STATEMENT OF WORK- M365 Security Assessment

For Click or tap here to enter text.

Ref: Click or tap here to enter text.

Version 1.0

1. Document Control Information

1.1 Version Control

Document Version	Revision Date	Author	Revision Summary	Distribution List(s)
0.1	Click or tap here to enter text.	Click or tap here to enter text.	Initial Draft	A

1.2 Distribution List

Name	Company	Contact Details	Project Responsibility	Review		
				A	B	C
Click or tap here to enter text.	Cisilion	Click or tap here to enter text.	Solutions Architect	X		
Click or tap here to enter text.	Cisilion	Click or tap here to enter text.	Account Director	X		

Key: A = Draft; B = General release issue; C = For information purposes

1.3 Disclaimer

1.4 Validity

This Statement of Work will be issued to the named recipient(s), on or before 23/05/2023 and is valid for acceptance for a period of 31 days.

1.5 Definitions

	Definition
Change Control Pricing	New pricing given to the Client for additional days going beyond the initial Project Delivery Timeframe
Change Control Quote	Quotes provided by Cisilion stating any Change Control Pricing
Project Delivery Timeframe	the duration of the works as quotes in this statement of works (SoW)
Project Kick-off Date	the date that Project delivery commences
Professional Services Days	the number of professional service days as per this SoW
Project	the works specified in this SoW

2. Introduction

This Statement of Work (**SoW**) is entered into on the date signed by both parties, this agreement is between **Cisilion Limited** a company incorporated in England and Wales (company registration number 03902228) whose registered is at Cisilion House, Guildford Road, Leatherhead, Surrey, United Kingdom, KT22 9UT (**Cisilion**) and [INSERT CLIENT NAME & COMPANY ADDRESS] (**Client**) and describes the services (**Services**) to be provided by Cisilion to the Client to assist the Client with [INSERT DETAILS] (**Project**) for the Initial Term of [Insert agreed initial term].

Each a "**Party**" and together, the "**Parties**"

By entering into this SoW and by signing below, the Client acknowledges and agrees to the terms of the Agreement as set out at Terms and Conditions (**Agreement**) and that such terms are incorporated by reference herein. Where no such agreement exists between the parties or such agreement has expired, Cisilion's standard terms and conditions shall govern, a copy of which can be found at here. https://www.cisilion.com/terms-of-sale

This SoW together with the Agreement and any other document agreed between the Parties, constitutes the entire agreement between the Parties in relation to the supply of the Services, to the exclusion of all other terms, including any terms. This SoW is a separate and severable contract between Cisilion and the Client.

This SoW shall be governed by and construed in accordance with the laws of England and Wales and the Parties hereby submit to the exclusive jurisdiction of the English courts.

Interpretation:

- Except as defined in this SoW, all capitalised terms used in this SoW shall have the meaning given to them in the Agreement.
- The terms set out in this SoW are in addition to and should be read in conjunction with the terms of the Agreement. In the event of a conflict between the Agreement and the SoW, the Agreement shall take precedence over the SoW unless specifically stated within the SoW.
- This SoW and the Agreement supersedes all prior agreements, arrangements, and understandings (and excludes any pre-Agreement communications of whatsoever nature) between the Parties and constitutes the entire agreement between the Parties relating to the subject matter hereof. Each Party agrees that it shall have no remedies in respect of any representation or warranty (whether made innocently or negligently) that is not set out in this Agreement.

This SoW defines the Services and Deliverables that Cisilion will provide to the Client. This includes the following:

- The working relationship between Cisilion and the Client including roles and responsibilities.
- A description of deliverable items under this SoW.
- The process for delivery and acceptance.
- The price and payment schedule.

3. Client Details

3.1 Client Contact Details

Name	Phone	Email

3.2 Location

Site Name	Address
Remote	All work will be remote

4. Project Overview

The primary objective of this project is to conduct a comprehensive security assessment of a Microsoft 365 environment. This environment encompasses Azure Active Directory, Microsoft Defender, Exchange Online, Teams, SharePoint, and OneDrive. The security baselines used for the assessment will align with the industry-leading guidance of the Cybersecurity and Infrastructure Security Agency (CISA).

