providing information on procedures for the management of the secret authentication information of the cloud service customer, including the procedures for allocating such information and for user authentication.

Microsoft is ensuring that arrangements are being made for the secure disposal or reuse of resources, in a timely manner.

Evidenced the appropriate logical segregation of cloud service customer data, virtualized applications, operating systems, storage, and network for the separation of resources used by cloud service customers in multi-tenant environments and the separation of Microsoft's internal administration from resources used by cloud service
customers.

Microsoft provides the specifications of its backup capabilities to the cloud service customer. The specifications include scope and schedule of backups, methods and data formats, retention periods for backup data, procedures for verifying integrity of backup data, timescales involved in restoring data from backup, backup capabilities. Microsoft also provide secure and segregated access to backups, such as virtual snapshots.

Evidenced that Microsoft make available to the cloud service customers information about the management of
technical vulnerabilities that can affect the cloud services being provided.

The risks associated with running cloud service customer-supplied software within the cloud services offered by the cloud service provider are defined.

When configuring virtual machines, Microsoft and the cloud service customers ensure that appropriate aspects
are hardened and that the appropriate technical measures are in place for each virtual machine used.

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

M365 BCM - 22301 / Business Continuity and Redundancy Controls::

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed:
- EBCM M365 Business Continuity Management - February 2025
- Enterprise Sponsorship at Microsoft
- EBCM and Enterprise Risk Organization, M365 BCM

- EBCM provides oversight to the enterprise BC practices across enterprise includes charter, policy, standards, methodology, tools set naming conventions and templates.

Each engineering unit is responsible for deploying Business Continuity
- The Engineering Units are responsible for the deliverables
- EBCM Framework FY 25 (includes BC/DR Methodology Overview validated each component within 12 months of last validation, Assessment (BIA/Dependency Mapping and Planning), must be reviewed and exercised every 12 months.
- BC Methodology Overview - verified
- If there are any impacts to the entire organization (enterprise), a risk is raised with the organization
- If there is an impact to the Service Level, gaps go into the Service Level repository
- M365 BCM Workflow (BCM Onboarding Site - Business Continuity Onboarding Request, Service Tree, BCDR Manager, EGRC Report)
- Reporting to Management 0 Workflow (Monthly Service Reviews and Meeting and Quarterly Service Review) Dec 2024
- EBCM Quarterly Score Card FY 25 Q1, EBCM Quarterly Report Review - Reports are the BC Objectives
- BCDR Manager Repository Pages (BIA, Dependencies, Recovery Plan and Test) (Compliance Tracked)

Example, Dec 11 2024 New Services Onboarded
SharePoint M365 Business Continuity Onboarding Request, validation is performed depending on services.
Reviewed Enterprise Repository

Example of completed SharePoint form, Change Communication Hub- Data Ingestion
M365 Continuity Onboarding Request Spreadsheets (529)

Example, Data Ingestion
Includes, Deliverables BIA, Dependencies, Recovery Plan and Recovery Test
Business Impact Analysis 2/01/24 (Impact of Service to Microsoft) RTO assessed

Customer Facing Services Recovery Objective is 5 hours (defined on customer SLAs)
- Enterprise mandate is 4 hours for Recovery Objective
- Workforce Recovery identifies the number of individuals trained, and the number of individuals required 14
- External Suppliers (none needed in this)
- Recovery Rating, Informational for Recovery Configuration to determine Resiliency (highest level)
Test Scenario failed over from one region to another.

- Disaster Recovery Plan, Tested on 2/1/24, Recovery 5 minutes
- Disaster Recovery Plan - Details of plan are restricted, however templates were reviewed
- SSP-A06 FedRAMP ISC- Information System Contingency Plan (ISCP) Template Microsoft Office Online

After action reports are being captured and gaps, remediations, and bug ID are linked. Reviewed after action that shows where the bugs are linked and vulnerabilities.
Reviewed and Approved by Technical Fellow
- Includes specific information related to their system
- No enterprise risks raised in the previous year

Service Level BCDR Champ, not reported to Enterprise BCDR Program Objectives

- M365 BCM Update Dec 22 (Program Renewal Onboarding is at 100%)
- BCM Compliance shows 3 RA (Risk accepted) 13 non-compliant. Compliance is tracked on EBCM Quarterly report Review which goes out to Leadership and monthly.

