Service name

Service name

Trustmarque Copilot for Microsoft 365

About your service

Service description

Microsoft Copilot for Microsoft 365 is an AI-powered productivity tool that coordinates large language models (LLMs), content in Microsoft Graph, and the Microsoft 365 applications such as Word, Excel, PowerPoint, Outlook, Teams, and others. This integration provides real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills.

Service categories

- Collaborative working
  - Presentations and slides (office productivity)
  - Spreadsheets (office productivity)
  - Word processing (office productivity)
- Creative, design and publishing
  - Presentations and slides (office productivity)
  - Word processing (office productivity)
- Information and communications technology (ICT)
  - Machine learning and artificial intelligence
  - Presentations and slides (office productivity)
  - Spreadsheets (office productivity)
  - Word processing (office productivity)
  - Other information and communications technology (ICT) services

Multi cloud support

No

Service features and benefits

Service features and benefits

Service features

- AI-Powered Productivity: Enhances productivity with AI integration in Microsoft 365.

- Data Residency and Compliance: Ensures EU data residency and compliance.
- Security and Encryption: Offers robust security with encryption.
- Enterprise-Grade Integration: Integrates with M365 policies.

Service benefits

- Efficiency: Streamlines document generation, swift notice issuance.
- Resource Optimization: Automates management of digital case files.
- Productivity: Saves time, improves communication and creativity.
- Customization: Creates tailored scenarios with Copilot Studio.

Service scope

Add-ons and extensions

Software add-on or extension

Yes

What software services is the service an extension to

Microsoft 365 E3/E5 Office 365 E3/E5

Cloud deployment model

Public cloud

Service constraints

Microsoft admins can view the status of services and find out when maintenance is scheduled. Service health information is available at any time by signing in. https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity.

System requirements

- Microsoft 365: Fully hosted, managed SaaS; no on-premises infrastructure needed.
- Cost-effective: Eliminates additional IT infrastructure for Onboarding system support.
- Accessibility: Use on any web-enabled device with modern internet browsers.
- Browser Compatibility: Supports Internet Explorer, Edge, Chrome, Safari.

- Mobile Availability: Native apps for Android and iOS devices provided.

Reselling

Supplier type

Supplier type

I’m a reseller providing extra support

Organisation whose services are being resold

Microsoft

User support

Email or ticketing support

Email or online ticketing support

Yes

Support response times

Response times vary based on support plan selected. For more information, visit: https://www.microsoft.com/en-us/microsoft-365/business/microsoft-365-for-business-support-options

User can manage status and priority of support tickets

Yes

Online ticketing support accessibility

WCAG 2.1 AA or EN 301 549

Phone support

Phone support

Yes

Phone support availability

24 hours, 7 days a week

Web chat support

Web chat support

Yes

Web chat support availability

24 hours, 7 days a week

Web chat support accessibility standard

WCAG 2.1 AA or EN 301 549

Web chat accessibility testing

Microsoft is committed to developing technology that empowers everyone, including people with disabilities. Microsoft has a Disability Answer Desk where customers with disabilities get support with Microsoft Office, Windows, and other products. Microsoft also has Accessibility Conformance Reports (ACR) which describe how products and services support recognized global accessibility standards. https://www.microsoft.com/en-us/Accessibility/disability-answer-desk https://www.microsoft.com/en-us/accessibility/conformance-reports https://learn.microsoft.com/en-us/windows/apps/design/accessibility/accessibility-testing

Onsite support

Yes, at extra cost

Support levels

Microsoft provides four (4) Modern Work support plan options. These include the following: - STANDARD (included for all customers) - BUSINESS ASSIST - PROFESSIONAL DIRECT - MICROSOFT UNIFIED For more information, visit https://www.microsoft.com/en-us/microsoft-365/business/microsoft-365-for-business-support-options

Support available to third parties

Yes

How users work with your service

Browsers

Web browser interface

Yes

Supported browsers

- Microsoft Edge
- Firefox
- Chrome
- Safari

Installation

Application to install

Yes

Compatible operating systems

- Android
- iOS
- Linux or Unix
- macOS
- Windows
- Windows Phone

Mobile

Designed for use on mobile devices

Yes

Differences between the mobile and desktop service

Microsoft offers distinct experiences on mobile and desktop devices for Microsoft 365. On desktop, users access the full suite of features, while the mobile app provides a streamlined interface for essential tasks and allows for offline working when there isn't network connectivity.