4.1 Objectives

The objectives for this engagement are to:

1. Evaluate the organization's current M365 security posture.
2. Identify potential security vulnerabilities or weaknesses.
3. Provide a detailed list of recommendations for improving security, aligned with CISA's guidelines.

4.2 Equipment Bill of Materials

Type	Item Description	Quantity
	n/a	

Key: HW = Hardware, SW = Software, LIC = License

5. Solution Description

The Microsoft 365 Security Assessment solution comprehensively evaluates an organization's current M365 security posture, pinpoints any vulnerabilities, and suggests improvements to meet industry-standard best practices outlined by the Cybersecurity and Infrastructure Security Agency (CISA).

5.1 Solution Components

5.1.1 Azure Active Directory Assessment

We will conduct an in-depth analysis of user and administrative access controls, monitoring suspicious activity, and compliance with security best practices. This assessment will help to identify misconfigurations, excessive permissions, unmonitored administrative accounts, and ensure Multi-Factor Authentication (MFA) is appropriately implemented.

5.1.2 Microsoft Defender Assessment

Our solution includes an exhaustive evaluation of antivirus and anti-malware configurations, endpoint detection and response mechanisms, and automated investigation and remediation capabilities. We aim to identify any gaps in the organization's defense and provide recommendations to strengthen endpoint security.

5.1.3 Exchange Online Assessment

This assessment will focus on protection measures against spam, malware, and other threats. It will scrutinize the organization's data loss prevention measures, email encryption practices, and mail flow rules to ensure maximum security and compliance with best practices.

5.1.4 Teams Security Assessment

We will evaluate access controls, data privacy, and adherence to security standards within Teams. This will include an analysis of guest access, external sharing, meeting and calling policies, and data governance and compliance features.

5.1.5 SharePoint and OneDrive Assessment

This part of the assessment will analyze data access controls, data loss prevention measures, and compliance with encryption standards. It will also cover sharing settings, versioning settings, data recovery options, and auditing capabilities.

5.2 Expected Outcomes

The organization will have a clear understanding of its current security posture within the Microsoft 365 environment, including identified vulnerabilities and a path to remediation. The implementation plan will enable the organization to enhance its M365 security posture and align with CISA's industry-leading security guidance.

By leveraging this solution, the organization can significantly reduce the risk of security breaches, ensure compliance, and maintain a robust Microsoft 365 security infrastructure.

5.3 Sample Report Extract (Azure Active Directory)

Please not that this section holds an example set of recommendations within the Azure Active Directory segment of the assessment.

Requirement	Result	Criticality	Details
Legacy authentication MUST be blocked	Fail	Must	0 conditional access policy(s) found that meet(s) all requirements.
MFA MUST be required for all users	Fail	Must	0 conditional access policy(s) found that meet(s) all requirements.
SMS or Voice as the MFA method MUST NOT be used	Fail	Must	SMS is currently enabled for a subset of users.
A minimum of two users and a maximum of four users MUST be provisioned with the Global Administrator role	Fail	Must	23 global admin(s) found.
Users that need to be assigned to highly privileged Azure AD roles MUST be provisioned cloud-only accounts that are separate from the on-premises directory or other federated identity providers	Fail	Must	17 admin(s) that are not cloud-only found.
Activation of highly privileged roles SHOULD require approval	Warning	Should	6 role(s) that do not require approval to activate found: Application Administrator, Cloud Application Administrator, Exchange Administrator, Global Administrator, Hybrid Identity Administrator, Privileged Role Administrator,
Managed devices SHOULD be required for authentication	Warning	Should	0 conditional access policy(s) found that meet(s) all requirements.
Guest users SHOULD have limited access to Azure AD directory objects	Pass	Should	Permission level set to "Limited access" (authorizationPolicy)

A notification SHOULD be sent to the administrator when high-risk users are detected	Pass	Should	This has been set up
If phishing-resistant MFA cannot be used, an MFA method from the list (Microsoft Authenticator, OTP) MUST be used in the interim	Pass	Must	Microsoft Authenticator is being used.