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

ISO 27018:2019; PII A.5.31; ISO 27701: 2019::

Planned activities have been fully realized. Methods for determining process results:

Evidence/Documentation Reviewed:
- Customer Agreement/Marketing advertising use-
- Law Enforcement Requests Report- July- December
- Screen shot- Communications- Customer Data Breach
- Microsoft Corporate Retention Schedule-
- O365 Data Handling Standard-
- Confidential Information Policy- Policy #- MSPOLICY- 804079558-11
- SSPA: Supplier & Privacy Assurance Program
- Confidential Information Policy
- Service Trust Portal

ISO 27018 2019 Privacy Controls Presentation – February 2025

ISO 27018 main standard to present controls, followed by the delta of the remaining ISO 27701 controls. The ISO 27018 controls are identified, with the corresponding ISO 27701 control mapped in brackets.

A.2.1. Consent and Choice (maps to ISO 27701 B.8.2.1)
Cloud Service Customers can access, correct, and erase customer data on the Admin Portal and IW Portal Settings
Customers can use the Azure Portal to fulfill their end user's GDPR DSR requests.
Tenant can make a request to delete and export user data.
MS Data Protection Addendum specifies the Processor's Purpose and Processor's Commercial Use
- Nature of Processing in DPA describes the ways that MS uses data (not used for marketing and developing new products for example)

A.3.2 Purpose legitimacy and specification (B.8.2.1)
A.3.1 Public Cloud PII Processor's Purpose and Commercial Use
DPA (Data Protection Addendum) is included in the MS Product Terms, stipulates that data is only used for what was committed to for PII Purpose and legitimate business purposes.
Examples of legitimate purposes are Delivering functional capabilities, Troubleshooting, Keeping Products up to date.

Office 365 Data Handling Standard, identifies the data classification taxonomy and whether data is permitted to be used for advertising or similar commercial purpose, for example, categories include, Access

Control Data, Customer Content, End User Identifiable, Support Data, Feedback Data, Account Data.

A.5 Data Minimization (B.8.4.2)
A.5.1 Secure erasure of temporary files, temp files created by OS, OS does cleanup
For temp files created by services, cleanup is by garbage collection process (If the session ends normally, temporary files are cleaned up when the session ends, if the session ends abnormally, the temp files get cleaned up in the garbage collection process)

A.6 Use and Retention of disclosure limitation, B.8.2.1 (Customer Agreement) B.8.4.2 (Return, Transfer and Disposal)
M365 MS Products and Services DPA

A.6.1 PII disclosure notification (B.8.5.1, B.8.5.4)
The contract between the cloud PII processor and CSC requires the cloud processor to notify the CSC according to the procedure and time periods per the terms of the contract, and any legally binding requests by law enforcement authorities.
MS will not disclose or provide access to any Processed Data except if the Customer requests, per the DPA, and if required by law.
Customers have 90 days to change their mind or extract data.

The DPA states that MS will only disclose access as required by law, provided that laws and practices respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society.

A.6 Use Retention and Disclosure Limitation, Record of PII Disclosure (B.8.5.1, B.8.5.3, B.8.5.4)
MS publishes Law Enforcement Requests Report, twice a year on their publicly facing web site, Example February 2025.

A.8 Openness, Transparency and Notice (B.8.5.1)
MS gives 6 months advance notice on Microsoft Trust Center, of subcontractors who have access to customer data and personal data, and customers can also receive alerts if they set them up.

A.10.1 Accountability
A.10.1 Notification of a data breach involving PII (B.8.2.1)
MS notifies of Security Incidents on and data breaches involving PII.
Data Breach Notification is documented in M365 Security and Privacy Incident Respond SOP
Under GDPR Microsoft is committed to notify customers and/or appropriate parties within 72 h once a data breach has been declared.