Service interface

Service interface

Yes

Description of service interface

Microsoft 365 can be managed via the M365 admin centre: https://learn.microsoft.com/en-us/microsoft-365/admin/?view=o365-worldwide

Accessibility standards

WCAG 2.1 AA or EN 301 549

Accessibility testing

Microsoft is committed to developing technology that empowers everyone, including people with disabilities. Microsoft has a Disability Answer Desk where customers with disabilities get support with Microsoft Office, Windows, and other products. Microsoft also has Accessibility Conformance Reports (ACR) which describe how products and services support recognized global accessibility standards. https://www.microsoft.com/en-us/Accessibility/disability-answer-desk https://www.microsoft.com/en-us/accessibility/conformance-reports https://learn.microsoft.com/en-us/windows/apps/design/accessibility/accessibility-testing

User support

User support accessibility

WCAG 2.1 AA or EN 301 549

API

API

Yes

What users can and can't do using the API

The Microsoft Graph API enables you to access data, intelligence, and insights from Microsoft applications. By integrating Modern Work with Graph API, developers can tap into user data and organizational information to enhance context-aware assistance from applications like Word, Excel, Teams, etc. Starting with users and groups at the core, Microsoft Graph forms a network of Modern Work services and features that manage, protect, and extract data to support a wide range of scenarios. Microsoft Graph lets you access this wealth of user data while always respecting proper authorization. For more information on Microsoft Graph's capabilities, services, and features, visit: - https://learn.microsoft.com/en-us/graph/overview - https://learn.microsoft.com/en-us/graph/overview-major-services For information on Microsoft Graph limitations (throttling limits, service-specific limits, connection limits, schema limits, and availability), visit: - https://learn.microsoft.com/en-us/graph/throttling-limits - https://learn.microsoft.com/en-us/graph/connecting-external-content-api-limits - https://learn.microsoft.com/en-us/graph/metered-api-overview Microsoft Azure OpenAI also offers a suite of artificial intelligence (AI) services that can be seamlessly integrated with Modern Work to enhance its functionality. By leveraging services such as Azure Cognitive Services and Azure Machine Learning, developers can extend capabilities in areas such as code summarization, sentiment analysis of code reviews, and even predictive coding assistance based on historical patterns.

API documentation

Yes

API documentation formats

- Open API (also known as Swagger)
- HTML
- PDF

API sandbox or test environment

Yes

Customisation

Customisation available

Yes

Description of customisation

Modern Work customers can customize their services in various ways: - The Microsoft 365 Admin Centre is a web-based portal where administrators can manage user accounts and settings for their organization. They can add or remove users, manage billing, reset passwords, and more. - The Office Customization Tool allows administrators to customize the installation of Office by choosing which applications and languages are installed, how those applications should be updated, and application preferences. - Users can personalize their Microsoft 365 experience by changing the theme, notifications, and other settings. - The Microsoft 365 Developer Program provides a sandbox environment where developers can learn and experiment with Modern Work technologies. - Developers can use the Microsoft Graph API to interact with data in Modern Work and build apps that integrate with Microsoft 365. For more information, visit: - https://learn.microsoft.com/en-us/deployoffice/admincenter/overview-office-customization-tool - https://learn.microsoft.com/en-us/microsoft-365/admin/setup/customize-your-organization-theme - https://support.microsoft.com/en-us/office/personalize-your-microsoft-365-experience-eb34a21b-52fa-4fbf-a8d5-146132242985

• Onboarding and offboarding

Getting started

Microsoft provides all Modern Work customers with 24/7 self-help resources, including Microsoft Learn, training documentation, templates, and community support. For more information, visit: - https://learn.microsoft.com/en-us/microsoft-365/ - https://support.microsoft.com/en-us/training - https://adoption.microsoft.com/en-us/customer-hub/ - https://support.microsoft.com/en-us/modernworkplace

