FREE TEMPLATE · STATEMENT OF WORK

Microsoft 365 Security Assessment — SOW Template

A complete scoping template for a Microsoft 365 / Zero Trust security assessment: strategy workshop, five discovery sessions, independent analysis, and an executive roadmap readout.

How to use this template

This is the SOW structure I use to scope a Microsoft 365 / Zero Trust security assessment engagement — a strategy workshop plus five discovery sessions, independent technical analysis, and an executive readout. Replace every «bracketed» placeholder with your own details before use. This is a scoping template, not legal advice — have counsel review terms, liability, and confidentiality language before you send it to a client.

Executive summary

«Client Abbreviation» has engaged «Consultant/Firm Name» to provide a holistic assessment of their Microsoft 365 environment. The assessment will review the current state of the environment and provide recommendations on future-state enhancements, including an analysis of the customer’s cross-platform security posture, evaluating vulnerabilities and identifying risks with recommendations to mitigate.

Objectives

- Evaluate current state of the Microsoft 365 tenant.
- Compare current state against Microsoft and CIS configuration baseline recommendations.
- Identify opportunities to remove duplication and cost of tooling by consolidating to a single platform.
- Build an Executive Security Adoption Roadmap including cost analysis, benefits and ROI, and/or licensing changes.

Scope of services — in scope

Strategy and Plan Workshop

Duration: 1 hour · **Audience:** technical and business stakeholders

- Provide an end-to-end view of the assessment engagement process and clarify roles and responsibilities.
- Current-state environment overview and licensing analysis.
- Discuss business objectives and priorities around security.
- Define specific outcomes that define success for the program.
- Zero Trust overview; Microsoft Secure Score and Defender for Cloud Secure Score; CIS tenant and endpoint benchmarks.

Discovery #1 — 365 tenant security and configuration best practices

Duration: 1.5 hours · **Audience:** technical

- Complete Zero Trust heatmapping exercise.
- Compare initial tenant review against Microsoft and CIS recommended baselines.
- Validate DMARC/DKIM/SPF records and review DMARC reporting options.
- Discuss current challenges or pain points with the tenant configuration.

Discovery #2 — Endpoint management

Duration: 1.5 hours · **Audience:** technical

- Review current Intune / ConfigMgr / device management configuration.
- Document current device lifecycle management and deployment technologies and methods.
- Discuss current mobile device and BYOD strategies and challenges.

Discovery #3 — Identity and access management

Duration: 1.5 hours · **Audience:** technical

- Review changes to password recommendations from NIST and Microsoft.
- Document current Conditional Access policies and run tooling to check for identities excluded or not captured by existing policies.
- Demonstration of an advanced layered Conditional Access approach.
- Review current state of passwordless authentication.

Discovery #4 — Microsoft security technologies

Duration: 1.5 hours · **Audience:** technical

- Defender for Endpoint / XDR configuration analysis.
- Check health and deployment of Defender for Identity and ensure on-premises AD is properly integrated.
- Defender for Office health check.
- Network access control platform integration with Intune device compliance.
- Competitive licensing analysis of third-party security tooling where overlaps exist with existing Microsoft licensing.

Discovery #5 — Data protection and lifecycle management

Duration: 1.5 hours · **Audience:** technical and compliance

- Identification of sensitive company data in the tenant.
- Validate DLP and alerting policies on data ingress and egress.
- Document insider-risk protection strategies.
- Review structure and governance for SharePoint sites and Teams, including creation and archiving processes.
- Copilot preparation.

Technical analysis and planning

«Consultant» works independently analyzing data and assembling the final report; no time commitment from the customer is needed beyond availability for questions.

- Evaluate security posture with all available Microsoft Secure Score and Azure Secure Score analysis.
- Analyze security gaps and vulnerabilities to compile recommendations aligned to the Zero Trust framework.
- Outline and create the final presentation of recommendations.