A.10.2 Retention period (B.8.4.2)
PII return, transfer and disposal.
- Information retained for 90 days.
- DPA describes how information is transferred.
- If data transferred out of EU, process is documented in the Data Protection Addendum (EU data stays in the EU)
- O365 Data Handling Standard, describes how long information is maintained, so that clients can extract or deleted data (90 days)

A.10.3 PII Return, Transfer and Disposal (B.8.4.2)
The public cloud PII processor should have a policy in respect to return, transfer and/or disposal of PII and should make this policy available to the CSC. The required policy is covered by the MS DPA

A.11.1 Confidentiality and NDA, all employees must sign, and policy is in the Standard Business Conduct Training and part of M365 Privacy Training
MS Policy Confidential Information Policy 804079558-11

A.11.2 Restriction of the creation of hardcopy material
- DPA, Asset Handling (printers or portable media are prohibited)
- Customer Data and Professional Services Data access is restricted and controlled - M365 prohibits connected printers or portable media in the DC.

A.11 Control and logging of data restoration
- Customer data is continuously replicated to multiple copies in geographically dispersed DC to provide restoration capability.
- Customers can restore data within the recoverable period and is logged in the user activity log.
- Outside of the recoverable period, customers require an assistant to restore the data and the activity will be logged in the support ticket.

A.11.4 Protecting data on storage media leaving the premises
- The MS Security Program Policy (MSPP) describes the policies for asset transfer.
- MS prohibits asset transportation, including data bearing devices.
- M365 Service encrypt Customer Data at rest, using FIPS-140-2 cryptographic method.

A.11.5 Use of unencrypted portable storage media and devices - M365 prohibits the use of portable storage media or devices
- Customer Data is not allowed to leave the compliance boundary.
- Access to Customer Data is restricted and no one has standing access.

A.11.6 Encryption of PII transmitted over public data transmission networks (B.8.4.3)
- M365S encrypts or enables customers to encrypt Customer Data transmitted over public networks to prevent unauthorized disclosure during transit.
- FIPS 140-2 validated cyphers that have integrity validation for customer connections, interconnected system connections and remote access.
- To connect to customers, M365 is configured to negotiate FIPS validated TLS protocols - Remote access connections from M365 service team use FIPS validated TLS protocols.

A.11.7 Secure disposal of hardcopy materials (B.8.4.2)
- Hardcopies are destroyed using cross-shredding, incinerating, pulping - Bins are on every floor (Iron Mountain)

A.11.8 Unique use of user IDs
- Dependency on Azure AD(AAD) to enforce unique identifiers.
- AD uses AAD deployments for identifying and authenticating users into the environment - Authentication is through FIPS 140-2 validated smart cards, or TPM modules.

A.11.9 Records of authorized users

- Secure and authorized access to information systems
- Just in Time Tools are used for granular conditions for privilege escalations - No standard access granted.
- No direct access to production, elevated access is for a finite period.

A.11 User ID Management
- AD enforces unique identifiers and doesn't reassign deactivated or expired IDs.
- IDM synchs with HR system and MS learning to ensure background screening and training are in synch with ID Management

A.11.11 Contract measures
- Committed to protect Customer Data, DPA contains MS commitments.
- Signed by customer (Appendix A Security Measures)

A.11.12 - Sub-contracted PII Processing (B.8.5.7)
- SSPA (Supplier Security and Privacy Assurance) program sets privacy and security requirements is built into GDPR requirements.
- Additional online Customer Data Addendum
- Customer notified 6 months prior for customer data and 90 days for personal data.
- E+D has a governance program to ensure engineering teams understand the requirements that sub processors have to meet prior to working with suppliers.
- CELA (Legal team) analyzes new legislations for delta for requirements not meeting GDPR (China, Brazil)

A.11.13 Access to data on pre-used data storage
- Access is segregated between M365 user sessions through AD (on-prem & hybrid) and AAD (Azure Active Directory)
- Shared resources require each user to have a unique AD identifier that AD enforces.
- Customer Data is encrypted, using FIPS 140-2 validated protocols.
- Eired Customer Data gets deleted after the retention period (90 days) in the data storage

A.12 Privacy Compliance
- Geographical location of PII
- PII specifies and document the countries where PII could possibly be stored - Information is provided to the customers in Learn.