Documentation

Service documentation

Yes

Documentation formats

- HTML
- PDF

Documentation accessibility standard

WCAG 2.1 AA or EN 301 549

End-of-contract data extraction

When the contract ends, your access to Modern Work services, applications, and customer data go through multiple stages before the subscription is fully turned off, or deleted: 1. Expired Stage (30 days): Users have normal access to Modern Work applications and files. 2. Disabled Stage (90 days): Data is accessible to admins only. Users can't access applications. Admins can access the admin centre to buy and manage other subscriptions. 3. Deleted Stage: After the 90-day retention period ends, Microsoft disables the account and deletes the customer data. During the term of an active subscription, a subscriber can access, extract, or delete customer data stored in Modern Work apps. For more information, visit https://learn.microsoft.com/en-us/microsoft-365/commerce/subscriptions/what-if-my-subscription-expires

End-of-contract process

Microsoft is governed by strict standards and follows specific processes for removing cloud customer data from systems under our control, overwriting storage resources before reuse, and purging or destroying decommissioned hardware. In our Online Service Terms, Microsoft contractually commits to specific processes when a customer leaves a cloud service or the subscription expires. This includes deleting customer data from systems under our control. Please see Data Protection Addendum for full and up to date details about how Microsoft manages your data. https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1 https://learn.microsoft.com/en-us/microsoft-365/commerce/subscriptions/what-if-my-subscription-expires?view=o365-worldwide

Data importing and exporting

Data export approach

Modern Work applications enable users to export their data in numerous ways. For information on how Outlook users can export their data, visit https://support.microsoft.com/en-us/office/export-emails-contacts-and-calendar-items-to-outlook-using-a-pst-file-14252b52-3075-4e9b-be4e-

ff9ef1068f91 For information on how Teams users can export their data, visit https://answers.microsoft.com/en-us/msteams/forum/all/how-to-download-data-and-activities-carried-out-on/0e21a9e5-71c8-4cdd-b817-a019dcd54592

Data export formats

Data export formats

- CSV
- Other

Other data export formats

- Microsoft Excel (as a workbook or PivotTable report)
- Text-only (tab delimited)
- Comma-separated values (CSV)
- Extensible Markup Language (XML)

Data import formats

Data import formats

- CSV
- ODF

Analytics

Metrics

Service usage metrics

Yes

Metrics types

You can use dashboards in the Microsoft 365 admin centre to monitor the health of various Microsoft services. Microsoft 365 Monitoring increases observability and minimizes downtime through providing near real-time user telemetry data with enriched alerts in the Microsoft 365 admin centre's Service Health dashboard. Additionally, Microsoft 365 usage analytics gives you access to a prebuilt dashboard providing a cross-product view of last 12 months and contains many prebuilt reports. Each report provides you with specific usage insights. User-specific information is available for the last full calendar month. For more information, visit: - https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-monitoring - https://learn.microsoft.com/en-US/microsoft-365/admin/usage-

analytics/usage-analytics - https://learn.microsoft.com/en-US/microsoft-365/admin/usage-analytics/enable-usage-analytics - https://learn.microsoft.com/en-us/graph/reportroot-concept-overview

Reporting types

- Through an API
- Real-time dashboards

Scaling

Independence of resources

Microsoft employs a combination of proactive monitoring and efficient management practices to mitigate the impact of demand fluctuations on Modern Work services. Microsoft focuses on several areas of service management to minimize the affect on Modern Work users by demands placed on the service: - Monitoring and Major Incident Management: - Service Desk and Normal Incident Management: - Administration and Feature Management: - Business Consumption and Productivity: For more information, visit: - https://learn.microsoft.com/en-us/microsoft-365/community/maturity-model-microsoft365-servicing-microsoft365-service-change-management - https://techcommunity.microsoft.com/t5/microsoft-365-blog/modern-service-management-for-office-365/ba-p/52793

Public sector networks

Public sector networks

Connection to public sector networks

No

Data-in-transit protection

Protection between networks

Data protection between buyer and supplier networks

- TLS (Version 1.2 or above)
- IPsec or TLS VPN gateway

Protection within your network

Data protection within supplier network

TLS (Version 1.2 or above)

Asset protection

Data storage and processing locations

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

- United Kingdom
- European Economic Area (EEA)
- Other locations

User control over data storage and processing locations

Yes

Datacentre security standards

Complies with a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

Penetration testing

Penetration testing frequency

At least once a year

Penetration testing approach

Another external penetration testing organisation

Protection of data at rest

Protecting data at rest

- Physical access control, complying with CSA CCM v3.0
- Physical access control, complying with SSAE-16 / ISAE 3402