Findings and recommendations to «Client»

Duration: 1.5 hours · **Audience:** technical and business stakeholders

- Review the project deliverable: business objectives and project scope, summary of technical workshops, and results and recommendations of the technical analysis.
- Review the proposed executive roadmap: prioritized risk-mitigation recommendations with appropriate Microsoft 365 solutions and benefits; third-party security solutions that can be offset by recommendations, with savings; licensing requirements and justification.
- Discuss updates, changes, and questions.

Scope of services — out of scope

- Review of software, server, and desktop assets: unmanaged devices, unsupported desktop and Windows Server OS versions, aging hardware warranty schedules, hardware refresh planning.
- Deployment of third-party scanning software.
- Implementation of Microsoft 365 or third-party solutions.
- Any other action or activity not specifically identified as being in scope.

Key deliverables and schedule

Schedule assumes sequential execution at or near full time and may shift based on availability on either side.

Deliverable	Description	Schedule
Strategy & Planning Workshop	Project kick-off; end-to-end view of the assessment; business objectives and priorities	Week 1
Discovery Session #1	Zero Trust matrix completion; 365 tenant security and configuration best practices	Week 1
Discovery Session #2	Endpoint management	Week 2
Discovery Session #3	Identity and access management	Week 2
Discovery Session #4	Microsoft security technologies	Week 3
Discovery Session #5	Data protection and lifecycle management	Week 3
Technical Analysis & Planning	Creation of final deliverable presentation	Week 4
Formal Presentation of Findings	Review recommendations and executive roadmap	Week 5

Roles and responsibilities

«Consultant» role

- Enterprise consultant providing expertise in the Microsoft security platform.
- Communicate with the project coordinator to keep «Client» and «Consultant» team members aware of technical direction.
- Provide a focal point for all communication and project activities.

«Client» roles

Role	Time commitment	Responsibilities
Executive Sponsor	1–4 hours per week	Identify and set business priorities, vision, and scope; establish and sustain the business case
Security Team	1–4 hours per week	Review results and recommendations to validate solutions conform to security guidelines
IT Team	1–4 hours per week	Assist with review and planning

«Client» responsibilities

- Provide the name of a single point of contact in writing prior to the start of the engagement, empowered to ensure all «Client» tasks can be completed within the allotted timeframe.
- Manage project issues, risks, and escalations.
- Provide technical resources with working knowledge of the project as a point of contact for each IT tower/team involved.
- Provide all remote access capabilities needed to perform work prior to project kick-off.

Assumptions, dependencies, and constraints

- «Consultant» shall not be responsible for project delays caused by «Client» conditions such as (but not limited to) product licensing, encryption certificates, personnel challenges, or facility issues.
- If third-party vendor involvement is required, «Client» will take responsibility to engage the vendor, and «Consultant» will not be responsible for resultant delays.
- «Consultant» will not access «Client» systems under a shared identity, and will request a new, dedicated account for any resource that requires system access.
- Completing this project within the agreed timeframe is contingent on receiving the necessary information and access to required resources, personnel, and facilities in a timely manner.

Unique project assumptions

- «Consultant» will require the Global Reader role in the Microsoft 365 tenant. *(Least privilege applies to consultants too: read-only access is sufficient for an assessment — no assessment engagement needs Global Admin.)*

Pricing

«Consultant» will deliver the project to the scope and deliverables listed in this statement of work. Any additional services requested that fall outside this scope will be handled as a change request, agreed to and signed off by both parties, with additional timeframes and costs documented in the approved change request.

Pricing detail — invoicing based on written acceptance of milestone completions, with payment due within the terms of this SOW:

Milestone	Acceptance criteria	Not-to-exceed amount
1	Project commencement — due at SOW signature	«$ amount»
Total fixed cost		**«$ amount»**

Ongoing support

Once the project is completed, technical support is available for purchase via a separate managed support agreement for both business-hours and after-hours support.

Travel

«State whether travel is required; if remote-only, say so explicitly.»

Confidentiality

Both parties agree to maintain the confidentiality of all proprietary information and trade secrets disclosed during the term of this SOW. *(Have counsel align this with your existing MSA/NDA framework.)*

Acceptance

Signature and date blocks for «Consultant» and «Client» authorized representatives.