A.12.2 Intended destination of PII (B.8.4.3)
- M365 relies on internet protocols and encryption (TLS over TCP) to ensure data reaches its intended destination.
- Encryption is used to prevent unauthorized disclosure of information and detect changes to information during transmission.
- FIPS 140-2 compliant ciphers that include integrity validation for customer connections, interconnected system connections, and remote access connections to M 365
- Connections to customers, M365 is configured to negotiate FIPS compliant TLS protocols, with supported client browsers, through non-FIPS compliant protocols supported for legacy browser support - Communication between DC is encrypted.

ISO 27701:2019 Privacy Information Management (PII Processor) Delta of controls not covered by ISO 27018
Presentation February 2025

Processor control is in Annex B of the standard.

B.8.2.1 Customer agreement (Privacy Principals, majority are covered by ISO 27018)
Data Protection Impact Assessment is the only control not covered by 27018 - Developed based on EU Article 29 Working Party

B.2.2 Organization's Purposes (covered by ISO 27018 A.3.1 & A.3.2) - exact same PII is only processed

B.8.2.3 Marketing and Advertising - Completely covered by ISO 27018, A.3.2

B.8.2.4 Infringing Instruction (ISO 27018 A.6.2)
- MS does not provide legal opinion or advice to its customers.
- MS re-directs 3rd party requests (including law enforcement requests) back to the customer, unless prohibited by law.
- MS re-directs enterprise and user requests to their tenant admin (including GDPR Data Subject Requests)
- MS provides the tenant admin controls and helps customers to understand these controls (includes feature on/off, opt in/out configuration and policy settings so that customers can make informed decisions on Customers rights to control their data
- MS does not provide legal opinions to our customers; MS puts customers in charge of how to control data (MS is just the processor)

B.8.2.5 - Customer Obligations (New control)
- MS provides customer with information so that they can demonstrate compliance with their obligations.
- Trust Center has Security, Privacy and Compliance related information.
- Service Trust Portal has M365 Audit Reports and Risk Assessment Guide, White Papers
Compliance Manager- Risk Assessments and compliance activities by international and regional compliance requirements
- Security and Compliance Center solutions - Data governance, data protection
- Public facing documentation - industry specific guidance
- Service Trust Portal (revamped, much more detail and easier to find information)
- Audit reports, White Papers - reviewed.
- Trust Portal (available to public, but sensitive documents require customer to sign in, MS tracks what is downloaded by customers)

B.8.2.6 Records related to processing PII - fully covered by 27018 A.11.9
- DPA, contract with customer, disclosure related to processed data (customer directed, as described in the DPA, as required by law)
- Data access requests are recorded in 1 CS.
- Just in Time Access elevation (Torus)

B.8.3.1 Obligations to PII Principals (New Control)
- Customer accepts product terms.
- Tenant Admin acts on behalf of customer, signs contracts
- Service Trust Portal, supports client to understand risk, provides audit reports, notifications for document updates.
- Microsoft Priva, Privacy management allows MS to honor commitment to their clients.
- Priva would allow MS customer's customer to search logs to honor DSR (example)

- Admin controls to allow tenant admin to turn on and off features and policy of settings (licenses, apps, features)
- Message center can receive alerts to fulfill their commitments, example, notification of a breach and take action.