Data sanitisation process

Data sanitisation process

Yes

Data sanitisation type

- Explicit overwriting of storage before reallocation
- Deleted data can’t be directly accessed

Equipment disposal approach

Complying with a recognised standard, for example CSA CCM v.30, CAS (Sanitisation) or ISO/IEC 27001

Availability and resilience

Guaranteed availability

Please note that the following links are collectively a high-level overview, and the actual terms can be found in the specific SLA and refund policy documents. • https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1&year=2023 • https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services • https://support.microsoft.com/en-us/account-billing/how-to-get-a-refund-on-a-microsoft-subscription-67dca30b-b323-44d5-acc2-e02f9902c472 • https://www.microsoft.com/en-us/store/b/returns • https://learn.microsoft.com/en-us/answers/questions/1275102/ms-365-business-premium-service-level-agreement?page=1 • https://learn.microsoft.com/en-us/dynamics365/customer-service/use/overview-service-level-agreements • https://learn.microsoft.com/en-us/training/modules/service-level-agreements/ • https://www.microsoft.com/licensing/servicelevelagreements%29

Approach to resilience

Microsoft's datacentre is designed to be resilient/align with the UK Government's 2nd Cloud Security Principle "Asset Protection and Resilience". * Redundant Architecture: Microsoft online services achieve service resilience through redundant architecture, which involves deploying multiple instances of a service on geographically and physically separate hardware. This provides increased fault-tolerance for Microsoft online services. * Data Replication and Automated Integrity Checking: Data replication and automated integrity checking are also part of Microsoft's strategy to ensure service resilience. * Compliance with UK G-Cloud: Every year, Microsoft prepares documentation and submits evidence to attest that its in-scope enterprise cloud services comply with the 14 Cloud Security Principles of G-Cloud. This gives potential G-Cloud customers an overview of its risk environment. * ISO/IEC 27001 Certification: The compliance process relies on the ISO/IEC 27001 certification. A Government Digital Service (GDS) accreditor then performs several random checks on the Microsoft assertion statement, samples the evidence, and makes a determination of compliance. * UK OFFICIAL Data: The appointment of Microsoft services to the Digital Marketplace means that UK government agencies and partners can use in-scope services to store and process UK

OFFICIAL government data. Please also see: • https://learn.microsoft.com/en-us/compliance/assurance/assurance-resiliency-and-continuity • https://learn.microsoft.com/en-us/compliance/regulatory/offering-g-cloud-uk • https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-uk-g-cloud • https://azure.microsoft.com/en-us/blog/trusted-cloud-security-privacy-compliance-resiliency-and-ip/ • https://azure.microsoft.com/en-us/blog/easing-compliance-for-uk-public-and-health-sectors-with-new-azure-blueprints/

Outage reporting

Microsoft provides several ways to report service outages for BizApps and Azure Cloud: *Public Dashboard: *API: Microsoft offers the Service Communications API in Microsoft Graph *Email Alerts: In addition to the public dashboard, API, and email alerts, Microsoft provides a few more methods for service outage notifications: *Mobile Push Notifications: For urgent issues, Microsoft recommends configuring Service Health alerts to send mobile push notifications through the Azure mobile app. *IT Service Management Tools: Many customers already have ticketing systems and IT service management (ITSM) tools in place. *Power BI Notifications: Power BI provides incident notification so you can optionally receive emails if there's a service disruption or degradation. Please also see: •https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide •https://azure.microsoft.com/en-us/get-started/azure-portal/service-health/ •https://learn.microsoft.com/en-us/graph/service-communications-concept-overview •https://learn.microsoft.com/en-us/azure/service-health/impacted-resources-outage •https://learn.microsoft.com/en-us/azure/azure-monitor/app/sla-report •https://azure.microsoft.com/en-us/blog/how-to-stay-informed-about-azure-service-issues/ •portal.microsoft.com. https://portal.microsoft.com/servicestatus •https://learn.microsoft.com/en-us/power-platform/admin/check-online-service-health •https://learn.microsoft.com/en-us/power-bi/support/service-interruption-notifications •https://techcommunity.microsoft.com/t5/microsoft-defender-xdr-blog/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518 •https://azure.microsoft.com/en-us/blog/three-ways-to-get-notified-about-azure-service-issues/ •https://learn.microsoft.com/en-us/power-bi/support/service-interruption-notifications •https://answers.microsoft.com/en-us/msoffice/forum/all/notifications-regarding-outages/0f8eb1e3-5caf-4e66-bbd9-e94415dba089