6. Deliverables

The following deliverables are considered as a part of this SoW. For all the Deliverables performed under this SoW, Cisilion will assess the Deliverables and assign the most relevant resource considering the complexity, skillset, knowledge, expertise, timeline, and business impact of the Deliverable. This will be at Cisilion's sole discretion, and we shall endeavour to maximise the Client's experience.

6.1 Deliverables, Acceptance Testing and Acceptance Criteria

The Client's technical project sponsor will be responsible for agreeing that described Acceptance Testing and Acceptance Criteria have been met. The following Acceptance Testing and Acceptance Criteria for the Deliverables are as follows:

Ref	Deliverables Name	Acceptance Testing	Acceptance Criteria	Acceptor
DEL001	Initial workshop to discuss access to the environment and handover of credentials to consultant	Credentials to be handed over to consultant to be able to start the project	Consultant able to log into client environment	Cisilion
DEL002	Data gathering on Azure Active Directory, MS Defender, Exchange Online, Teams, SharePoint and OneDrive	Data to be extracted from M365 tenant and compiled.	Cisilion to gather all information needed to proceed to create a report	Cisilion
DEL003	Microsoft 365 Security Report covering the areas in DEL002 which will provide the client with guidance and advice for there M365 environment	N/A	Completed Document	Client
DEL004	A Cisilion Solution Architect to work with client to scope any remediation work that Cisilion will need to assist with	N/A	Next steps document	Client/Cisilion

7. Exclusions and Constraints

7.1 Exclusions

The following activities are considered outside of the scope of Cisilion's activities:

- Weekend and out of hours work unless stated explicitly in this SoW; If the Client requires the Cisilion consultant to work weekends or out of hours, additional charge will be incurred at Cisilion's then current rate.
- On-site attendance of engineers, all Services to be performed remotely unless stated explicitly in this SoW. If on-site attendance is required, this shall follow any current (at the time of the required Site visit) government advice and/or restrictions in relation to COVID as well as any health and safety requirements confirmed by the Client to Cisilion in writing. Cisilion may also charge for travel and accommodation as per Cisilion's then current rate.
- Reconfiguring, redeploying, or changing any device, software or service not outlined in this SoW.
- Training on deployed solutions, unless stated explicitly in this SoW.
- For the avoidance of doubt, any activity not listed in the SoW is not included within the Deliverables.

7.2 Constraints

The dependencies for project success that fall outside of Cisilion's control are referenced here for the purposes of clarity, expectation, and risk management.

- n/a

7.3 Responsibility Matrix

This matrix should be used to define responsibilities for all known activities, assumptions, and provision of materials.

*Cisilion and Cisilion's approved 3rd Parties

**External/Client third Parties, not under Cisilion's control

Item	Client	Cisilion	Third Party	Out of Scope
Scheduling required Kick Off, Discovery and Review Sessions	X	X		
Providing the necessary access to the **Error! Reference source not found.** M365 Tenancy for conducting the audit	X			
Recommendations Documentation Review and Walkthrough		X		
Project Sign Off	X			
Management of client 3rd parties	X			
Management of supplier 3rd parties		X		

Supply of additional equipment, licences that may be required	X	X		
Access to resource to enable the activities defined in this Scope of Works to be performed	X			
Notification of regulations that Cisilion may be required to work under	X			
Notification of any special access requirements for accessing client's environment.	X			
Single point of contact for project related issues	X	X		
Notification of change in scope.	X	X		

8. Client Responsibilities

The Client agrees that the successful performance of this SoW by Cisilion depends upon the Client's compliance with the following :

- Cisilion are provided access to:
  - The Client's staff.
  - The Client's premises including computer room and wiring closets.
  - Network infrastructure documentation.
  - Network device management.
  - secure data remote access.
  - Any other facilities reasonably requested.
  - Consultant must be provided with the following permissions to conduct the report:

Product	Role
Azure Active Directory	Global Reader
Teams	Global Reader (or Teams Administrator)
Exchange Online	Global Reader (or Exchange Administrator)
Defender for Office 365	Global Reader (or Exchange Administrator)
Sharepoint Online	SharePoint Administrator
OneDrive	SharePoint Administrator