B.8.4.1 Temporary Files (A.5.1)
-MS arranges the Secure erasure of temporary files
B.8.4.2. Covered by Covered by 3 27018 controls, A.6.1, A.10.3, A.11.7
B.8.4.3 Covered by A.11.6 and A.12.2 from ISO 27018
B.8.5.1 Covered by A.6.1, A.6.2, A.8.1
B.8.5.2 Covered by A.10.3
- EU commitment for EU customers and their data will remain in EU in transit and rest.
B.8.5.3 Covered by A.6.2 and A.8.1
B.8.5.4 Covered by A.6.2 and A.8.1
B.8.5.5. Covered by A.8.1
B.8.5.6 Covered by A.8.1
B.8.5.7 Covered by A.12
B.8.5.8 Covered by A.8.1

MS Products and Services Data Protection Addendum
Data Handling Standard (Spreadsheet)

Law Enforcement Report - Published on web site, Corporate Social Responsibility

Document Detail Page (Service Trust Portal), Subcontractors List that have access to client data.

Security Incident Response

Corporate Retention Schedule, CELA compliance site, accessible internally

MS Information Security Policies

SSPA Website (Supplier Security and Policies) - verified.

Data Tenant Isolation - Public facing documentation in M365 (Logical Separation)

Data Residency in Trust Center on Web Site
Data Residency Public Facing Documentation

Link - 3D tour of DC link.

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

Physical and Environmental Security (People Controls A.7)::

By successfully implementing and adhering to these controls, Microsoft has demonstrated their commitment to human resource security and information protection. The organization recognizes the importance of maintaining a robust security culture that involves every employee and contractor, thus minimizing the risk of security breaches and safeguarding sensitive information. These controls have been deemed effective.

Evidence/Documentation Reviewed:
- Company Standards are in the internal internet
- DOM-10 Physical and Environmental Security
- All Badge access is controlled by GSAM
- Verified system settings showing 10 minutes for battery powered and 20 mins for plugged in
- Microsoft Intune
- Global Security Design Requirement

Control Specific Processes:
A.7.1 Microsoft has identified and designated secure areas within their facilities where access is strictly controlled. Access controls include physical barriers, such as locks and access cards, as well as surveillance systems to monitor and record entry and exit.
A.7.8 Equipment security: All equipment, including servers, workstations, and mobile devices, are appropriately secured to prevent unauthorized access or theft. Physical security measures, such as cable locks, secure cabinets, and alarm systems, are implemented to safeguard these assets.
A.7.14 Secure disposal or reuse of equipment: Microsoft has established procedures for the secure disposal or reuse of equipment to prevent unauthorized access to sensitive information. Prior to disposal or reuse, all data and software are thoroughly removed or securely wiped from the devices using approved methods. Iron Mountain is utilized on site.
A.7.7. Clear desk and clear screen policy: Employees are required to adhere to a clear desk and clear screen policy, ensuring that sensitive information is not left unattended or visible on desks, screens, or other work areas. This control minimizes the risk of unauthorized access or information leakage.
A.7.2-7.4 - Physical access control: Microsoft has implemented strict access controls to manage physical access to their premises. This includes entry points equipped with access cards, visitor management processes, and the presence of security personnel to monitor and control access.
A.7.13 - Equipment maintenance: Regular maintenance and inspection of equipment are carried out to identify any potential physical vulnerabilities or risks. This helps to ensure that equipment remains in good working condition and any issues are promptly addressed. This is managed at an Enterprise level as well.
Microsoft has established a strong foundation for physical and environmental security in their organization. Microsoft recognize the importance of protecting their physical assets, facilities, and information systems from unauthorized access, theft, and damage. Their commitment to these controls ensures the confidentiality, integrity, and availability of our critical resources, contributing to the overall security posture of the organization.

Summary: Planned results have been achieved; processes are deemed effective. Controls are appropriately managed and effectively implemented, as identified in the related ISMS documentation, the SOA, and the evidence reviewed.

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 organization's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organizations 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 defined in the plan provided in terms of locations and areas of the system and organization to be assessed.