• Governance

Named board-level person responsible for service security

Yes

Security governance

Security governance certified

Yes

Security governance standards

- CSA CCM version 3.0
- ISO/IEC 27001
- Other

Other security governance standards

Microsoft adheres to numerous, rigorous security and compliance standards, including CSA CCM version 3.0, ISO 27001, ISO 27018, SOC 1, SOC 2, SOC 3, FedRAMP, and HITRUST, among others. For more on specific compliance, visit: - https://learn.microsoft.com/en-us/compliance/assurance/assurance-governance - https://learn.microsoft.com/en-us/microsoft-365/community/microsoft365-maturity-model--governance-and-compliance - https://servicetrust.microsoft.com/

Information security policies and processes

Microsoft's approach to security governance is multi-faceted and includes several key components: *Microsoft Power Platform: Microsoft Power Platform plays a crucial role in security and governance. It helps secure and govern apps like Power Automate and Power Apps. The platform allows administrators to create simple environment and tenant-wide Data Loss Prevention (DLP) policies. It also provides tools like the Microsoft Power Platform Centre of Excellence (COE) toolkit. *Data Loss Prevention Policies: These policies are used to prevent data leakage and ensure data security. *Security Design Considerations: Microsoft provides best practices for security design considerations. *Governance Model: Microsoft provides guidance on defining the governance model between citizen developers and managed IT services, as well as between central IT and the business unit admins. *Monitoring: Microsoft provides tools for capturing compliance/auditing data and measuring adoption and usage within an organization. *App Governance in Microsoft Defender for Cloud Apps: This provides visibility, remediation, and governance into how apps and their users access, use, and share sensitive data in Microsoft 365 and other cloud platforms. For more detailed information, you may want to explore

these resources on the following resources: •https://learn.microsoft.com/en-us/training/modules/security-governance-intro/ •https://learn.microsoft.com/en-us/power-platform/admin/governance-considerations •https://learn.microsoft.com/en-gb/defender-cloud-apps/app-governance-manage-app-governance?view=o365-worldwide •https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-app-policies-overview •https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-security-privacy-compliance?view=o365-worldwide

Operational security

Configuration and change management standard

Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

Configuration and change management approach

Modern Work enforces change management procedures for both code and non-code changes to maintain its security posture. Detailed change management processes are enforced to maintain system integrity. Service teams utilize ticketing or source control tools to document evidence of approval and track all changes. Changes are deployed through Microsoft's Secure Development Lifecycle (SDL), which includes specific security considerations related to code reviews, tests, and approvals before systematically releasing code into the Modern Work environment. Critical security review and approval checkpoints are part of the SDL. For more information, visit https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-change-management

Vulnerability management type

Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

Vulnerability management approach

Microsoft uses a variety of methods to assess potential threats. The Microsoft Detection and Response Team actively looks for cyberthreats that have penetrated an environment, looking beyond known alerts or malicious threats to discover new potential threats and vulnerabilities. Deploying Patches The pace at which Microsoft deploys patches is dependent on specific requirements. Sources of Information About Potential Threats Microsoft aggregates data from various sources to gather information about potential threats. Please also see: •https://www.microsoft.com/en-

us/security/blog/2022/09/08/part-1-the-art-and-science-of-threat-hunting/
•https://learn.microsoft.com/en-us/microsoft-365/security/defender/criteria?view=o365-worldwide
•https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/overview/windows-autopatch-deployment-guide

Protective monitoring type

Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

Protective monitoring approach

Azure security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include the Microsoft Monitoring Agent (MMA) and System Centre Operations Manager. These tools are configured to provide time alerts to Azure security personnel in situations that require immediate action. Azure continuously monitors and detects risk in your organization, even when devices aren’t connected to the corporate network. Azure security has defined requirements for active monitoring. For a breakdown of initial response times by several level and business impact, please visit https://azure.microsoft.com/en-us/support/plans/response/