- The Client is committed to:
  - Working with Cisilion to configure network devices if required.
  - Ensure quick turn-around times on queries.
  - Meeting attendance.
  - Scope change management process.
  - Managing any interdependencies with other projects.
  - Providing all required information and accurately identifying design and project constraints.
  - Designating a backup when the primary Client PM is not available.
  - To allow Cisilion's consultants to use the Client's name in any engagement with third parties for this SoW and if necessary, provide a letter of authority (not to be unreasonably withheld of delayed) and confidentiality agreement that can be used prior to any engagement, particularly as commercial vendors will be used.
  - Providing a single point of contact to whom all Cisilion communications are to be addressed. This Client contact shall have the authority to act on all aspects of the services including binding the Client to any supplemental documents necessary. Including any undertaking to guarantee continuous supply of any relevant resource and information required to fulfil the Client's obligations under this SoW.
  - Requirements for change to the project scope will be communicated to the Cisilion Project Manager or assigned Project Coordinator.

- Providing Cisilion with a copy of the Client's health and safety policy prior to any site activity taking place and notify Cisilion of any Personal Protective Equipment (PPE) required at least five (5) business days prior to any relevant site activity. The Client must provide a single point of contact for any health and safety issues related to individual site(s).

9. Governance

9.1 Project Management

On receipt of a signed copy of this SoW, Cisilion will align a Project Manager to manage the delivery of the project. Full details of our PMO and the methodologies used are available within our PMO Service Description, available on request.

9.2 Scope Change

If the Client would like Cisilion to undertake any additional work, not included in this SoW, the Client can request this via a Change Request, as per 9.3.

It may become necessary to amend this SoW for as a result of, but not limited to, the following:

- Changes to this SoW and/or specifications for the Services or deliverables
- Changes to the project schedule
- Non-availability of resources which are beyond either Party's control
- The inability of external vendors to provide a suitable product
- Information that was not known at negotiation and creation of this SoW comes to light which if known would have affected the quotation
- Environmental or architectural impediments not previously identified
- Client obligations not being met
- Delays to the project schedule beyond Cisilion's control.

The Client acknowledges that change requests will have an impact on the price and schedule of the Services as stated in this SoW. This includes both the impact of performing the change request evaluation and the impact of the change request implementation.

9.3 Change Approval Process

The Client will identify the representative who will be designated as the authorized representative for approving changes, as per the Agreement, to this SoW.

The Cisilion Project Manager will be designated as the authorized Cisilion representative for approving changes, as per the Agreement, to this SoW.

9.4 Project Reporting

Review sessions (if required) will be held to ensure the project deliverables are met on time, as listed in the latest mutually accepted plan for the project.

- Review sessions will be held as agreed to assess the project progress.
- Review sessions will be attended by the Client's Project Manager and the Cisilion Project Manager
- The review session will also review:
    - any required changes to this SoW
    - general progress and acceptance of the activity undertaken by Cisilion

Review sessions will be delivered in a form of telephone/conference calls or face to face meetings as appropriate.

9.5 Communication and Reporting

Communication and Reporting related to this project will follow the communications plan below.

Audience Groups:

- **All** – everyone associated with the project
- **Executive Sponsors** – Cisilion executive representative
- **Project Team** – those involved in the day-to-day project activities
- **Super Users** – those involved with Acceptance Testing and initial training

Activity	Format	Vehicle	Responsibility	Audience	Frequency
SOW	Word	Email	Cisilion	Project Team	Once
Kick-off meeting	Conference Call – MS Teams	Conference Call – MS Teams	Cisilion	Project Team	Once
Kick-off meeting minutes	Word	Email	Cisilion	Project Team	Once
Status Update Meetings	Conference calls + emails	Conference calls + emails	Cisilion	Project Team	Weekly as needed
Final Documentation	Word	Email	Cisilion	Project Team	Once
Review Meeting and Closure	Conference Call – MS Teams	Conference Call – MS Teams	Cisilion	Project Team, Executive Sponsor	Once

10. Price and Payment Schedule

Task	Total
M365 Security Assessment covering all areas in Section 6 of this document	£5,000.00
Total (Ex VAT)	£5,000.00

Commented [AH1]: just use one line to refer back to the deliverables in section 6. @Jon Jarvis

Total Fees for the Professional Services associated with this project will be £4,200.00 excluding VAT (the "Fees").