The criterion of the assessment is ISO 27001, 27701, 27017, 27018, and 22301 and Microsoft's 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
			ISMS Changes + ISMS Scope Review	
			Context of the organization	
			Information Security Policy	
			Information Security Objectives	
			Competence, Awareness, Communication	
			Information security risk assessment, information security risk treatment, and Statement of Applicability (SOA)	
			Documented information	
			Management Review	
			Internal Audit	
			Nonconformity and Corrective Action	
			A.5 Information security policies	
			A.6 Organization of information security	
			A.7 Human resource security	
			A.8 Asset management	
			A.9 Access control	
			A.10 Cryptography	
			A.11 Physical and environmental security	
			A.12 Operations security	
			A.13 Communications security	
			A.14 System acquisition, development, and maintenance	
			A.15 Supplier relationships	
			A.16 Information security incident management	
			A.17 Information security aspects of business continuity management	
			A.18 Compliance	

Next Hybrid Audit Visit Plan

Appendix: Your certification structure & ongoing assessment program

Scope of Certification

IS 552878 (ISO/IEC 27001:2022)

The management of Microsoft 365 Service's Information Security Management System (ISMS), development, operations, and protection of personally identifiable information (PII), in accordance with the Statement of Applicability dated February 14, 2024.

PII 663484 (ISO/IEC 27018:2019)

The management of Microsoft 365 Service's Information Security Management System (ISMS), development, operations, support, and protection of personally identifiable information (PII) in accordance with the Statement of Applicability dated February 14, 2024. (ref. ISO 27001:2022 certificate number IS 552878).

CLOUD 663485 (ISO/IEC 27017:2015)

The management of Microsoft 365 Service's Information Security Management System (ISMS), development, operations, and protection of personally identifiable information (PII), in accordance with the Statement of Applicability dated February 14, 2024. (ref. ISO 27001:2022 certificate number IS 552878).

BCMS 706252 (ISO 22301:2019)

The business continuity management system in relation to the availability of Microsoft 365 services.

PM 741035 (ISO/IEC 27701:2019)

The management of Microsoft 365 Service's Information Security Management System (ISMS), development, operations, support, and protection of personally identifiable information (PII) as a processor in accordance with the Statement of Applicability dated February 14, 2024. (ref. ISO 27001:2022 certificate number IS 552878).

Assessed location(s)

The audit has been performed at Central Office.

Redmond / PM 741035 (ISO/IEC 27701:2019)

Location reference	**0047358928-001**
Address	Microsoft Corporation 1 Microsoft Way Redmond Washington

	98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3977932
Assessment dates	02/26/2025
Audit Plan (Revision Date)	01/01/2025
Deviation from Audit Plan	No
Total number of Employees	26
Total number of persons with access to PII	26
Total number of PII records	100000
Scope of activities at the site	The Privacy Information System applicable to Microsoft 365 Services Privacy Information Management System Development, Operations and Support.
Assessment duration	3 Day(s)

Redmond / CLOUD 663485 (ISO/IEC 27017:2015)

Location reference	**0047358928-001**
Address	Microsoft Corporation 1 Microsoft Way Redmond Washington 98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3975839
Assessment dates	02/27/2025
Audit Plan (Revision Date)	01/01/2025
Deviation from Audit Plan	No
Total number of Employees	26
Effective number of Employees	26
Scope of activities at the site	The management of Microsoft 365 Service's Information Security Management System (ISMS), development, operations, and protection of personally identifiable information (PII).
Assessment duration	1 Day(s)

Redmond / IS 552878 (ISO/IEC 27001:2022)

Location reference	0047358928-001
Address	Microsoft Corporation 1 Microsoft Way Redmond Washington 98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3974029
Assessment dates	02/24/2025
Audit Plan (Revision Date)	01/01/2025
Deviation from Audit Plan	No
Total number persons within scope of certification across ALL locations	26
Total number of persons within scope of certification at THIS location	26
Scope of activities at the site	The management of Microsoft 365 Service's Information Security Management System (ISMS), development, operations, and protection of personally identifiable information.
Assessment duration	2.5 Day(s)

Redmond / PII 663484 (ISO/IEC 27018:2019)