Incident management type

Conforms to a recognised standard, for example, CSA CCM v3.0 or ISO/IEC 27035:2011 or SSAE-16 / ISAE 3402

Incident management approach

Microsoft employs a federated security incident response model. Each major online service team adheres to a shared incident management process, shared definitions, shared training to provide consistency. The Microsoft365 Security Response team provides service teams with centralized security expertise and incident response guidance as part of our federated security response model. Responsibilities for security incident response are shared between the Microsoft365 Security Response team and each Modern Work service team. Our incident response strategy, based on the NIST 800-61 response management phases, through phases of interconnected activity: -Preparation -Containment, eradication, recovery -Post-incident activity For more information, visit https://learn.microsoft.com/en-us/compliance/assurance/assurance-incident-management

• Staff security

Staff security clearance

Staff screening performed with conforms to BS7858:2019

Government security clearance

Up to Developed Vetting (DV)

Secure development

Approach to secure software development best practice

Answer question

Identity and authentication

User authentication

User authentication needed

Yes

User authentication

- 2-factor authentication
- Public key authentication (including by TLS client certificate)
- Identity federation with existing provider (for example Google apps)
- Limited access over government network (for example PSN)
- Dedicated link (for example VPN or bonded fibre)
- Username or password

Access restrictions in management interfaces and support channels

Using Microsoft Entra, Modern Work allows you to create or update dynamic groups based on defined rules. These groups automatically adjust their membership based on specified criteria. You can implement multifactor authentication and control device access based on group, team, or site sensitivity, as well as use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites. Sensitivity labels enable you to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites. You can block access entirely from unmanaged devices or allow limited, web-only access. SharePoint, can restrict access to sites from specified network locations.

Access restriction testing frequency

At least once a year

Management access

Management access authentication

- 2-factor authentication
- Public key authentication (including by TLS client certificate)
- Identity federation with existing provider (for example Google apps)
- Limited access over government network (for example PSN)
- Dedicated link (for example VPN or bonded fibre)
- Username or password
- Other

Description of management access authentication

The identity/access management features that are built into Azure products/services help protect your organizational and personal information from unauthorized access while making it available to legitimate users whenever and wherever they need it. For information: https://azure.microsoft.com/en-us/services/active-directory/ -Microsoft Entra Authenticator (formerly Microsoft Authenticator) -Password policy enforcement -Token-based authentication -Role-based access control (RBAC) -Integrated identity management (hybrid identity) -Secure infrastructure Azure is the foundation for many Microsoft services. Microsoft Entra ID (Azure Active Directory) and Windows Server Active Directory Domain Services enable you to monitor access patterns both in the cloud and on-premises, and identify/address unauthorized access attempts/other potential threats.

Audit information for users

Audit for buyers' users' actions

Access to user activity audit information

Users have access to real-time audit information

How long user audit data is stored for

User-defined

Audit for suppliers' users' actions

Access to supplier activity audit information

Users have access to real-time audit information

How long supplier audit data is stored for

User-defined

How long system logs are stored for

User-defined

Standards and certifications

ISO/IEC 27001 certification

ISO/IEC 27001 certification

Yes

Who accredited the ISO/IEC 27001

The Certification Body of Schellman & Company, LLC

ISO/IEC 27001 accreditation date

28/11/2023

What the ISO/IEC 27001 doesn’t cover

Not Applicable

ISO 28000:2007 certification

ISO 28000:2007 certification

No

CSA STAR certification

CSA STAR certification

Yes

CSA STAR accreditation date

2013

CSA STAR certification level

Level 2: CSA STAR Attestation

What the CSA STAR doesn’t cover

Not Applicable

PCI certification

PCI certification

Yes

Who accredited the PCI DSS certification

Coalfire, an independent Qualified Security Assessor (QSA) company

PCI DSS accreditation date

15/03/2021

What the PCI DSS doesn’t cover

Not Applicable

Cyber essentials

Cyber essentials

Yes

Cyber essentials plus

Yes

Other security certifications

Other security certifications

Yes

Any other security certifications

https://learn.microsoft.com/en-us/compliance/regulatory/offering-home?view=o365-worldwide