Any reasonable expenses incurred will be invoiced to the Client at cost.

Cisilion reserve the right to raise an invoice for any hardware being purchased on receipt of your purchase order/signed quote/signed SOW, whichever is relevant for Professional Services (PS) [(except Goods)]. Payment of invoices shall be as set out below:

Cisilion will invoice for the engagement as follows:

- Equipment (including software licences) will be invoiced at the time of delivery to the Client Site, or, if earlier (for example where Cisilion is pre-staging the equipment in its own facility) when the equipment is delivered to Cisilion;
    - Professional Services including design, installation and consultancy shall be invoiced upon completion of the relevant milestone as set out below:
        - 50% of upon signature of this document.
        - 50% following project acceptance.
- Cisilion reserves the right to raise an invoice for any hardware or software being purchased on receipt of the Client's purchase order/signed quote/signed SoW, whichever is relevant.
- Payment terms which are 30 days from the date of invoice are as set out in the Agreement.
- Cisilion shall not be liable for any failure of or delay in the provision of the project which is caused or contributed to by the Client failing to:
    - Comply with its specific responsibilities set out in the agreed project plan; or
    - Any other actions or omissions of the Client (or any third party appointed by or under the control of the Client).
    - Deliver any of the items shown as being the Client's responsibility within the responsibilities matrix in the timeframe shown.

In the case of such failure or delay the timetable or any completion date agreed by the parties for the work specified in this SoW shall be automatically extended to the extent that the failure or period of delay was caused or contributed to by the Client and the Client shall be responsible for paying any additional costs incurred by Cisilion as a result.

If the number of Professional Services Days quoted in this SoW are exceeded prior to the completion of the Project, Cisilion reserves the right to issue a Change Control Quote at the then current Cisilion standard Fees for any additional days required to complete the project. Cisilion shall not continue to deliver the Services for any additional days until the Parties have agreed the Change Control Pricing in writing.

Unless the Project Delivery Timeframe in this SoW states differently, should the Project Delivery Timeframe exceed 12-months from the initial Project Kick-off Date then Cisilion reserves the right to re-quote the Project based on Cisilion's then standard Fees as of the time of re-quoting. Cisilion reserves the right to put any further works on-hold until the Parties have agreed the revised pricing.

Should this SoW be for up to 9 days' and/or £9,999 the SoW shall remain valid for up to 6 months maximum. Should this SoW be for 10+ days and/or £10,000+ the SoW shall remain valid for up to 12 months maximum.
Should this SoW be milestone based and/or contain invoicing triggers, and Cisilion reach the end of the 6-month or 12-month period (whichever applies), if any works performed exceed the last milestone and/or invoice trigger, Cisilion reserve the right to invoice the Client for the actual days worked.
Where Cisilion requote the SoW, this shall be based on Cisilion's then current rates.

10.1 Late Cancellation

The Client technical project sponsor will be responsible for agreeing that described acceptance criteria have been met. Specific acceptance criteria for the project deliverables are described as follows:

If the Client cancels scheduled work with less than 72 hours' notice, Cisilion reserves the right to charge for the consultancy time using the following sliding scale:

#	Notice	Charge
1	Less than 120 hours' notice (5 days)	25% of the Charges
2	Less than72 hours' notice (3 days)	50% of the Charges
3	Less than 48 hours' notice (2 days)	75% of the Charges
4	Less than 24 hours' notice	100% of the Charges

Similarly, when Cisilion personnel, or an appointed contractor, attends site and an installation fails because of the Client's documented responsibilities not being met, or site access being refused, Cisilion reserves the right to charge for the consultancy time at the same day rate.

11. Sign off

Please indicate your agreement with the terms of this SoW and the terms of the Agreement, which sets out the terms of our relationship, and allow Cisilion to commence work as specified by signing on the space provided below. In addition to this please also supply a Purchase Order for the full amount and return both to your Account Director jbeckram@cisilion.com.

	Client
Authorised Signature:	
Printed Name:	
Title:	
Date:	
Email Address:	
Purchase Order Number:	