Location reference	0047358928-001
Address	Microsoft Corporation 1 Microsoft Way Redmond Washington 98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3975838
Assessment dates	02/26/2025
Audit Plan (Revision Date)	01/01/2025
Deviation from Audit Plan	No
Total number of Employees	26

Effective number of Employees	26
Scope of activities at the site	The management of Microsoft 365 Service's Information Security Management System (ISMS), development, operations, support, and protection of personally identifiable information (PII).
Assessment duration	1 Day(s)

Redmond / BCMS 706252 (ISO 22301:2019)

Location reference	**0047358928-001**
Address	Microsoft Corporation 1 Microsoft Way Redmond Washington 98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3994029
Assessment dates	02/24/2025
Audit Plan (Revision Date)	01/01/2025
Deviation from Audit Plan	No
Total number of Employees	26
Effective number of Employees	26
Scope of activities at the site	The business continuity management system in relation to the availability of Microsoft 365 services.
Assessment duration	2 Day(s)

Certification assessment program

Certificate Number - IS 552878
Location reference - 0047358928-001

		Audit1	Audit2	Audit3	Audit4
Business area/Location	**Date (mm/yy):**	02/24	02/25	02/26	02/27
	Duration (days):	4.5	2.5	2.5	4.5
ISMS Changes + ISMS Scope Review		X	X	X	X
Context of the organization		X	X	X	X
Information Security Policy		X	X	X	X
Information Security Objectives		X	X	X	X
Competence, Awareness, Communication		X	X	X	X
Information security risk assessment, information security risk treatment, and Statement of Applicability (SOA)		X	X	X	X
Documented information		X	X	X	X
Management Review		X	X	X	X
Internal Audit		X	X	X	X
Nonconformity and Corrective Action		X	X	X	X
A.5 Information security policies		X	X	X	X
A.6 Organization of information security		X	X	X	X
A.7 Human resource security		X	X	X	X
A.8 Asset management		X	X	X	X
A.9 Access control		X	X	X	X
A.10 Cryptography		X	X	X	X
A.11 Physical and environmental security		X	X	X	X
A.12 Operations security		X	X	X	X
A.13 Communications security		X	X	X	X
A.14 System acquisition, development, and maintenance		X	X	X	X
A.15 Supplier relationships		X	X	X	X
A.16 Information security incident management		X	X	X	X

A.17 Information security aspects of business continuity management	X	X	X	X
A.18 Compliance	X	X	X	X
Transition to 27001:2022 + 2.5 days	X	X		X
Program Management + 1.0 day	X	X		X
27701 (CAV + 3 days)	X	X		X
27018 (CAV + 1 days)	X	X		X
27017 (CAV + 1/2 day)	X	X		X
22301 (CAV + 2 days)	X	X		X

Certificate Number - PII 663484
Location reference - 0047358928-001

		Audit1	**Audit2**	**Audit3**
Business area/Location	**Date (mm/yy):**	02/20	02/21	02/22
	Duration (days):	1.0	1.0	1.0
A.1 General		X	X	X
A.2 Consent and choice		X	X	X
A.3 Purpose legitimacy and specification		X	X	X
A.4 Collection limitation		X	X	X
A.5 Data minimization		X	X	X
A.6 Use, retention, and disclosure limitation		X	X	X
A.7 Accuracy and quality		X	X	X
A.8 Openness, transparency, and notice		X	X	X
A.9 Individual participation and access		X	X	X
A.10 Accountability		X	X	X
A.11 Information security		X	X	X
A.12 Privacy compliance		X	X	X

Certificate Number - CLOUD 663485
Location reference - 0047358928-001

	Audit1	**Audit2**	**Audit3**

Business area/Location	Date (mm/yy):	02/20	02/21	02/22
	Duration (days):	1.0	1.0	1.0
CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment		X	X	X
CLD.8.1.5 Removal of cloud service customer assets		X	X	X
CLD.9.5.1 Segregation in virtual computing environments		X	X	X
CLD.9.5.2 Virtual machine hardening		X	X	X
CLD.12.1.5 Administrator's operational security		X	X	X
CLD 12.4.5 Monitoring of Cloud Services		X	X	X
CLD 13.1.4 Alignment of security management for virtual and physical networks		X	X	X

Certificate Number - BCMS 706252
Location reference - 0047358928-001

		Audit1	Audit2	Audit3
Business area/Location	**Date (mm/yy):**	01/20	02/21	2/22
	Duration (days):	1	1	2
Scope and Policy		X	X	X
Organizational context		X	X	X
Leadership and Commitment		X	X	X
Management System Support			X	X
Planning and Resources		X		X
Human Resource Management			X	X
Control of Documents and Records		X		X
Objectives / Performance Monitoring & Measurement		X		X
Management Review		X	X	X
Supply Chain				X
Internal Audits		X	X	X
Actions / Non-Conformity / Incidents / Complaints		X	X	X
Risk Management / Prevention			X	X
Legal and Other Requirements				X
Improvement		X	X	X

Certificate Number - PM 741035
Location reference - 0047358928-001

		Audit1
Business area/Location	**Date (mm/yy):**	03/21
	Duration (days):	7.5
Scope and Policy		X
Organizational context		X
Leadership and Commitment		X
Management System Support		X
Planning and Resources		X
Human Resource Management		X
Control of Documents and Records		X
Objectives / Performance Monitoring & Measurement		X
Management Review		X
Supply Chain		X
Internal Audits		X
Actions / Non-Conformity / Incidents / Complaints		X
Risk Management / Prevention		X
Legal and Other Requirements		X
Improvement		X

Hybrid Audit Certification Assessment Program

Expected outcomes for accredited certification.

What accredited management system certification means?

To achieve an organization's objectives related to the Expected Outcomes intended by the management systems standard, the accredited management system certification is expected to provide confidence that the organization has a management system that conforms to the applicable requirements of the specific ISO standard.

In particular, it is to be expected that the organization.

• has a system which is appropriate for its organizational context and certification scope, a defined policy appropriate for the intent of the specific management system standard and to the nature, scale and impacts of its activities, products and services over their lifecycles, is addressing risks and opportunities associated with its context and objectives;
• analyses and understands customer needs and expectations, as well as the relevant statutory and regulatory requirements related to its products, processes and services;
• ensures that product, process and service characteristics have been specified in order to meet customer and applicable statutory/regulatory requirements;
• has determined and is managing the processes needed to achieve the Expected Outcomes intended by the management system standard;
• has ensured the availability of resources necessary to support the operation and monitoring of these products, processes and services;
• monitors and controls the defined product process and service characteristics;
• aims to prevent nonconformities, and has systematic improvement processes in place including the addressing of complaints from interested parties;
• has implemented an effective internal audit and management review process;
• is monitoring, measuring, analyzing, evaluating and improving the effectiveness of its management system and has implemented processes for communicating internally, as well as responding to and communicating with interested external parties.

What accredited management systems certification does not mean?

It is important to recognize that management system standards define requirements for an organization's management system, and not the specific performance criteria that are to be achieved (such as product or service standards, environmental performance criteria etc.).

Accredited management systems certification should provide confidence in the organization's ability to meet its objectives related to the intent of the management system standard. A management systems audit is not a full legal compliance audit and does not necessarily ensure ethical behaviour or that the organization will always achieve 100% conformity and legal compliance, though this should of course be a permanent goal.

Within its scope of certification, accredited management systems certification does not imply or ensure, for example:
• that the organization is providing a superior product and service, or
• that the organization's product and service itself is certified as meeting the requirements of an ISO (or any other) standard or specification.

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

Visit the BSI Connect Portal, our web-based self-service tool to access all your BSI assessment and testing data at a time that is convenient to you. View future audit schedules, submit your corrective action plans, and download your reports and Mark of Trust logos to promote your achievement. Plus, you can benchmark your performance using our dashboards to help with your continual improvement journey.

Should you wish to speak with BSI in relation to your certification, please contact your local BSI office – contact details available from the BSI website:

https://www.bsigroup.com/en-US/contact-us/

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 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.